trinity ti
GESTÃO INTEGRADA EM T.I.

E-BOOK GRATUITO · ÁREA DA SAÚDE

Guia de TI para Clínicas e Saúde: atendimento que não para, dados que não vazam

Como manter prontuário e agenda sempre no ar, proteger os dados dos pacientes, cumprir a LGPD e escolher o parceiro de TI certo — sem precisar entender de tecnologia.

- Continuidade do atendimento
- Segurança contra ransomware
- Suporte, SLA e contrato
- Backup e guarda do prontuário
- LGPD na prática da clínica
- Checklist com 36 pontos

trinityti.com · (21) 4062-7800

ANTES DE COMEÇAR

Sobre este guia

Clínicas, consultórios, laboratórios e centros de diagnóstico vivem de duas coisas: atender bem e guardar bem as informações de quem atendem. Hoje, as duas dependem da tecnologia.

Prontuário eletrônico, agenda online, faturamento de convênios, laudos, exames de imagem, prescrição digital, telemedicina e WhatsApp com pacientes: tudo passa pelos computadores, pela rede e pela internet da clínica. Quando algo falha, a recepção trava, o paciente espera e o faturamento atrasa. Quando um dado vaza, o problema deixa de ser técnico e passa a ser jurídico, financeiro e de reputação.

Mesmo assim, em muitas operações de saúde a TI ainda é tratada como um assunto secundário — resolvido pelo "técnico que aparece quando quebra". Este guia foi escrito pela Trinity TI para sócios, diretores clínicos e gestores administrativos que querem mudar isso com decisões simples, na ordem certa.

O que você vai encontrar aqui

- O cenário de risco da saúde e por que o setor é o alvo preferido dos criminosos;
- As seis dores de TI que mais atrapalham clínicas e consultórios;
- Cinco capítulos práticos: continuidade, backup, segurança, LGPD e suporte — cada um com um checklist rápido;
- Um checklist completo com 36 pontos para avaliar a sua operação ainda hoje.

Para quem é

Para quem administra ou responde por uma operação de saúde de pequeno ou médio porte — clínica médica ou multidisciplinar, odontologia, laboratório, imagem, fisioterapia, psicologia, estética ou hospital-dia — e quer reduzir riscos sem virar especialista em tecnologia.

> ***"Na saúde, TI não é bastidor. Quando o sistema para, o atendimento para junto."***

Este guia tem caráter informativo. Ele não substitui uma avaliação técnica do seu ambiente nem orientação jurídica. Normas e prazos citados estavam vigentes na data de edição (novembro de 2026).

O CENÁRIO

Por que a saúde é o alvo preferido

Dado de paciente vale muito para o crime: serve para golpes, fraudes em convênios e extorsão. E poucas operações têm tanta pressa para voltar a funcionar quanto uma clínica com a recepção cheia.

US$ 6,64 mi

custo médio de um vazamento na saúde

A saúde segue como o setor com o vazamento mais caro, segundo o relatório Cost of a Data Breach 2026, da IBM.

R$ 50 mi

teto da multa da LGPD por infração

Até 2% do faturamento, limitado a R$ 50 milhões por infração (Lei 13.709/2018, art. 52).

3 dias úteis

para comunicar um incidente

Prazo para avisar a ANPD e os titulares sobre incidentes que possam causar risco ou dano relevante (Resolução CD/ANPD nº 15/2024).

Dado de saúde é dado sensível

A LGPD classifica o dado referente à saúde como **dado pessoal sensível** (art. 5º, II) e dá a ele regras mais rígidas de tratamento (art. 11). Para a clínica, isso significa mais cuidado com quem acessa, onde os dados ficam, com quem são compartilhados e como são protegidos.

O prontuário precisa durar décadas

A Lei 13.787/2018 determina que o prontuário seja guardado por, no mínimo, **20 anos a partir do último registro**. Os conselhos profissionais (medicina, odontologia, psicologia, fisioterapia e outros) têm normas próprias sobre registro e guarda — vale confirmar a regra que se aplica à sua área. Em qualquer caso, a pergunta técnica é a mesma: os seus dados estarão íntegros e acessíveis daqui a muitos anos?

A operação depende de muitos sistemas

Prontuário, agenda, faturamento TISS, laudos, PACS, equipamentos de exame conectados à rede, certificado digital, prescrição eletrônica e telemedicina. Cada um deles é um ponto que pode parar — e uma porta que pode ser aberta.

> *"A pergunta não é se a clínica vai enfrentar um incidente de TI, mas quanto tempo levará para voltar a atender."*

O QUE VEMOS NO DIA A DIA

As 6 maiores dores de TI na saúde

1

Sistema fora do ar com paciente na recepção

Internet da operadora sem redundância, servidor antigo, falta de nobreak. Uma falha simples para a agenda, o prontuário e o faturamento — e a recepção passa o dia remarcando pelo WhatsApp.

2

Backup que ninguém testou

Existe uma rotina de cópia, mas ninguém sabe se ela restaura, quanto tempo leva ou se a cópia também seria criptografada num ataque. O problema só aparece no dia em que o backup é necessário.

3

Rede aberta e roteador da operadora

Wi-Fi de pacientes na mesma rede dos computadores, do prontuário e dos equipamentos de exame. Sem firewall corporativo, qualquer dispositivo infectado chega perto do que é mais sensível.

4

Senha compartilhada e acessos esquecidos

Um login único para a recepção, senhas anotadas em papel, ex-colaboradores que ainda acessam o e-mail ou o sistema. Não dá para saber quem fez o quê — e a LGPD exige esse controle.

5

LGPD só no papel

Um termo assinado na recepção não é adequação. Faltam o mapeamento dos dados, a política de acesso, o encarregado definido e um plano para quando algo der errado.

6

Suporte só quando quebra

Sem monitoramento, sem atualização preventiva, sem documentação. O problema é descoberto pelo paciente que está esperando — e cada visita técnica avulsa custa caro e resolve pouco.

CAPÍTULO 1

01 Continuidade do atendimento

O objetivo é simples: se algo falhar, a clínica continua atendendo — ou volta a atender no tempo que você decidiu antes, e não no tempo que o problema impuser.

Elimine os pontos únicos de falha

- **Internet:** dois links de operadoras diferentes (por exemplo, fibra + 4G/5G), com troca automática no firewall. Se o prontuário é na nuvem, a internet é o seu sistema.
- **Energia:** nobreak dimensionado para servidor, firewall, switches e os computadores da recepção — com tempo suficiente para um desligamento seguro.
- **Servidor:** servidor local precisa de garantia, discos redundantes e monitoramento.
- **Computadores:** padronizados, com uma máquina reserva pronta para uso.

Defina, por escrito, o tempo de retorno

Liste os sistemas da clínica e defina para cada um quanto tempo ele pode ficar fora do ar (RTO) e quanto dado é aceitável perder (RPO). Isso orienta o backup, a redundância e o investimento — e evita discussões no meio da crise.

Tenha um plano de contingência

O que a recepção faz se o sistema cair? Como confirmar a agenda e registrar o atendimento para lançar depois? Um plano de uma página, impresso e treinado, vale mais que um documento longo esquecido numa pasta.

Calcule o custo de um dia parado

Profissionais atendendo (A)	____
Atendimentos por profissional por dia (B)	____
Ticket médio por atendimento (C)	R$ ____
Receita em risco por dia parado (A × B × C)	R$ ____

Exemplo: 6 profissionais × 10 atendimentos × R$ 200 = R$ 12.000 por dia — sem contar retrabalho da recepção, glosas e o desgaste com o paciente.

Checklist rápido

- [ ] Temos link de internet reserva com troca automática.
- [ ] Servidor, rede e recepção estão no nobreak.
- [ ] Sabemos quanto tempo cada sistema pode ficar parado.
- [ ] A recepção sabe o que fazer se o sistema cair.

02 CAPÍTULO 2

Backup e proteção do prontuário

Backup não é ter uma cópia. É conseguir recuperar o que precisa, no tempo que precisa — inclusive depois de um ataque.

A regra 3-2-1 (e o "1" a mais)

3 · 2 · 1

Mantenha **3 cópias** dos dados, em **2 mídias** diferentes, com **1 cópia fora da clínica** (em nuvem ou em outro local).

+ 1 imutável

Pelo menos uma cópia precisa ser **imutável** ou desconectada: o ransomware procura e criptografa também os backups ligados à rede.

O que entra no backup

Não só o prontuário. Entram também agenda, financeiro, faturamento, laudos e imagens, documentos, planilhas, e-mails e as configurações dos sistemas. Se o prontuário é em nuvem, leia o contrato do fornecedor: ele protege a infraestrutura dele, mas o que acontece se um usuário apagar dados por engano, ou se o contrato for encerrado? Você consegue exportar tudo num formato legível?

Teste a restauração

Agende testes periódicos: restaure um prontuário, uma pasta e um sistema inteiro num ambiente separado e anote o tempo gasto. Guarde o registro — ele é a prova de que o backup funciona e uma evidência útil de boas práticas de segurança.

Pense em décadas

Prontuários precisam ser guardados por muitos anos. Defina a retenção de acordo com as regras da sua área, use formatos e mídias que continuarão legíveis e revise o plano quando trocar de sistema — a migração de prontuário é um dos momentos de maior risco de perda.

Criptografia e acesso ao backup

A cópia deve ser criptografada e o acesso a ela, restrito. Backup aberto é só mais um lugar de onde os dados podem vazar.

Checklist rápido

- [ ] Temos 3 cópias, em 2 mídias, com 1 fora da clínica.
- [ ] Pelo menos uma cópia é imutável ou desconectada.
- [ ] Testamos a restauração e registramos o resultado.
- [ ] Sabemos como exportar os dados do sistema de prontuário.

03 CAPÍTULO 3

Segurança cibernética na saúde

A maior parte dos ataques não é sofisticada: começa num e-mail, num link pelo WhatsApp ou numa senha fraca. Por isso, o básico bem feito protege muito.

Rede: separe o que é sensível

- Troque o roteador da operadora por um **firewall corporativo** (Sophos, Fortinet ou MikroTik, por exemplo), com filtro de conteúdo, inspeção de tráfego e registro de acessos.
- **Wi-Fi de pacientes** isolado, só com acesso à internet.
- **Equipamentos de exame e imagem** em uma rede própria: muitos rodam sistemas antigos que não podem ser atualizados com facilidade.

Computadores: proteção gerenciada

- Antivírus corporativo com EDR (detecção e resposta), administrado de forma centralizada — não o gratuito instalado em cada máquina.
- Atualizações do sistema e dos programas aplicadas com rotina e controle.
- Softwares licenciados: programa pirata é uma das portas de entrada mais comuns de vírus.

Identidade: cada um com o seu acesso

- Usuário individual para cada profissional, inclusive na recepção — nada de senha compartilhada.
- **Verificação em duas etapas (MFA)** no e-mail, na nuvem e nos sistemas que permitirem.
- Permissões por função e acessos revogados no mesmo dia em que alguém sai.
- Certificados digitais (ICP-Brasil) guardados com cuidado: eles assinam prescrições e documentos em nome do profissional.

Pessoas: a última linha de defesa

Treine a equipe para desconfiar de e-mails com boletos, links de "atualização de cadastro", mensagens urgentes pelo WhatsApp e pedidos de código por telefone. Use números de WhatsApp da clínica em aparelhos gerenciados, e não no celular pessoal de cada colaborador.

Checklist rápido

- [ ] Temos firewall corporativo e Wi-Fi de pacientes isolado.
- [ ] Antivírus gerenciado em todas as máquinas.
- [ ] MFA ativo no e-mail e na nuvem.
- [ ] A equipe recebeu treinamento contra golpes neste ano.

CAPÍTULO 4

04 LGPD na prática da clínica

A LGPD não pede perfeição: pede que a clínica saiba quais dados trata, por que trata, quem acessa e como protege — e que consiga demonstrar isso.

Os passos essenciais

- **Mapeie os dados:** onde estão os dados de pacientes (prontuário, agenda, planilhas, e-mail, WhatsApp, papel), quem acessa e com quem são compartilhados (convênios, laboratórios, contabilidade, fornecedores de sistema).
- **Identifique a base legal:** o atendimento de saúde tem hipótese própria na LGPD (art. 11, II, "f" — tutela da saúde, em procedimento realizado por profissionais ou serviços de saúde). Já ações de marketing com dados de pacientes exigem outra base, normalmente o consentimento.
- **Indique um encarregado (DPO):** a pessoa ou empresa que responde pelos dados perante pacientes e a ANPD.
- **Publique o aviso de privacidade** e tenha um canal para os pacientes exercerem seus direitos (acesso, correção, informações sobre compartilhamento).
- **Revise contratos com fornecedores** que tratam dados por você — sistema de prontuário, laboratório de apoio, nuvem, TI.
- **Adote medidas de segurança** — os capítulos 2 e 3 deste guia são a parte técnica da LGPD.

E se acontecer um incidente?

Pela Resolução CD/ANPD nº 15/2024, incidentes que possam causar risco ou dano relevante aos titulares devem ser comunicados à ANPD e aos titulares em até **3 dias úteis**. Na prática, a clínica precisa saber, com antecedência: quem decide, quem investiga, quem comunica e como registrar o que aconteceu. Sem um plano, esse prazo passa enquanto a equipe ainda está tentando entender o problema.

Divida bem as responsabilidades

A adequação tem uma parte jurídica (bases legais, contratos, avisos, atendimento aos titulares) e uma parte técnica (controle de acesso, backup, segurança, registros). As duas precisam conversar. A Trinity cuida da parte técnica e trabalha em conjunto com o jurídico da clínica.

Checklist rápido

- [ ] Sabemos onde estão os dados de pacientes.
- [ ] Temos encarregado (DPO) definido e aviso de privacidade.
- [ ] Contratos com fornecedores tratam de proteção de dados.
- [ ] Temos plano de resposta a incidentes com o prazo da ANPD.

05 CAPÍTULO 5

Suporte, SLA e o parceiro de TI certo

A diferença entre um técnico avulso e uma gestão de TI está em uma palavra: prevenção. O bom parceiro descobre o problema antes do paciente.

Avulso × gerenciado

Suporte avulso

- Chamado só quando quebra
- Sem monitoramento
- Sem documentação do ambiente
- Custo imprevisível

Gestão de TI (MSP)

- Monitoramento 24/7 e alertas
- Manutenção preventiva
- Ambiente documentado
- Mensalidade e SLA definidos

O que exigir no contrato

- **Escopo claro:** o que está incluído (computadores, servidor, rede, backup, e-mail, segurança) e o que é cobrado à parte.
- **SLA por escrito:** tempo de resposta e de solução por prioridade — um computador da recepção parado não pode esperar como uma dúvida simples.
- **Atendimento presencial:** quando ele acontece e em que regiões.
- **Relatórios periódicos:** chamados, backups, alertas de segurança e recomendações.
- **Documentação e saída:** senhas, inventário e diagramas pertencem à clínica e são entregues se o contrato acabar.
- **Proteção de dados:** cláusulas de confidencialidade e LGPD, já que o parceiro de TI acessa o seu ambiente.

Perguntas para fazer antes de contratar

- Vocês já atendem outras operações de saúde? Como lidam com o fornecedor do sistema de prontuário?
- Como é feito e testado o backup? Com que frequência recebo o resultado?
- O que acontece numa sexta-feira à noite se o servidor parar?

Checklist rápido

- [ ] Temos contrato com escopo e SLA por escrito.
- [ ] Recebemos relatórios periódicos do ambiente.
- [ ] A documentação da TI está com a clínica.

BÔNUS

Checklist completo: 36 pontos

Marque o que a sua clínica já tem. No fim, some os itens marcados e veja onde você está.

Continuidade 6

- [ ] Link de internet reserva, de outra operadora
- [ ] Troca automática de link no firewall
- [ ] Nobreak para servidor, rede e recepção
- [ ] Tempo de retorno definido para cada sistema
- [ ] Plano de contingência impresso e treinado
- [ ] Computador reserva pronto para uso

Backup 6

- [ ] Backup automático diário
- [ ] 3 cópias, 2 mídias, 1 fora da clínica
- [ ] Uma cópia imutável ou desconectada
- [ ] Backup criptografado e com acesso restrito
- [ ] Teste de restauração registrado
- [ ] Retenção alinhada à guarda do prontuário

Rede e equipamentos 6

- [ ] Firewall corporativo (não o roteador da operadora)
- [ ] Wi-Fi de pacientes isolado
- [ ] Equipamentos de exame em rede própria
- [ ] Inventário de computadores e equipamentos
- [ ] Sem portas de acesso remoto abertas na internet
- [ ] Acesso remoto só por VPN ou ferramenta gerenciada

Computadores e acessos 6

- [ ] Antivírus corporativo com EDR gerenciado
- [ ] Atualizações aplicadas com rotina
- [ ] Softwares 100% licenciados
- [ ] Login individual para cada profissional
- [ ] MFA no e-mail e na nuvem
- [ ] Acessos revogados no dia do desligamento

LGPD 6

- [ ] Dados de pacientes mapeados
- [ ] Encarregado (DPO) definido
- [ ] Aviso de privacidade publicado
- [ ] Contratos com fornecedores revisados
- [ ] Canal para pedidos dos pacientes
- [ ] Plano de incidentes com prazo da ANPD

Pessoas e suporte 6

- [ ] Treinamento anual contra golpes e phishing
- [ ] WhatsApp da clínica em aparelho gerenciado
- [ ] Política de uso de e-mail, celular e senhas
- [ ] Monitoramento 24/7 do ambiente
- [ ] Contrato de TI com escopo e SLA
- [ ] Documentação da TI em poder da clínica

SEU RESULTADO

Quantos itens você marcou?

30 a 36
Boa base. Mantenha a rotina de testes e revise o ambiente pelo menos uma vez por ano.

18 a 29
Atenção. Há lacunas importantes — comece pelo backup, pelos acessos e pela rede de pacientes.

0 a 17
Risco alto. Um único incidente pode parar o atendimento e expor dados. Priorize agora.

Como a Trinity TI apoia operações de saúde

Há mais de 20 anos a Trinity TI faz a gestão integrada de TI de empresas que não podem parar. Na saúde, assumimos a operação de tecnologia para que a clínica se dedique ao paciente:

- **Continuidade:** link redundante, nobreak, servidor e nuvem dimensionados e plano de contingência.
- **Backup 3-2-1** com cópia imutável e testes de restauração documentados.
- **Segurança:** firewall Sophos, Fortinet ou MikroTik, antivírus com EDR, Wi-Fi segregado e MFA.
- **LGPD técnica:** controle de acessos, registros, plano de resposta a incidentes e treinamento da equipe.
- **Monitoramento 24/7 e suporte** nos planos Remoto ou Remoto + Presencial, com atendimento presencial em todo o Estado do Rio de Janeiro.

+20
anos de mercado

+1.500
clientes atendidos

+1.500
dispositivos monitorados

1h
tempo médio de resposta no suporte remoto

Parceiros e tecnologias: Microsoft, Microsoft 365, Azure, Google Workspace, Linux/Proxmox, Sophos, Fortinet, MikroTik, HP/Aruba e Cisco.

PRÓXIMO PASSO

Quer saber exatamente onde a sua clínica está?

Este guia mostra o caminho. O diagnóstico mostra o seu ponto de partida.

Diagnóstico gratuito com um especialista Trinity

Avaliamos rede, backup, segurança, acessos e os pontos de atenção da LGPD da sua operação e entregamos, por escrito, as prioridades e o que dá para resolver em 30, 60 e 90 dias. Sem compromisso.

Solicitar meu diagnóstico →

Prefere começar sozinho? Faça o Raio-X de TI & LGPD em 2 minutos e receba o relatório na hora.

Fale com a Trinity TI

Telefone e WhatsApp: (21) 4062-7800

E-mail: contato@trinityti.com

Site: www.trinityti.com

Endereço: Av. Rio Branco, 151 — Centro, Rio de Janeiro/RJ

Atendimento: seg. a sex. · 8h às 18h

trinity ti
GESTÃO INTEGRADA EM T.I.

© 2026 Trinity TI
Trinity TI Soluções Tecnológicas de Informática Ltda.