Penso

BUDGET 2026

ENFRENTANDO OS DESAFIOS ATUAIS

Um guia definitivo para convencer C-Levels com estratégias urgentes para blindar seu negócio contra os novos riscos.

- CYBERCRIME E INTELIGÊNCIA ARTIFICIAL
- SOBERANIA DE DADOS
- CONTINUIDADE DE NEGÓCIOS

Apoio: veeam Adistec

Introdução

Ao final de 2025, o cenário digital enfrentou desafios críticos: o cybercrime gerou perdas de US$10,5 trilhões globais, com projeções de US$13 trilhões até 2028, segundo relatórios da indústria. Soberania de dados tornou-se uma ferramenta geopolítica, bloqueando acessos sem aviso, enquanto interrupções de sistemas eliminam faturamento em minutos.

Criado pela Penso Tecnologia a partir do webinar realizado em 15 de outubro de 2025, ministrado por Thiago Lima - CEO da Penso, este e-book é seu **guia estratégico para convencer os C-Levels a priorizar cybersegurança** e soberania de dados no orçamento do próximo ano.

Nas próximas páginas você irá explorar casos reais, números impactantes e táticas para conquistar o board com argumentos que aliam risco, ROI e visão estratégica.

Apoio: veeam Adistec

Sobre a **Penso**

A Penso é parceira estratégica da **VEEAM**, líder global em backup e recuperação.

Com as mais altas certificações do mercado e **ISO-27001**, oferecemos **Backup em Nuvem, Backup Imutável e DRaaS**, garantindo segurança máxima e recuperação rápida para seus dados.

+22	**+1600**	**+250**	**+5**	**98%**
Anos de know-how tecnológico	Clientes de grande porte	Especialistas em tecnologia	Data Centers Tier III no Brasil	de satisfação com nossas soluções

Acesse nosso site e conheça as **soluções da Penso**

Protegemos seus dados para que sua empresa nunca pare.

- Linhas de defesa contra ransomware
- Disaster Recovery as a Service (DRaaS)
- Cyber Security
- BaaS para Microsoft 365
- Backup Cloud e replicação

veeam
Competency Partner
DRaaS
BaaS *for 365*
Off-site Backup

Com mais de 22 anos de experiência, a **Penso é uma referência em soluções tecnológicas, reconhecida como Impact Cloud and Service Provider Partner of the Year Brasil pela Veeam.**

Esse prêmio destaca nosso papel como parceiro de maior impacto no ano, além de sermos uma das empresas mais certificadas entre os parceiros Veeam.

Com uma equipe de **mais de 250 profissionais,** oferecemos backup em nuvem, **backup imutável e DRaaS, garantindo segurança e recuperação rápida para grandes empresas.**

ÍNDICE

SPEAKER

Thiago Lima

CEO na Penso

+ 1.600 clientes corporativos ativos

+ Especialista em resiliência de dados

“Acredito que dados resilientes e sistemas disponíveis são a base de qualquer negócio moderno. **É isso que entregamos todos os dias**.”

Apoio: veeam Adistec

Soberania de Dados – A ameaça geopolítica que exige orçamento já

Soberania de dados é o conceito que coloca seus dados sob as leis do país onde são armazenados ou processados, abrangendo segurança, privacidade e acesso. Em 2025, com **60% dos dados globais nas nuvens americanas** como AWS, Azure e Google, esse tema ganhou um peso enorme, especialmente no Brasil, onde a LGPD impõe multas de até 2% do faturamento global por violações.

Discutir esse tema tornou-se crucial para proteger sua empresa de sanções internacionais, evitar perdas financeiras e posicionar você à frente no orçamento de 2026.

Líderes de TI têm a missão de convencer os C-Levels que ignorar os riscos pode custar caro.

Até 2025, **87% das empresas brasileiras** relataram preocupações com a soberania devido a sanções, segundo estimativas baseadas em tendências globais. **A questão transcende tecnologia: é sobre autonomia econômica e segurança nacional.**

A soberania é a base para continuidade de negócios em um mundo onde interrupções por leis estrangeiras crescem 200% desde 2024

Acontecimentos reais

O impacto da soberania de dados transcende debates teóricos e se traduz em cenários que desafiam a continuidade dos negócios em 2025, exigindo que líderes de TI transformem esses alertas em prioridades concretas para o próximo ano.

Os episódios reais apresentados a seguir ilustram como a falta de controle local pode expor vulnerabilidades críticas, oferecendo lições valiosas para moldar uma estratégia robusta no orçamento 2026. Veja alguns exemplos que comprovam essa realidade:

Nayara Energy (Índia)

Os impactos da Lei Magnitsky e de sanções globais encontram um exemplo concreto no caso da Nayara Energy, uma gigante indiana do setor de combustíveis.

Essa empresa teve sua **nuvem Microsoft abruptamente interrompida** por uma sanção da União Europeia contra a Rússia, motivada por laços comerciais da Nayara com aquele país em meio a tensões geopolíticas. **Os serviços foram paralisados por dias,** com a reativação levando quase 48 horas, resultando em perdas operacionais significativas.

Esse incidente ilustra como sanções podem atingir empresas sem envolvimento direto.

Nosso blog sobre soberania digital governamental destaca como esse tipo de risco pressiona migrações para soluções locais. **CLIQUE AQUI para acessar a matéria completa.**

Tribunal Penal Internacional (Haia, Holanda)

Seguindo o exemplo do STF, onde a Lei Magnitsky revelou vulnerabilidades em instituições públicas brasileiras, o caso do Tribunal Penal Internacional (TPI) em Haia reforça os riscos de interferências estrangeiras, destacando a urgência de soberania digital.

Monitor Mercantil

Microsoft bloqueia e-mail de chefe do TPI e Europa enfrenta dependência digital

O governo holandês está alarmado com a controversa decisão da Microsoft de bloquear a conta de e-mail de Karim Khan, procurador-chefe do Tribunal Penal Internacional (TPI), sediado em Haia. Em resposta, as autoridades começaram a reavaliar a infraestrutura digital oficial e a explorar alternativas aos provedores de tecnologia dos EUA.

Estabelecido como neutro desde o século XIX e ratificado pela ONU na década de 90, o TPI enfrentou em 2025 o bloqueio da conta do procurador-chefe pela Microsoft devido a uma sanção, rompendo sua neutralidade centenária.

Isso levou a Holanda a reavaliar a segurança de sua infraestrutura financeira em big techs, evidenciando como dependências tecnológicas podem ser exploradas por decisões externas.

Para empresas brasileiras, essa vulnerabilidade é um alerta: se um tribunal internacional, projetado para imparcialidade, sucumbe a sanções, o risco de paralisações em operações locais aumenta.

O Veeam Data Protection Trends Report 2025 aponta que a violação média custa US$4,5 milhões, amplificada por riscos soberanos. Tarifas como o “tarifaço americano” podem dobrar custos de serviços como Salesforce ou Office 365 em 2026.

Essa visão aponta para a necessidade de uma estratégia local robusta, pavimentando o caminho para que líderes de TI apresentem aos C-Levels uma solução que transforme vulnerabilidades em vantagens competitivas.

“Organizações brasileiras que depositam sua infraestrutura em grandes provedores internacionais ficam expostas a riscos globais voláteis”.

Pitch para C-Levels: Por que soberania no Budget 2026?

A vulnerabilidade revelada pela dependência de provedores internacionais não é apenas um risco, mas um chamado para líderes de TI assumirem o comando, reconhecerem que sanções e bloqueios já provaram seu poder de paralisar operações e moldarem o orçamento para 2026.

Para transformar essa necessidade em uma proposta vencedora, prepare um pitch que combine dados impactantes, exemplos reais e uma narrativa convincente. Por exemplo:

Risco financeiro:

Um dia de downtime custa US$9 mil por minuto em grandes empresas. Soberania evita isso." Reforce o caso do Apagão Indiano no Azure, que perdeu milhões em semanas devido a sanções e também destaque como data centers locais podem mitigar esse impacto.

Regulatório:

Multas LGPD podem chegar a bilhões. Backup soberano é conformidade barata." Use o exemplo de Haia para ilustrar a vulnerabilidade regulatória, sugerindo que conformidade com LGPD via soberania reduz riscos legais.

ROI claro:

"Investir em data centers nacionais retorna 5x em savings, protegendo receita." Apresente isso como um investimento estratégico, citando a economia de downtime e a competitividade frente a empresas vulneráveis.

Framework para Ação

Com os argumentos prontos para conquistar o board, o próximo passo é transformar a visão de soberania em ações concretas que fortaleçam sua empresa em 2026. Este framework oferece um roteiro claro para líderes de TI implementarem estratégias que protejam dados e assegurem competitividade, convertendo os riscos discutidos em oportunidades tangíveis.

Mapeie dependências: Identifique ferramentas como Office 365 (comunicação, SharePoint) sob o CLOUD Act. Um backup interno sozinho expõe tudo a cortes.

Avalie por segmento: Uma loja de parafusos enfrenta risco baixo, mas uma exportadora nuclear exige DR soberano como prioridade.

Mitigações práticas:

- **Office 365:** Adote backup imutável em data centers brasileiros, como os da Penso. Restaure em menos de 24 horas, vire MX e evite paralisia.
- **AWS/Azure:** Para ERP na zona SP, ainda sob CLOUD Act, implemente DR soberano para virar para nuvem local em minutos, cobrindo múltiplos riscos.

Budget 2026: Aloque 20-30% para soberania, investindo em backups e storage nacionais.

Máxima: Duas cópias, dois mundos. Sem isso, 2026 será um pesadelo geopolítico.

Cybercrime com IA – A máquina que derrete trilhões e exige defesas robustas

Após assegurar a soberania de dados contra ameaças externas, o cybercrime impulsionado por inteligência artificial emergiu em 2025 como um novo desafio dentro das operações da sua empresa, com ataques cada vez mais sofisticados que colocaram empresas em risco constante de paralisações e vazamentos.

Segundo o Veeam 2025 Ransomware Trends and Proactive Strategies Report, **97% dos ransomwares miram backups primeiro, enquanto 69% das empresas sofreram violações.** Essa evolução exige uma nova camada de proteção no orçamento 2026, equipando líderes de TI com estratégias para convencer C-Levels a agir e transformar vulnerabilidades em fortalezas digitais.

O Poder destrutivo da IA nos ataques

A crescente sofisticação do cybercrime com IA exige que líderes de TI compreendam como essa tecnologia transforma ameaças tradicionais em riscos imediatos para suas empresas, pavimentando o caminho para uma defesa proativa no orçamento 2026.

Esses ataques, alimentados por inteligência artificial, exploram vulnerabilidades humanas e tecnológicas com precisão assustadora, desafiando a segurança digital a um novo nível.

Veja como os ataques podem se manifestar:

Phishing Hiperpersonalizado

A IA analisa perfis em redes sociais, como Instagram ou LinkedIn, identificando detalhes pessoais – hobbies, nomes de familiares ou preferências – para criar e-mails sob medida. Imagine receber uma mensagem como “Thiago, participe desta exclusiva trilha de corrida com desconto especial!”, com um link que parece legítimo, mas instala malware ao ser clicado. Isso custa zero aos criminosos, mas pode comprometer toda a rede corporativa em minutos, exigindo defesas robustas.

Vishing (Voice Phishing)

A IA realiza ligações automáticas que gravam sua voz em segundos, capturando tons e padrões para criar deepfakes usados em fraudes telefônicas. Por exemplo, um criminoso pode simular sua voz para autorizar transações bancárias, explorando a confiança interna. A recomendação é desligar imediatamente chamadas de números desconhecidos para evitar esse risco crescente.

Quebra de Senhas

A IA cruza informações pessoais como nomes de filhos ou times favoritos, com bancos de dados de breaches para testar senhas em massa. Com 80% dos ataques originando-se de atualizações pendentes, que somam cerca de 6 por estação a cada semana, uma senha fraca como “Tecnologia2025” pode ser descoberta em horas, abrindo portas a invasões devastadoras.

Em 2024, o Brasil registrou

84,6 MILHÕES

DE CONTAS VIOLADAS

um aumento de 340% em relação ao ano anterior

1.827 INCIDENTES

de ransomware no último trimestre

Essa é uma urgência real: sem estratégias robustas de cybersegurança com Disaster Recovery, serviços críticos podem parar por semanas.

Ficou preocupado com a vulnerabilidade do seu e-mail?

No artigo "Descubra o poder da Criptografia S/MIME no email: Benefícios e Motivos de Uso", publicado em nosso blog, explicamos os principais motivos para adotar a criptografia S/MIME como defesa contra ameaças como phishing impulsionado por IA. Esta solução capacita líderes de TI a levarem ao board uma estratégia que protege sua empresa, combinando segurança avançada com custos acessíveis.

Confira os benefícios que justificam sua inclusão no orçamento 2026:

Autenticação e verificação do remetente: Garante que e-mails venham de fontes legítimas, bloqueando tentativas de phishing que comprometem redes.

Integridade das mensagens: Protege contra alterações não autorizadas durante o trânsito, assegurando a confiabilidade das comunicações.

Confidencialidade das informações: Criptografa o conteúdo, permitindo acesso apenas ao destinatário, essencial para dados sensíveis.

Cumprimento de regulamentações: Atende à LGPD e outras normas, reduzindo o risco de multas bilionárias.

Para explorar mais detalhes e implementar essa proteção, acesse nosso blog.

Cybersegurança é investimento essencial

A escala das ameaças digitais abre a porta para líderes de TI promoverem uma revolução no orçamento 2026. Esta é a oportunidade de elevar a segurança da empresa ao próximo nível, apresentando aos C-Levels uma visão que transforma vulnerabilidades em ativos estratégicos. Use os seguintes argumentos:

Ameaça evolutiva: A IA adapta ataques em tempo real, tornando defesas estáticas obsoletas. Investir em monitoramento ativo é essencial.

Produtividade preservada: Paralisações por ransomware custam semanas de trabalho. Soluções proativas mantêm operações fluindo

Confiança do mercado: Segurança avançada contra IA reforça a reputação, atraindo clientes e parceiros em um cenário de riscos crescentes.

Defesas para 2026

Com os C-Levels convencidos pela visão estratégica, o momento é de transformar o orçamento 2026 em um escudo contra o cybercrime com IA, posicionando sua empresa como líder em resiliência.

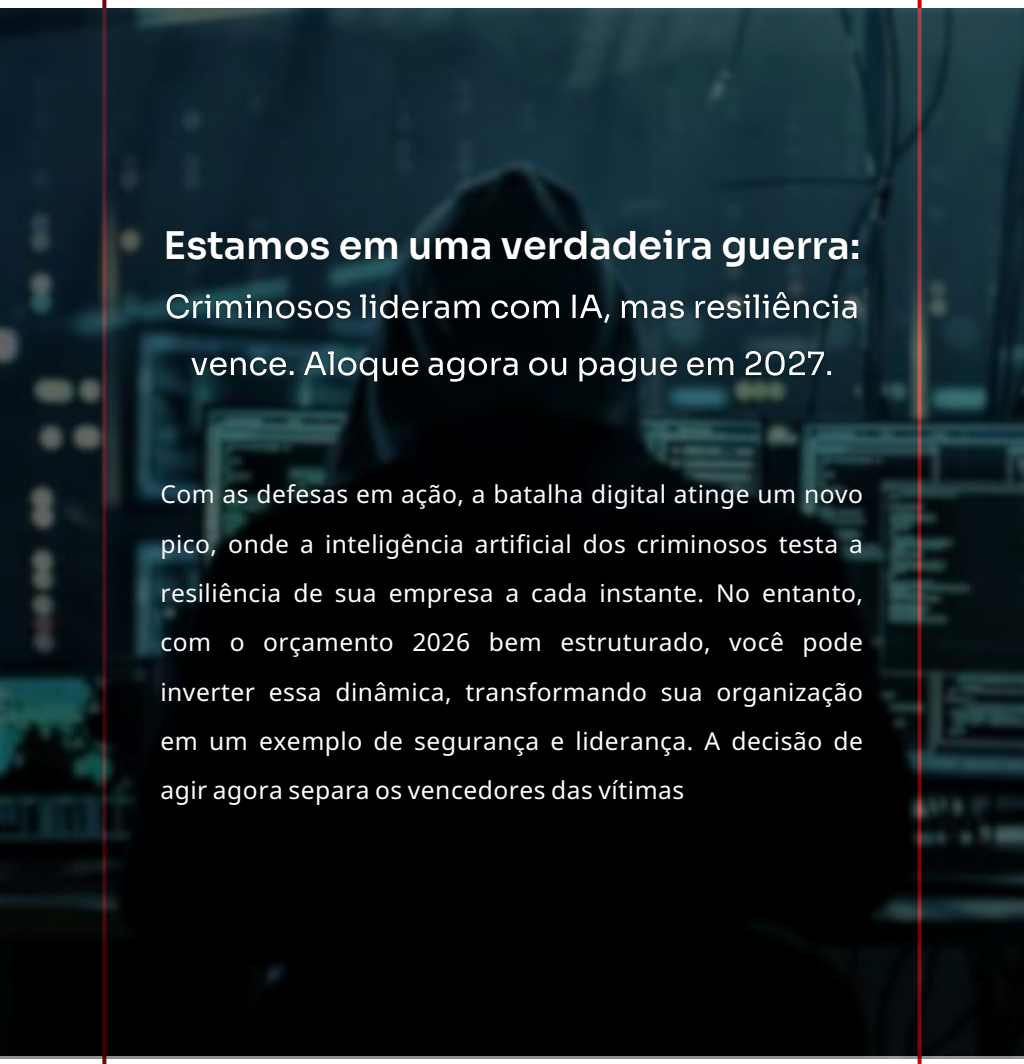
Este plano prático capacita líderes de TI a implementarem defesas que não apenas reagem, mas antecipam ameaças, assegurando operações contínuas e fortalecendo a confiança do mercado. Adote as seguintes medidas:

Patching Automatizado: Use RMM para gerenciar 6 updates semanais, cobrindo home office e filiais. Scans semanais fecham 80% das brechas.

MFA Universal: Aplique autenticação multifator em e-mail e ERP, usando tokens no celular. Revise acessos ao demitir para prevenir brechas.

Endpoint e Treinamento: Instale anti-spam, EDR e bloqueie USBs. Treine usuários para evitar 70% dos cliques errados.

IA Defensiva: Integre ferramentas que detectem anomalias em tempo real, conforme recomendado pelo Veeam 2025 Ransomware Trends and Proactive Strategies Report.



Estamos em uma verdadeira guerra:

Criminosos lideram com IA, mas resiliência vence. Aloque agora ou pague em 2027.

Com as defesas em ação, a batalha digital atinge um novo pico, onde a inteligência artificial dos criminosos testa a resiliência de sua empresa a cada instante. No entanto, com o orçamento 2026 bem estruturado, você pode inverter essa dinâmica, transformando sua organização em um exemplo de segurança e liderança. A decisão de agir agora separa os vencedores das vítimas

Continuidade de Negócios: Transformando crises em oportunidades de liderança

No cenário digital de 2025, uma falha em sistemas pode paralisar seu faturamento em instantes. O Veeam 2025 Ransomware Trends and Proactive Strategies Report destaca o aumento de 25% nos orçamentos de segurança, embora 70% das empresas permaneçam vulneráveis e enfrentando downtimes médios de 3 semanas.

A continuidade surge como o alicerce essencial do orçamento 2026 e líderes de TI têm a oportunidade de guiar os C-Levels rumo a uma estratégia que não apenas mitigue crises, mas eleve sua empresa a um patamar de liderança.

Resiliência de dados é sobre proteger o coração do negócio

A vulnerabilidade exposta pelos downtimes prolongados exige que a continuidade comece pela proteção dos dados, o sangue vital de sua empresa, tornando essa prioridade uma alavanca para o orçamento 2026.

Líderes de TI têm a missão de demonstrar aos C-Levels como resguardar informações críticas não é apenas uma defesa, mas um investimento que assegura operações sem interrupções.

Dados são a alma da operação. Perder isso é falência digital.

Exemplo de Cenário Vulnerável:

Com apenas um backup local em um storage separado, o tempo de recuperação total (RTO) pode alcançar 7 dias, enquanto o ponto de recuperação (RPO), baseado em backups diários às 4h, resulta na perda de um dia inteiro de trabalho se um incidente ocorrer às 17h – afetando notas fiscais e faturamento. Um incêndio no centro de dados adiciona o risco de destruição total.

Solução Estratégica:

Um backup imutável em nuvem, armazenado em data centers brasileiros como os da Penso, protege contra ransomwares e desastres. Testes mensais reduzem o RTO para horas. Exemplo: Um cliente varejista restaurou operações em 6 horas, economizando R$1,5 milhão em downtime.

Pitch para C-Levels:

"Um dia sem dados custa milhões. Backup imutável retorna 5x o investimento, com SLA comprovado pela Penso Tecnologia."

Resiliência de sistemas: Como garantir operações ininterruptas

Com os dados protegidos como alicerce, o foco agora se volta para sustentar os sistemas que os mantêm vivos, posicionando a continuidade como um diferencial estratégico no orçamento de 2026. Essa etapa eleva sua empresa a um patamar de excelência operacional, onde a interrupção deixa de ser uma ameaça e passa a ser uma oportunidade de demonstrar resiliência.

1 Cenário crítico

Se SAP cair por ransomware, sem um plano de recuperação, a restauração pode levar 7 dias, tempo demais para emitir notas fiscais ou processar folha de pagamento.

2 Solução

Um Disaster Recovery (DR) soberano em data centers brasileiros garante que, em caso de falha, a operação mude para um ambiente de contingência em 15 minutos, mantendo os usuários ativos.

3 Benefícios extras

DR cobre desastres físicos e falhas de provedores. Um cliente industrial evitou R$ 8 milhões em perdas com DR da Penso.

4 Pitch Executivo

“7 dias offline custam milhões; DR soberano mantém faturamento por fração do custo.”

Soluções que inspiram continuidade

Diante das enchentes que devastaram o Rio Grande do Sul em maio de 2024, com impactos em 2025, a Penso Tecnologia lançou uma iniciativa relatada na matéria "Penso Tecnologia anuncia ajuda às Empresas Afetadas pelas Enchentes no Rio Grande do Sul", publicada em nosso blog.

Essa iniciativa combinou tecnologia Veeam com data centers locais, liberando 1 petabyte de storage soberano gratuito para restaurar operações em dias e provando que a continuidade leva à liderança de mercado.

Técnicas para garantir o budget de Cybersegurança e Soberania

Convencer C-Levels em 2025 exige estratégia, números e histórias de impacto. O board quer ROI e mitigação de riscos financeiros. Aqui está um playbook para garantir que cybersegurança e soberania sejam prioridades no orçamento 2026 – e posicionar sua empresa como líder.

Passo a passo para um pitch imbatível

Com o board atento aos números e histórias que ressoam, o próximo movimento é estruturar um pitch que converta essas evidências em decisões concretas. Esta sequência guia líderes de TI através de uma abordagem comprovada que cativa executivos, alinha segurança à visão estratégica e garante alocação de recursos. Siga estes passos:

Apresente os riscos com Big Numbers:

> 60% dos dados globais estão em nuvens americanas sob o CLOUD Act, expostas a cortes como no caso indiano.

> Ataques de ransomware atingiram 69% das empresas em 2025, segundo o Veeam 2025 Ransomware Trends and Proactive Strategies Report.

Mostre ROI Tangível:

> Backup imutável evita perdas de US$ 4,5 milhões por violação, com retorno de 5x.

> DR soberano reduz downtime de 7 dias para 15 minutos, salvando milhões.

Proponha Alocação Estratégica:

30%
Soberania
backups e storage nacionais.

40%
Cibersegurança
RMM, MFA, anti-phishing.

30%
Continuidade
DR e testes regulares.

Use Casos Reais:

> A Penso restaurou operações no Rio Grande do Sul com 1 petabyte gratuito, provando resiliência.

Foco na Competitividade:

> Enquanto 70% das empresas são vulneráveis, investir agora representa uma vantagem diante do mercado.

Superando objeções comuns

Com um pitch estruturado em mãos, o desafio agora é desarmar as dúvidas que podem bloquear o orçamento 2026, transformando resistências em aliados. Esta abordagem capacita líderes de TI a anteciparem objeções dos C-Levels e responder com confiança, usando lógica e exemplos que solidifiquem o compromisso com cybersegurança e a soberania.

Prepare-se para enfrentar essas barreiras:

"É caro!"	**Responda:** **"Um ataque custa US$ 4,5 milhões; nossas soluções custam 10% disso."**
"Não temos risco!"	**Responda:** **"A suspensão do TPI em Haia mostra que ninguém está imune."**
"Já temos proteção!"	**Responda:** **"97% dos ransomwares miram backups; sua solução é imutável?"**

Com as objeções superadas, o caminho se abre para reforçar sua proposta com uma base sólida de conhecimento, elevando a credibilidade perante os C-Levels no orçamento 2026. Esta abordagem destaca como a experiência da Penso transforma desafios em estratégias vencedoras, oferecendo aos líderes de TI ferramentas para consolidar o caso de investimento.

Ferramentas para o Pitch

Com a credibilidade consolidada pelo conhecimento estratégico, o próximo passo é equipar você, líder de TI, com recursos que transformam ideias em ação, assegurando o orçamento 2026. Estas táticas práticas elevam seu pitch a um nível irresistível, capturando a atenção dos C-Levels e pavimentando o caminho para investimentos que protejam e impulsionem o negócio. Adicione estas ferramentas ao seu arsenal:

One-Pager:
Crie um resumo com números (60% sob CLOUD Act, 69% de ataques) e o case do RS.

Citação de Impacto:
"Parar um sistema hoje é parar de vender, faturar, prestar serviço. Continuidade é o coração do orçamento 2026," disse Thiago Lima, CEO da Penso, durante o webinar.

Storytelling:
Use o exemplo do RS para mostrar impacto real da Penso.

Dica Final: Agende uma reunião com o board e use nossos cases para provar que a Penso, com 98% de satisfação, é o parceiro ideal.

Casos de Sucesso da Penso: Histórias reais que inspiram o orçamento 2026

Com as técnicas de pitch já em seu domínio, o poder de persuadir os C-Levels ganha vida através de histórias que provam resultados. Esses casos da Penso oferecem a você a munição perfeita para conquistar o board e posicionar sua organização como referência em resiliência.

Caso 1:

1 Petabyte de resiliência no Rio Grande do Sul

Enchentes devastadoras no RS em 2025 deixaram empresas sem acesso a dados. A Penso agiu rápido, liberando 1 petabyte de storage soberano gratuito em seus data centers Tier III.

- **Execução:** Implementamos backups imutáveis para PMEs afetadas, com suporte 24/7. Dados de vendas, estoque e clientes foram restaurados em 3 dias, contra meses de recuperação típica.

- **Impacto:** Dezenas de PMEs restauraram operações em 3 dias, contra meses de recuperação típica. Um cliente varejista retomou vendas online, preservando R$2 milhões em receita mensal e 50 empregos.

- **Lições para o Budget:** Storage soberano é acessível e escalável, atendendo LGPD e riscos geopolíticos. Para C-Levels: “1 PB salvou o RS; nossa operação merece essa proteção.”

Matéria Completa: Clique aqui

Caso 2:

DR Soberano para uma exportadora de tecnologia sensível

Uma exportadora de tecnologia nuclear enfrentava riscos soberanos por operar com países sob sanções. Adotou DR soberano nos data centers da Penso.

- **Execução:** Configuramos um ambiente contingente para ERP e CRM, com failover automático. Em uma tentativa de bloqueio, a virada levou 15 minutos.

- **Impacto:** Economia de R$10 milhões em downtime evitado, além de conformidade LGPD. A empresa manteve contratos internacionais.

- **Lições para o Budget:** DR soberano é vital para setores sensíveis. Diga ao board: “15 minutos para voltar ao ar é liderança.”

Matéria Completa: Clique aqui

Caso 3:

Criptografia S/MIME Contra Phishing em uma Financeira

Uma instituição financeira enfrentava phishing direcionado por IA, comprometendo dados de clientes. Implementou criptografia S/MIME com suporte da Penso.

- **Execução:** Integramos S/MIME em sistemas de e-mail, com treinamento que reduziu cliques errados em 70%.

- **Impacto:** Zero violações em comunicações críticas após 6 meses, evitando multas LGPD de até R$50 milhões. A confiança dos stakeholders cresceu.

- **Lições para o Budget:** S/MIME é investimento de baixo custo. Apresente: “Proteger e-mails evita milhões de perdas.”

Matéria Completa: Clique aqui

Argumentos para o Board

As vitórias da Penso nos casos de sucesso abrem um caminho claro para posicionar sua empresa como líder, oferecendo a você, líder de TI, uma base sólida para influenciar o orçamento 2026.

"Temos 22 anos de know-how porque entregamos resiliência que não falha. Nossos clientes voltam a operar em minutos, não semanas."

- Thiago Lima
CEO da Penso Tecnologia

Esses argumentos transformam as histórias em propostas poderosas, unindo proteção, retorno e competitividade para conquistar o board. Considere estas razões:

Prova de Resiliência:
A restauração de 1 petabyte no Rio Grande do Sul salvou R$ 2 milhões em receita, provando que soberania funciona.

Impacto Financeiro:
DR soberano evitou R$10 milhões em perdas para uma exportadora, destacando o valor de contingência rápida.

Segurança Acessível:
Criptografia S/MIME protegeu uma financeira de R$50 milhões em multas, com baixo custo de implementação.

Ferramentas Essenciais da Penso:

Seu arsenal para um 2026 inquebrável

Com os casos de sucesso e argumentos já conquistando o board, o foco agora se volta para as ferramentas que colocam essas promessas em prática, fortalecendo sua empresa no orçamento de 2026. Esta jornada oferece a você, líder de TI, soluções testadas pela Penso que unem tecnologia e estratégia, permitindo apresentar ao C-Levels um plano que não só protege, mas projeta sua organização como líder em resiliência.

Snapshots e Virtualização

Snapshots transformam a recuperação de desastres, criando cópias instantâneas de sistemas inteiros. Essas cópias são replicadas para um ambiente secundário (nuvem ou data center), permitindo restauração em minutos.

Diferente do DR tradicional, que exigia reconstrução lenta, os snapshots garantem agilidade sem comprometer dados.

Multi-cloud

Soluções multicloud permitem que o DR funcione com qualquer plataforma – de on-premises a AWS, Azure ou nuvens privadas. Isso elimina a dependência de fornecedores específicos e possibilita replicar sistemas de Hyper-V, VMware ou Nutanix para o destino mais conveniente, reduzindo custos e complexidade.

Isolamento Seguro

A segurança é prioridade no DR moderno. Ambientes secundários são isolados, com credenciais separadas do ambiente principal, evitando que uma invasão se propague. O versionamento permite restaurar pontos íntegros, como o estado do sistema antes de um ataque, minimizando perdas.

Suporte e flexibilidade

A Penso adapta soluções para qualquer órgão, de pequenas prefeituras a grandes autarquias. **Oferecemos suporte avançado, monitoramento contínuo e licenciamento Veeam** (VUL, Data Cloud, SaaS). Projetos são implementados em até três meses, com custo acessível e sem surpresas orçamentárias.

Como a Penso pode garantir a segurança dos seus dados?

- ✓ Realizar BIAs para identificar processos críticos.
- ✓ Construir políticas globais e contínuas de resiliência de dados.
- ✓ Implementar disaster recovery com **recuperação de 15 minutos.**
- ✓ Garantir governança e testes periódicos.
- ✓ Fazer um diagnóstico da infraestrutura atual.

O que é o BIA? Business Impact Analysis

Realizamos uma análise de impacto de negócio (BIA) para identificar sistemas e processos críticos, definindo tempos aceitáveis de interrupção do setor.

Implementar Estratégia de Resiliência de Dados Global e Contínua

Auxiliamos os nossos clientes a construírem uma política sólida de backup global e contínua, envolvendo todos os seus dados, mesmo em ambientes multicloud.

Resiliência de Processos e Sistemas (DR)

Implementamos soluções de Disaster Recovery, estabelecendo em conjunto com todos os setores quais serão as prioridades e quanto tempo levará para recuperação, além de realizarmos testes periódicos para garantir o funcionamento perfeito.

O nosso plano de Disaster Recovery define tempos de recuperação (RTO) e pontos de recuperação (RPO) para sistemas críticos, de acordo com as necessidades de cada negócio.

Mas o que é RPO e RTO ?

O Recovery Point Objective (RPO) define o intervalo máximo aceitável de perda de dados em caso de falha, indicando quanto tempo de informações uma empresa pode perder sem comprometer a continuidade dos negócios. Quanto menor o RPO, maior a frequência dos backups, reduzindo a perda de dados em caso de desastre.

O Recovery Time Objective (RTO), por sua vez, determina o tempo máximo que um sistema pode ficar indisponível antes de causar impactos críticos. Quanto menor o RTO, maior a necessidade de tecnologias rápidas de recuperação, como failover automático e storage redundante, para garantir a rápida retomada das operações.

RPO e RTO na Prática		
Cenário	**RPO (Ponto de Recuperação)**	**RTO (Tempo de Recuperação)**
Banco de Dados Financeiro	5 minutos	15 minutos
E-commerce	10 minutos	30 minutos
Sistema de Atendimento ao Cliente	30 minutos	1 hora
Arquivos Internos e E-mail	12 horas	6 horas

Saiba mais sobre RPO e RTO em nosso Blog. VER ARTIGO

Estratégia de Resiliência de Dados

Adotamos uma política robusta de recuperação, chamada **"Golden Rule" 3-2-1-1-0 (3 cópias, 2 mídias diferentes, 1 off-site, 1 imutável, 0 erros),** além de implementarmos uma rotina de testes regular, que garante sua eficácia diante de qualquer cenário.

Se você deseja se aprofundar na Regra 3-2-1-1-0, acesse o conteúdo completo no nosso blog.

Fundamentos para Liderar em 2026

Dos desafios de soberania expostos por sanções globais às ameaças de cybercrime com IA e à necessidade de continuidade diante de crises, este e-book traçou um caminho de resiliência para sua empresa.

A Penso uniu tecnologia avançada e estratégias práticas para proteger dados, assegurar sistemas e blindar operações, como visto nos casos reais.

Agora, você, líder de TI, tem em mãos a base para apresentar aos C-Levels um orçamento 2026 que não apenas defende, mas posiciona sua organização como líder no mercado.

Como a Penso ajuda a transformar seu orçamento 2026 em vitória

O relógio está correndo. Com US$ 10,5 trilhões perdidos em 2025, 97% dos ataques mirando backups, e soberania cortando acessos sem aviso, adiar o planejamento para 2026 é assinar um atestado de vulnerabilidade.

Você, líder de TI, pode transformar o orçamento 2026 em um escudo de liderança digital, guiando o board com a visão da Penso.

Sem continuidade, sua empresa para de vender e faturar. Um orçamento bem estruturado pode salvar a operação.

Como a Penso pode ajudar você agora

Nossos especialistas, pioneiros em soluções personalizadas, garantem resultados que elevam sua empresa:

Consultoria Estratégica Gratuita: Avaliamos suas vulnerabilidades em soberania, cyber e continuidade, entregando um roadmap personalizado para o budget 2026.

Soluções Sob Medida:

- **Backup Imutável Veeam:** Proteção contra ransomwares, com storage soberano.
- **DR Soberano:** Continuidade em minutos, não dias, em data centers brasileiros.
- **Criptografia S/MIME:** Blindagem contra phishing IA-potencializado.
- **RMM e Treinamento:** Gestão de updates e educação para fechar 80% das brechas.
- **Suporte 24/7:** Nossa equipe garante SLA de recuperação rápida.

Com a Penso, o orçamento 2026 é a chave para reinar no caos digital, transformando cada risco em um troféu de liderança. Sua ação agora define o futuro.

Experiência comprovada

Como primeiro provedor brasileiro com certificações Veeam em DR, backup offsite e Office 365, a Penso tem experiência com prefeituras, estados, forças armadas e órgãos federais. Nossos cinco data centers e equipe especializada garantem soluções personalizadas, mas padronizadas para agilidade e economia.

Com ataques cibernéticos crescendo, parceiros confiáveis como a Penso são essenciais para proteger serviços e cumprir normas regulatórias.

Pronto para fortalecer a resiliência dos seus dados?

Transforme a tecnologia em aliada da sua empresa

veeam
Competency Partner
DRaaS
BaaS *for 365*
Off-site Backup

Penso Tecnologia recebe prêmio da Veeam como "Impact VCSP Partner of the Year"

Reconhecimento destaca a excelência da Penso Tecnologia em resiliência de dados e consolida sua posição como referência no mercado de TI

Por PressWorks
14/03/2025 08h40 · Atualizado há 4 semanas

Conheça nosso portfólio completo para **proteger dados, otimizar processos e garantir a continuidade** do seu negócio.

PROTEÇÃO DE DADOS

Veeam Backup

Solução para proteger os dados da sua empresa.

Backup na Nuvem

Segurança para sua empresa e benefícios aos usuários.

Disaster Recovery

Proteção contínua para uma empresa mais segura.

Backup 365

Backup seguro dos seus e-mails Microsoft 365.

CYBER SECURITY

Pentest como serviço

Mapeamento e redução de falhas na segurança.

Segurança para o usuário

Proteção efetiva contra ameaças virtuais.

Firewall como serviço

Proteção avançada da rede da sua empresa.

SERVIÇOS DE TI

Gestão e suporte de TI

Atendimento especializado remoto ou presencial.

Suporte Avançado N2, N3 e Especialistas

Apoio para demandas de alta complexidade

COMPUTAÇÃO EM NUVEM

Penso Cloud Corporativo

Migração segura para nossa nuvem

Penso S3 Storage

Armazenamento em nuvem

EMAIL E COLABORAÇÃO

PensoMail

E-mail corporativo personalizado para sua empresa.

Zimbra: e-mail corporativo

Conheça nossas soluções baseadas em Zimbra

Auditoria de e-mail

Acompanhe os e-mails trafegados no seu negócio.

Cloud Antispam

A solução antispam ideal para nuvem.

Conclusão

O cenário de tecnologia e negócios mudou de forma irreversível. Soberania de dados, ciberataques e automação inteligente deixaram de ser temas restritos à TI e se tornaram parte da estratégia central das organizações.

Cada decisão de planejamento agora precisa considerar segurança, continuidade e autonomia digital como fundamentos da operação. O risco não está apenas em perder dados, mas em interromper o que sustenta o negócio. As empresas que compreendem essa dinâmica ganham tempo, estabilidade e capacidade de reação.

O desafio é permanente, mas o conhecimento é a primeira defesa

Entender, antecipar e agir com consciência é o que garante que, independentemente do cenário, o essencial continue em movimento.

Seguimos juntos, transformando complexidade em continuidade.

Penso

BUDGET 2026

ENFRENTANDO OS DESAFIOS ATUAIS

#Obrigado

Apoio: veeam Adistec