TRINITY TI
GESTÃOINTEGRADA EM T.I.

EBOOK GRATUITO — ESCRITÓRIOS CONTÁBEIS

GUIA DE TI PARA CONTADORES

Como montar uma infraestrutura segura, econômica e em conformidade com a LGPD no seu escritório contábil.

1.627	+20	97%
EMPRESAS ATENDIDAS	ANOS DE MERCADO	SATISFAÇÃO

Leia este guia e proteja os dados dos seus clientes ainda hoje.

Leia mais em: trinityti.com.br

Missão Trinity TI

Na Trinity TI, facilitamos a relação entre contadores e tecnologia, proporcionando mais segurança, eficiência e conformidade com a LGPD nos escritórios contábeis.
Com soluções personalizadas e suporte ágil, somos o parceiro de TI que você precisa para crescer sem depender de improvisação ou sorte tecnológica.

Sumario

00 **Introdução**
Porqueescritórios contábeis correm risco com a TI?

01 **Capítulo 1 — Segurança de Dados & LGPD**
O que a lei exige e como implementar na prática

02 **Capítulo 2 — Backup Inteligente**
Regra 3-2-1 e como escolher a solução certa

03 **Capítulo 3 — Antivírus e Ransomware**
Por que contábilidades são alvo e como se proteger

04 **Capítulo 4 — Redes e Acessó Remoto**
Wi-Fi, VPN e segmentação para home office seguro

05 **Capítulo 5 — Suporte e Continuidade**
ComoescolherumparceirodeTIemontarumplano B

\+ **Bônus — Checklist com 30+ Pontos**
Avalie a infraestrutura do seu escritório agora

INTRODUÇÃO

Por que escritórios contábeis correm riscocom a TI?

A TI negligenciada é a porta de entrada para perdas financeiras, multas e danos a reputação.

O Custo Oculto da Ineficiência

Vivemosem umaera onde a tecnologia deveriasimplificar a vida do contador. Mas para 7 em cada 10 escritórios contábeis no Brasil, ela se tornou uma fonte constante de gastos não planejados, riscos desnecessários e dores de cabeca evitáveis.

70%	3x	R$50M	48h
SEM BACKUP TESTADO	MAISVULNERÁVEIS A RANSOMWARE	MULTA MÁXIMA LGPD	MÉDIA PARA RECUPERAR DADOS

Alem dos custos visíveis de TI (licenças, equipamentos, internet, suporte), existem custos invisíveis muito maiores: o downtime que paralisa o escritório no dia de entrega do SPED, o ransomware que criptografa anos de documentos, a multa de LGPD por vazamento de dados de um cliente, a perda de reputação que não tem preço.

Este guia foi desenvolvido pela equipe Trinity TI com base em mais de 20 anos de experiência. Cada capítulo traz orientações práticas que você pode comecar a aplicar ainda hoje, sem precisar de um orçamento milionário.

CAPÍTULO 1

Segurança de Dados & LGPD

O que a lei exige do seu escritório contábil e como implementar as medidas certas.

01

O que a LGPD Exige de Você

Escritórios contábeistratam uma quantidade enormede dados pessoais: CPF, CNPJ, folhas de pagamento, dados bancários e informações de saude de centenas de clientes. A Lei Geral de Proteção de Dados (LGPD) não é opcional e se aplica a você.

Medidas técnicas obrigatórias:

Controle de acesso: Cada colaborador acessa apenas o que precisa. Nada de senha compartilhada ou acessó total a todos.

Criptografia: Dados em repousó e em transito devem ser criptografados, especialmente backups e e-mails com dados de clientes.

Registro de atividades (logs): Saber quem acessou o que e quando. Sem logs, e impossível investigar um incidente.

Gestão de incidentes: Plano documentado para vazamentos — com obrigação de notificar a ANPD em até 72 horas.

Backup e recuperação: Garantia de que os dados podem ser restaurados mesmo apos falha ou ataque.

Política de Senhas — Padrão Mínimo Recomendado

Critério	Padrão Mínimo	Recomendado
Comprimento	8 caracteres	12+ caracteres
Complexidade	Letras e números	Letras, números e símbolos
Renovação	A cada 6 meses	A cada 3 meses
Reútilização	Não reútilizar 3 ultimas	Não reútilizar 12 ultimas
Autenticação	Simples	MFA obrigatório

Checklist — Segurança & LGPD

Marque o que seu escritório ja tem implementado:

CONTROLE DE ACESSO:

- ☐ Política de senhas documentada e em vigor
- ☐ MFA habilitado em todos os sistemas com dados de clientes
- ☐ Perfis de acessó por função (quem ve o que)
- ☐ Gestão de usuários — desativação imediata de ex-colaboradores
- ☐ Auditoria periódica de acessos ativos

DADOS E PRIVACIDADE (LGPD):

- ☐ Mapeamento dos dados pessoais tratados no escritório
- ☐ Política de privacidade atualizada e disponível a clientes
- ☐ Contrato com cláusula de confidencialidade de dados
- ☐ Plano de resposta a incidentes documentado
- ☐ Contato da ANPD identificado (notificação em até 72h)

SEGURANÇA TÉCNICA:

- ☐ Antivírus corporativo em todas as máquinas
- ☐ Sistemas operacionais e softwares atualizados automaticamente
- ☐ Criptografia ativa em dispositivos móveis e notebooks
- ☐ Wi-Fi corporativo separado do de visitantes
- ☐ VPN configurada para acessó remoto

CAPÍTULO 2

Backup Inteligente para Contábilidades

A regra 3-2-1 e como escolher entre backup local, nuvem ou hibrido.

02

A Regra 3-2-1 na Prática

A regra3-2-1 e o padrão da industria:**3 cópias** dos dados, em **2 mídias diferentes**, sendo **1 fora do local.**

3 Cópias	Original no servidor + backup local (NAS) + backup em nuvem
2 Mídias	Disco rígido ou NAS (local) + armazenamento em nuvem
1 Offsite	Sempre uma cópia fora do escritório — nuvem ou HD externo em outro endereço

Frequência de Backup por Tipo de Dado

Tipo de Dado	Frequência Ideal	Retenção Minima
SPED, ECF, EFD	Diário	5 anos (exigência legal)
Documentos de clientes	Diário	5 anos
Folha de pagamento	Diário	5 anos
E-mails profissionais	Semanal	2 anos
Banco de dados ERP	Diário (incremental) + Semanal (completo	5 anos
Configurações de sistemas	Semanal	1 ano

Lembre-se: ter backup não e suficiente, você precisa testar a restauração.

Recomendamos um teste de recuperação completo a cada 3 meses.
Um backup não testado pode ser inútil quando você mais precisar.

Por que Contábilidades são o Alvo Favorito

Escritórios contábeis combinamtres fatores que os tornam altamente atrativos: acesso a dados financeiros de centenas de empresas, infraestrutura de TI geralmente deficiente e alta disposição para pagar o resgate para recuperar dados de clientes.

Como o Ransomware Chega no Escritório:

65%	**Phishing (e-mail falso)** E-mail que imita Receita Federal, cliente ou banco — um clique e o escritório e infectado.
20%	**Acessó remoto sem segurança** RDP com senha fraca exposto na internet — invadido em minutos por scans automáticos.
8%	**Mídias removiveis** Pendrive infectado conectado a qualquer máquina propaga o virus para toda a rede.
7%	**Software desatualizado** Windows sem suporte ou ERP sem patch de segurança são portas abertas.

Antivírus Gratuito vs. Corporativo (Sophos)

Recurso	Antivírus Gratuito	Antivírus Corporativo
Proteção em tempo real	Básica	Avancada com IA
Anti-ransomware	Não ou limitado	Sim — com rollback automático
Gerenciamento central	Nao	Console único para todos os PCs
Resposta a incidentes	Nao	Alertas e isolamento automático
Custo	Gratis	A partir de R$ 45/dispositivo/mes
Adequado para contábilidade	NÃO	SIM

CAPÍTULO 3

Antivírus, Ransomware e Ameaças Reais

Como o ransomware chega no escritório contábil e como se proteger.

Segmentação de Rede — O Básico que Protege Muito

A maioria dos escritórios tem uma única rede Wi-Fi para funcionários e visitantes. Isso e um risco crítico: um dispositivo infectado de qualquer visita pode contaminar toda a rede interna, incluindo servidores e bancos de dados de clientes.

Rede Corporativa	Só funcionários e dispositivos gerenciados. Acessó a servidores, ERP e dados de clientes.
Rede de Visitantes	Clientes e prestadores — apenas internet, sem acessó a rede interna.
Rede de Gerenciamento	Impressoras, NAS, infraestrutura — acessível apenas por TI.

VPN para Home Office — Configuração Minima

Qualquer acessó remoto ao servidor deve ser feito por VPN, nunca por RDP diretamente exposto na internet:

- VPN com autenticação por certificado (não apenas senha)
- MFA obrigatório para conexão VPN
- Timeout automático de sessão inativa (máximo 30 minutos)
- Log de todas as conexões remotas
- Lista de IPs autorizados quando possível

Como Escolher um Parceiro de TI

Não existe "TI boa" feita por improviso. Escritórios contábeis precisam de um parceiro especializado, com SLA definido, experiência no setor e disponibilidade real, não de um "amigo que entende de computador".

O que deve constar no contrato de suporte:

SLA de atendimento: Tempo máximo para primeiro contato: 2h em horario comercial, 4h fora do horario para críticos.

Escopo definido: O que esta incluso: hardware, software, impressoras, celulares, cloud.

Backup monitorado: Confirmação diária de que o backup foi executado com sucesso.

Relatório mensal: Chamados, incidentes, status de equipamentos e recomendações.

Suporte remoto e presencial: Quando é remoto e quando o técnico vai ao escritório — com tempo de resposta claro.

Cláusula de confidencialidade: O prestador assina sigilo sobre os dados dos seus clientes.

Plano de Continuidade — 3 Etapas Essenciais

1. Identificar sistemas críticos	ERP, e-mail, acesso ao portal da Receita Federal, sistemas de folha. O que o escritório não pode ficar sem por mais de 1 hora?
2. Definir tempo máximo de inatividade	Para cada sistema crítico, qual e o impacto de ficar 1h, 4h, 1 dia sem acesso? Isso define a prioridade de recuperação.
3. Documentar o plano de recuperação	Quem liga para quem, o que verificar primeiro, como ativar o backup. Imprimir e manter fora do sistema digital.

CAPÍTULO 4

Redes, Wi-Fi e Acesso Remoto Seguro

Segmentação de rede, VPN e home office sem abrir portas para invasores.

Checklist Mestre — TI para Escritórios Contábeis

Use este checklist para avaliar sua infraestrutura atual.
Marque cada item e priorize oque esta faltando.

SEGURANÇA E LGPD:

- ■ Política de senhas documentada e em vigor
- ■ MFA habilitado em todos os sistemas com acessó a dados de clientes
- ■ Perfis de acessó por função definidos e revisados
- ■ Log de acessos ativado e revisado periódicamente
- ■ Plano de resposta a incidentes de segurança documentado
- ■ Mapeamento dos dados pessoais tratados (requisito LGPD)
- ■ Contrato de confidencialidade com todos colaboradores e prestadores

BACKUP:

- ■ Backup diário automatizado dos dados críticos (SPED, folha, contratos)
- ■ Cópia offsite — nuvem ou físico em outro endereço
- ■ Teste de restauração realizado nos últimos 3 meses
- ■ Retenção de pelo menos 5 anos para documentos fiscais
- ■ Alerta automático em casó de falha no backup

ANTIVÍRUS E ENDPOINT:

- ■ Antivírus corporativo (não gratuito) em todos os dispositivos
- ■ Atualizacoes automaticas de sistema operacional habilitadas
- ■ Política de usó de pendrives documentada
- ■ Filtro de e-mail com bloqueio de phishing ativo
- ■ Usuarios sem privilegio de administrador local

CAPÍTULO 5

Suporte, Continuidade e Plano B

Como escolher um parceiro de TI confiável e o que fazer quando tudo para.

Checklist Mestre — continuação

REDES E ACESSO REMOTO:

- ■ Rede Wi-Fi corporativa separada da rede de visitantes
- ■ Roteador corporativo com firewall ativo (não modem residencial)
- ■ VPN configurada para todos os acessos remotos
- ■ MFA obrigatório para conexão VPN
- ■ Inventário de todos os dispositivos conectados a rede

SUPORTE E CONTINUIDADE:

- ■ Contrato com fornecedor de TI com SLA definido
- ■ Documentacao de sistemas e senhas em local seguro (cofre de senhas)
- ■ Plano de continuidade básico documentado e impresso
- ■ Lista de contatos de emergencia (TI, provedor, software)
- ■ Inventário atualizado de hardware e licenças de software
- ■ Processó de offboarding — desativação imediata de acessos de ex-colaboradores

CLOUD E SISTEMAS ERP:

- ■ Acessó ao sistema contábil protegido por senha forte e MFA
- ■ Licenças de software regulares (sem versões piratas ou descontinuadas)
- ■ Contrato de suporte ativo com fornecedor do sistema contábil (ERP)
- ■ Política de atualização definida para sistemas críticos (ERP, SO, antivírus)

Como interpretar seu resultado:

Itens marcados	Situação	Próximo passo
28-32	EXCELENTE	Mantenha e revise anualmente
20-27	BOM	Foque nos itens de backup e acesso remoto primeiro
12-19	ATENÇÃO	Priorize segurança e backup imediatamente
Menos de 12	CRÍTICO	Busque suporte especializado com urgência

BÔNUS

Checklist Completo com 30+ Pontos

Avalie a infraestrutura do seu escritório agora.

TRINITY TI

GESTÃO INTEGRADA EM T.I.

Quer aplicar este guia no seu escritório?

Nossa equipe faz um diagnóstico gratuito da TI do seu escritório e apresenta um **Plano de Ação**.

WhatsApp: (21) 4062-7800

contato@trinityti.com

trinityti.com.br

Diagnóstico gratuito e sem compromisso

Resposta em até 24 horas úteis — Rio de Janeiro e todo o Brasil

Parceiros tecnológicos certificados:

Microsoft | Google Workspace | Sophos | MikroTik