O Método da Proteção Inteligente

Como proteger os dados da sua empresa e evitar multas com a LGPD, mesmo sem ter um time de TI

Tumim7

SEGURANÇA, TECNOLOGIA E PRIVACIDADE

2025

Introdução

Imagine receber uma ligação do seu cliente mais importante dizendo que os dados dele vazaram... e isso porque sua empresa não tinha nenhuma política de proteção implantada. Parece distante? Em 2024, 2.766 ataques cibernéticos aconteceram por semana no Brasil. E sim, a maioria em pequenas e médias empresas.

> *"Este e-book é um manual prático para quem deseja proteger sua empresa, conquistar a confiança dos clientes e evitar multas pesadas, mesmo sem ser especialista técnico."*
>
> — Tumim7

Capitulo 1:

Por que segurança da informação não é mais opcional?

Segundo o Global Risks Report 2025, do Fórum Econômico Mundial, os ataques cibernéticos estão entre os 10 maiores riscos globais, ao lado de desastres climáticos e crises econômicas. No Brasil, a situação é ainda mais crítica: entre julho e setembro de 2024, o país registrou um aumento de 95% nos ataques cibernéticos, com 2.766 ataques por semana em média.

Imagine receber um e-mail informando que todos os dados dos seus clientes foram expostos. Nome, CPF, endereço, número de cartão de crédito — tudo vazado.

Isso aconteceu com milhares de empresas brasileiras só no último ano. E o mais assustador? A maioria delas eram pequenas ou médias, como a sua.

E não pense que isso é coisa de filme ou que só acontece com grandes corporações.

Pelo contrário. O que os criminosos descobriram é que pequenas empresas geralmente não têm proteção adequada – e por isso são alvos fáceis.

Por que isso está acontece?

Vivemos em um mundo cada vez mais digital. E onde há dados, há valor.

- Dados de clientes
- Registros financeiros
- E-mails, senhas e documentos confidenciais

Todos esses dados são como ouro para cibercriminosos. E não é só sobre roubo. É também sobre danos à reputação, multas e perda de confiança dos seus clientes.

O custo de não agir:

Uma pizzaria foi multada em R$ 10 mil por armazenar dados sem consentimento.

Um consultório odontológico perdeu mais de R$ 20 mil após ter seu sistema invadido e os dados dos pacientes criptografados.

Um pequeno e-commerce ficou 4 dias fora do ar após um ataque de ransomware – e perdeu mais de 60% dos seus pedidos do mês.

Mini exercício:

Faça uma rápida autoavaliação

Sua empresa coleta dados dos clientes? (Ex.: nome, telefone, e-mail, CPF?).

Esses dados estão armazenados com segurança? (Planilhas, sistemas, backups, senhas fortes?)

Você já pensou no que faria se esses dados vazassem amanhã? Se você respondeu “não” ou “não sei” para alguma dessas perguntas, você está vulnerável.

> *Segurança da informação não é mais um “luxo” ou “coisa de empresa grande”. É uma questão de sobrevivência.*
>
> — Tumim7

Capitulo 2:

Entendendo a LGPD em 5 Minutos.

Você já preencheu um formulário online e ficou se perguntando: “Pra que tudo isso?”

Pois é... agora imagine seus clientes pensando o mesmo quando sua empresa pede nome, CPF, e-mail, telefone e outras informações.

Foi por isso que surgiu a LGPD – Lei Geral de Proteção de Dados. Criada para proteger o direito das pessoas à privacidade, a LGPD entrou em vigor no Brasil para garantir que os dados pessoais sejam coletados, armazenados e utilizados com responsabilidade.

O que é a LGPD, na prática? A LGPD obriga qualquer empresa – seja grande ou pequena – a cuidar dos dados pessoais como se fossem um tesouro confidencial.

Isso inclui:

- Coletar dados com consentimento Armazenar com segurança
- Usar os dados de forma clara e legal
- Excluir quando não forem mais necessários
- Informar o cliente sobre o uso dos dados

Dados pessoais são todas as informações que permitem identificar uma pessoa, como:

- Nome completo
- CPF ou RG
- E-mail
- Telefone
- Endereço
- Placa de veículo
- Dados bancários
- IP de acesso à internet

O que acontece com quem ignora a LGPD?

Empresas que descumprem a lei podem sofrer:

- Multas de até R$ 50 milhões por infração
- Proibição de usar os dados coletados
- Danificação da reputação com clientes e parceiros
- Perda de negócios e ações judiciais

Exemplo real:

Uma clínica estética foi notificada por enviar promoções via WhatsApp sem autorização dos clientes. Resultado? Teve que pagar multa, apagar todos os dados e ainda precisou contratar uma consultoria para ajustar seus processos.

Checklist: Você está respeitando a LGPD?

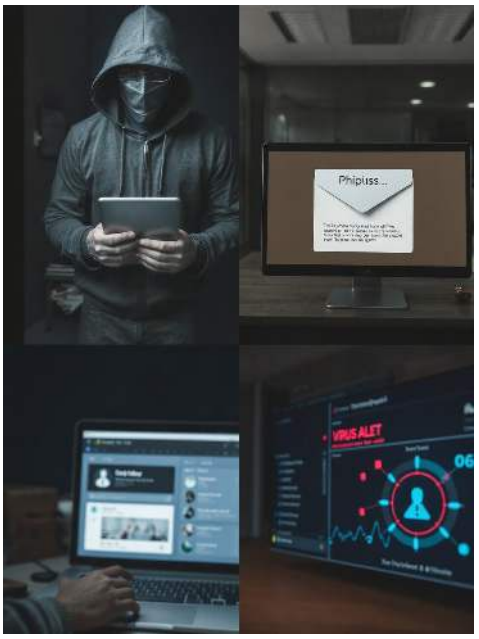
- Você informa aos clientes por que está coletando os dados?
- Os dados coletados são realmente necessários?
- Você tem consentimento dos clientes?
- Consegue excluir os dados caso o cliente peça?
- Tem alguém responsável por cuidar disso dentro da empresa?

A LGPD não veio para complicar sua vida. Veio para proteger a confiança entre você e seus clientes. E empresas que respeitam a privacidade saem na frente.

> *A LGPD não veio para complicar sua vida. Veio para proteger a confiança entre você e seus clientes. E empresas que respeitam a privacidade saem na frente.*
>
> — Tumim7

Capitulo 3:

As 4 principais ameaças que atacam sua empresa.



Você pode ter os melhores produtos, o melhor atendimento e uma equipe dedicada. Mas se a segurança digital da sua empresa tiver brechas, basta um clique errado para tudo desmoronar.

Hoje, os ataques virtuais são mais silenciosos, sofisticados e perigosos do que nunca. E adivinha? O elo mais fraco ainda é o ser humano.

As 4 ameaças mais comuns e como elas entram na sua empresa:

1) Phishing

O golpe do “e-mail falso” que parece verdadeiro. Você já recebeu um e-mail com um boleto suspeito, ou uma mensagem dizendo que precisa “atualizar sua senha urgente”?

Esse é o **phishing** — uma técnica usada para enganar seus funcionários e fazê-los clicar em links maliciosos que roubam senhas, acessam sistemas ou instalam vírus.

Exemplo real: Um colaborador clicou em um link achando que era do banco. Em segundos, hackers conseguiram acesso ao sistema financeiro da empresa e desviaram R$ 12 mil.

2) Ransomware

O sequestro de dados com pedido de resgate. Esse tipo de ataque bloqueia todos os arquivos da empresa e exige um pagamento (geralmente em criptomoedas) para liberar os dados. Empresas que não possuem backup atualizado ficam de mãos atadas.

E mesmo pagando, não há garantia de recuperação. Impacto comum: dias (ou semanas) parados, perda de clientes e processos judiciais.

3) Vazamento de Dados

Informações sensíveis que escapam pelas frestas. Pode ser um pendrive perdido, um e-mail enviado para o destinatário errado ou até um ex-funcionário que levou informações quando saiu. Consequência: quebra de confiança, dano à reputação e multas com base na LGPD.

4) Roubo de Senhas

Quando a senha da empresa é "*123456*"... Muitas empresas ainda usam senhas fracas, repetidas ou compartilhadas entre funcionários. Hackers usam softwares que testam milhares de combinações por um longo tempo até acertar. Dica prática: Use autenticação em dois fatores e senhas geradas por ferramentas específicas para geração de senhas complexas.

Reflexão: Pense rápido...

Você sabe quem tem acesso aos sistemas da sua empresa? Seus funcionários sabem identificar um e-mail de phishing? Existe um backup automatizado dos dados mais importantes? Se você hesitou em responder qualquer uma dessas perguntas... **É hora de agir.**

> *A maioria dos ataques não acontece por falhas técnicas. Acontece por falta de preparo das pessoas. E você pode mudar isso agora mesmo com medidas simples e estratégicas.*
>
> — Tumim7

Capitulo 4:

5 Ações que você pode aplicar hoje

Proteger sua empresa contra ataques virtuais e estar em conformidade com a LGPD não exige fórmulas mágicas nem investimentos astronômicos. Com pequenas mudanças no dia a dia, é possível dar um salto enorme em segurança.

É aqui que entra o *"Método da Proteção Inteligente"*, um modelo de 5 passos simples, práticos e eficazes — criados para empresas como a sua, que precisam de segurança sem complicação.

1) Use senhas fortes e ative a autenticação em dois fatores.

Evite senhas como "123456" e "Senha123", datas de nascimento, nomes simples. Prefira: Geradores de senhas automáticas + apps de cofres de senha.

Ação extra: Ative a autenticação em dois fatores (2FA) em e-mails, sistemas de gestão, bancos e redes sociais da empresa. Ferramentas úteis: Bitwarden, LastPass, Google Authenticator

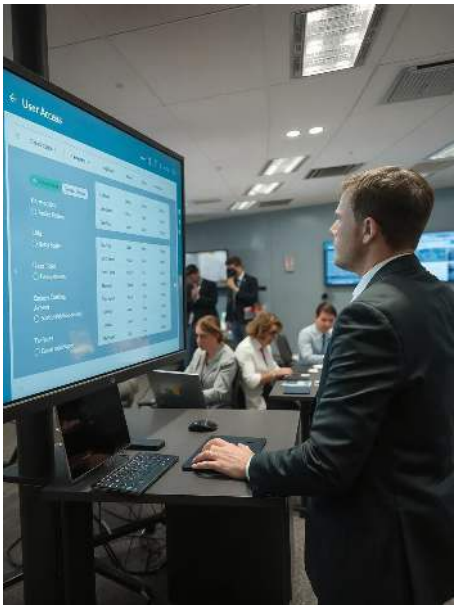
2) Atualize seus sistemas com frequência.

Sistemas desatualizados são portas abertas para ataques Mantenha Windows, antivírus, navegadores, plugins e sistemas internos sempre com as atualizações em dia Ative a opção de atualização automática sempre que possível.

Dica: A maioria dos vírus explora falhas já conhecidas — que são corrigidas por atualizações simples!

3) Controle quem acessa o quê.

Defina níveis de acesso: nem todo colaborador precisa acessar tudo Crie usuários individuais em vez de “compartilhar logins” Registre acessos, logins e tentativas suspeitas.



Acesso consciente = menos riscos + mais controle

4) Treine sua equipe, mmesmo que seja pequena.

Promova reuniões curtas de conscientização (30 min) Ensine a reconhecer golpes, e-mails suspeitos e comportamentos de risco. Faça testes periódicos com simulações de phishing.

Exemplo: Envie um e-mail falso de teste e veja quem clica — depois, use isso como aprendizado para todos.

5) Faça backup regularmente e fora da empresa.

Estabeleça um cronograma automático de backup Guarde cópias em nuvem e/ou em um HD externo offline Teste a restauração dos arquivos com frequência.

Lembre-se: Backup não é só salvar — é garantir que você consegue recuperar.

Checklist: Já aplicou esses 5 passos?

- Senhas fortes + autenticação 2FA
- Atualização automáticas ativadas
- Controle de acessos implantados
- Treinamento de equipe iniciado
- Backup automático e seguro ativo

Identifique acima se já ativou esses 5 itens e onde você precisa agir ***hoje mesmo.***

Grandes mudanças começam com pequenas ações. Com o "Método da Proteção Inteligente", sua empresa pode sair da zona de risco com decisões simples, práticas e inteligentes.

— Tumim7

Capitulo 5:

LGPD na Prática – Como se adequar mesmo sem um jurídico interno

Quando falamos de LGPD, muita gente pensa logo em processos complexos, termos jurídicos complicados e altos custos com advogados.

Mas a verdade é que você pode começar a adequação com passos simples, organizados e estratégicos, mesmo sem um time jurídico dedicado.

Vamos te mostrar agora um roteiro prático de como colocar a LGPD em ação na sua empresa usando o que chamamos de Plano de Adequação Essencial:

Etapa 1: Mapeie os dados pessoais que sua empresa coleta.

Pergunte-se:

• Quais dados você coleta dos seus clientes, colaboradores e parceiros?
• Onde esses dados ficam armazenados? (e-mail, planilha, software, papel)
• Para que você está coletando esses dados?
• Crie uma planilha com as colunas: Tipo de dados, finalidade, onde está salvo e quem tem acesso.

Etapa 2: Faça um diagnóstico de riscos.

Identifique possíveis pontos de vazamento (ex: dados salvos em pendrive, computadores compartilhados, arquivos sem senha) Liste quais medidas de segurança já estão sendo aplicadas e quais ainda precisam ser implantadas.

Dica: Olhe com cuidado para o que está “espalhado” fora do controle da empresa — é aí que moram os maiores riscos.

Etapa 3: Crie ou revise sua política de privacidade.

Escreva de forma clara como sua empresa coleta, usa, armazena e protege os dados.
Publique isso em seu site, redes sociais ou comunicações com o cliente.
Garanta que todos os colaboradores conheçam essa política

Exemplo simples: "Coletamos dados apenas para prestação de serviços contratados. Armazenamos em ambiente seguro e não compartilhamos com terceiros sem autorização."

Etapa 4: Tenha um plano de resposta a incidentes.

E se um dado vazar? Quem será acionado? O que você fará? Crie um roteiro de ação emergencial:

- Identificar o incidente Isolar o problema.
- Notificar envolvidos.
- Corrigir falha.
- Documentar tudo

Ter um plano pronto evita pânico e reduz prejuízos.

Etapa 5: Nomeie um Encarregado de Dados (mesmo terceirizado)

Esse é o famoso DPO (Data Protection Officer) — alguém responsável por garantir que sua empresa siga a LGPD. Se você não tem alguém interno com esse perfil, pode contratar um modelo chamado DPO as a Service, com profissionais especializados que cuidam disso de forma terceirizada e acessível.

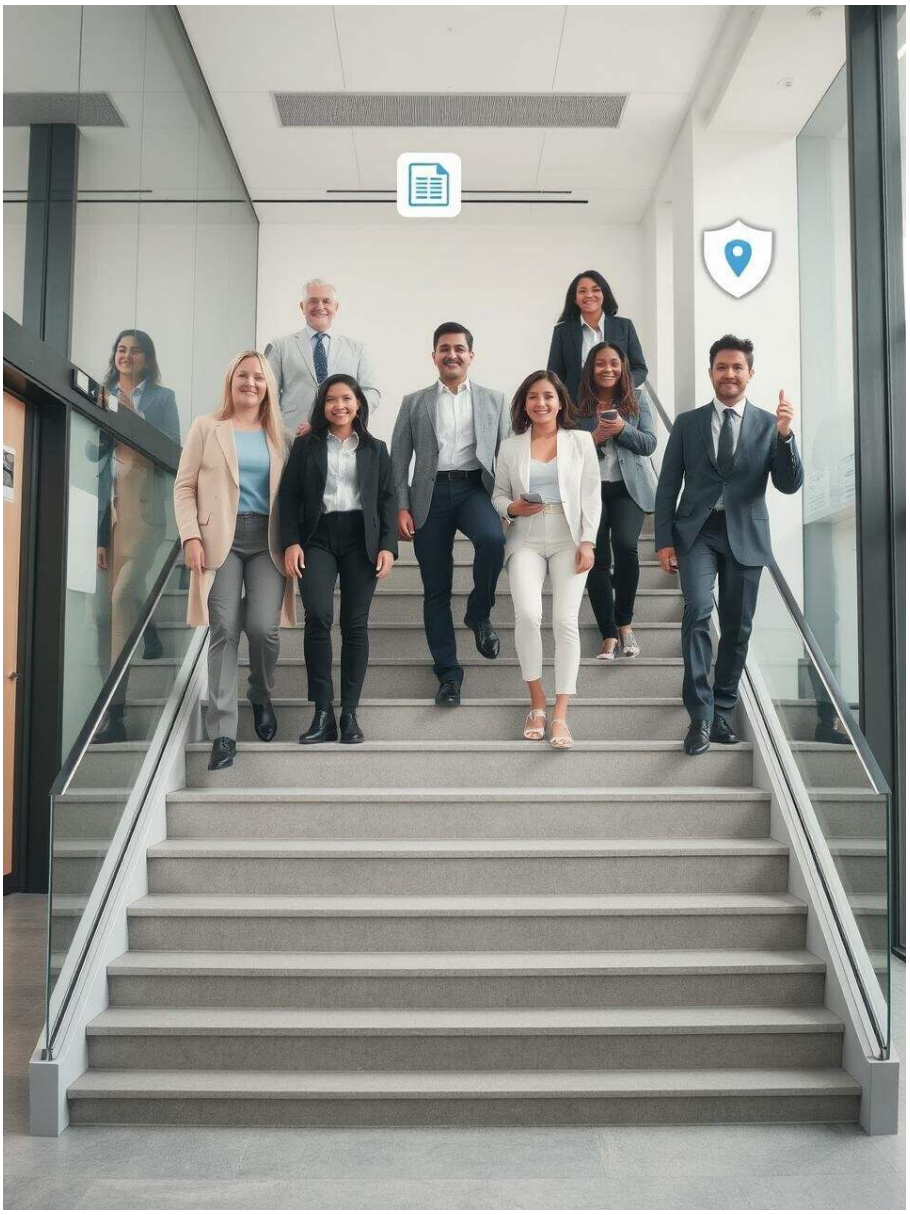
Desafio!

Pegue uma folha de papel (ou abra um doc) e responda:

- Você sabe exatamente quais dados pessoais sua empresa coleta?
- Sabe onde estão salvos esses dados?
- Tem uma política de privacidade publicada?
- Tem um plano de resposta a incidentes montado?
- Já definiu quem é o responsável pelos dados na sua empresa?

Se você respondeu "não" para 2 ou mais perguntas, já sabe o que precisa fazer. E o melhor: você não precisa fazer isso sozinho.

> *A adequação à LGPD é como um passo a passo. E quanto antes você começar, mais simples (e barata) será sua jornada de conformidade.*
>
> — Tumim7



Capitulo 6:

Benefícios de estar em conformidade

Muita gente enxerga a LGPD e a segurança da informação como um “mal necessário”. Mas quem muda esse olhar, descobre algo valioso: proteger os dados e seguir a lei pode se tornar uma vantagem real no mercado.

Sim, estar em conformidade pode ser um argumento de vendas. Pode ser o que vai fazer um cliente escolher você — e não o concorrente.

Desta forma, sabendo da importância da proteção de dados para qualquer negócio, atente-se as recomendações a seguir. Se algo lhe passou despercebído, volte a este e-book sempre que setnir necessidade, revise, estude e torne a sua empresa segura, dentro das normas da legislação.

1) Evita multas e sanções da ANPD

A **Autoridade Nacional de Proteção de Dados (ANPD)** já está fiscalizando empresas de todos os portes. E quando encontra irregularidades, pode aplicar sanções como:

- Advertência pública (sua reputação vai pro chão),
- Multas que podem chegar a 2% do faturamento anual, limitadas a R$ 50 milhões por infração,
- Suspensão do uso de dados (o que paralisa muitos negócios)

Estar em conformidade é o melhor seguro contra prejuízos legais e financeiros.

2) Aumenta a confiança dos clientes

Hoje, os consumidores estão mais atentos. Eles querem saber como seus dados estão sendo usados, com quem estão sendo compartilhados e se estão seguros. Quando sua empresa mostra transparência e responsabilidade, você:

- Ganha a confiança do cliente
- Se diferencia dos concorrentes
- Cria relacionamentos mais duradouros

Exemplo real: Uma clínica médica colocou no site sua política de privacidade clara e passou a receber elogios dos pacientes, que se sentiam mais seguros em compartilhar informações.

3) Diferencial competitivo no mercado

Empresas que seguem boas práticas de proteção de dados t**êm mais chances em licitações, parcerias e contratos com grandes players.**

Muitas empresas só fecham parcerias com quem prova que está em conformidade com a LGPD.

Exemplo: Um escritório de contabilidade fechou um contrato com uma empresa multinacional porque já tinha política de segurança implantada e DPO nomeado.

4) Redução de riscos operacionais e cibernéticos

Estar em conformidade geralmente vem acompanhado de:

- Melhor controle dos acessos
- Processos mais organizados
- Backups automatizados
- Equipe mais consciente e treinada

O resultado? Menos vulnerabilidades, menos sustos, mais segurança para crescer.

Exercício prático

Liste agora **3 benefícios** que sua empresa pode conquistar ao mostrar que está em conformidade com a LGPD:

Guarde isso. Use nas suas apresentações, nos seus argumentos de venda, no seu site. Você está criando uma vantagem real e mensurável.

> *Conformidade não é só prevenção. É também uma poderosa estratégia de posicionamento e crescimento.*
>
> — Tumim7

Capitulo 7:

Soluções e Serviços: Proteja e fortaleça sua empresa com apoio especializado

Você já entendeu os riscos, as oportunidades e os benefícios de proteger os dados da sua empresa.

Mas agora vem a pergunta que não quer calar:

Por onde eu começo?

A resposta é simples: você não precisa fazer isso sozinho. A **TUMIM7** oferece soluções sob medida para empresas que desejam segurança, conformidade e crescimento sustentável.

Conheça agora os principais serviços e escolha o que faz mais sentido para o momento da sua empresa:

1) Consultoria em Cibersegurança

Estratégia, análise e implementação completa de boas práticas de segurança da informação com base na ISO 27001.

Ideal para empresas que: Não têm um setor de TI estruturado. Precisam mapear riscos e definir prioridades. Querem proteger seus ativos digitais com metodologia internacional.

2) Testes de invasão (Pentest)

Simulação controlada de ataques para descobrir falhas antes que os hackers descubram.

Ideal para: Identificar vulnerabilidades reais em sites, sistemas e redes. Validar a segurança de plataformas digitais. Tomar decisões com base em evidências técnicas.

3) Testes de Vulnerabilidades Web

Avaliação profunda de sites, portais e aplicações para encontrar e corrigir falhas de segurança digital. Relatórios claros e ações corretivas.

4) Análise Forense Digital

Investigação técnica de incidentes de segurança, com coleta de evidências digitais e reconstrução dos fatos.

Ideal para: Há suspeita de vazamento, fraude ou acesso indevido. Você precisa comprovar fatos com dados técnicos

5) Plano Gestor de TI

Criação de uma estrutura tecnológica organizada, eficiente e segura, alinhada aos objetivos de crescimento da empresa.

Inclui: Diagnóstico de sistemas Planejamento estratégico de tecnologia Apoio na tomada de decisões.

6) CISO Virtual (Chief Information Security Officer)

Um profissional sênior de segurança da informação cuidando da sua empresa de forma remota, estratégica e acessível.

Ideal para empresas que: Não podem contratar um CISO em tempo integral. Precisam de orientação de alto nível. Buscam proteção contínua com custo reduzido.

7) DPO as a Service

Nomeação e gestão completa do Encarregado de Dados exigido pela LGPD.

Ideal para empresas que: Não podem contratar um CISO em tempo integral. Precisam de orientação de alto nível. Buscam proteção contínua com custo reduzido.

8) Treinamento e Capacitação

Programas de conscientização e boas práticas em segurança da informação e LGPD para equipes, gestores e parceiros.

Modalidades: Presencial ou online. Oficinas práticas ou treinamentos contínuos. Certificados de participação.

Benefício extra:

Ao contratar qualquer solução, você conta com o know-how de profissionais com mais de 20 anos de experiência, reconhecidos por certificações como:

- ISO 27001 Data Protection Officer (DPO)
- CISM (Certified Information Security Manager)
- MBA em Estratégia de Negócios e Gestão de TI

> *Você não precisa entender tudo sobre segurança e LGPD. Você só precisa das pessoas certas ao seu lado.*
>
> — Tumim7

Capitulo 8:

Conclusão: Está na hora de agir

Se você chegou até aqui, já deu o passo mais importante: se informar, entender os riscos e enxergar as oportunidades que vêm com a proteção de dados e a conformidade com a LGPD.

Agora, você já sabe que:

✅ Toda empresa, independentemente do porte, está vulnerável a ataques
✅ A LGPD não é um bicho de sete cabeças — e sim uma aliada da sua reputação
✅ Medidas simples já fazem uma enorme diferença na sua segurança
✅ Conformidade pode (e deve) ser um diferencial competitivo
✅ Não precisa fazer tudo sozinho: existem soluções acessíveis e estratégicas ao seu alcance

E agora te pergunto:

Sua empresa está realmente protegida?
Se um incidente acontecer amanhã, você está preparado?

Se você sentiu que ainda há lacunas, não se preocupe. **A maioria das empresas está exatamente nesse ponto** — e é por isso que nós estamos aqui para te ajudar.

Próximo passo: AÇÃO!

Se você quer:

- Evitar multas e penalidades.
- Ganhar a confiança dos seus clientes.
- Tornar sua empresa mais segura, moderna e valorizada no mercado.

Então o próximo passo é simples:

Agende uma conversa gratuita com nosso time de especialistas.

Agende uma conversa gratuita
com nosso time de especialistas.
www.tumim7.com.br

+55 (41) 99529-3672

Você vai receber:

✅ Um diagnóstico inicial personalizado
✅ Recomendações práticas para começar sua adequação ou fortalecimento da segurança
✅ Orientação sobre os serviços que melhor se encaixam na realidade da sua empresa

Sem pressão. Sem complicação. Só orientação clara e profissional.

> *Segurança da informação e privacidade de dados não são mais opcionais. São a nova base de confiança entre empresas e clientes. E você está a um passo de transformar isso em um diferencial competitivo poderoso.*
>
> — Tumim7

A decisão está nas suas mãos. Proteja sua empresa hoje para crescer com segurança amanhã.

Tumim7 – Segurança, Tecnologia e Privacidade

Rua XV de Novembro, 964 3º andar – Conj. 30 Centro 80060-000 - Curitiba-Paraná

+55 (41) 99529-3672 - contato@tumim7.com.br - www.tumim7.com.br