Soberania de dados no Brasil e a lei Magnitsky

Apoio: veeam Adistec

Introdução

A soberania de dados no Brasil está sob ameaça crescente devido à aplicação de leis internacionais como a Magnitsky e o Cloud Act, que podem resultar em interrupções abruptas de serviços essenciais.

Neste eBook, baseado no webinar exclusivo realizado pela Penso Tecnologia em 20 de agosto de 2025, exploramos em profundidade os impactos dessas normas nas empresas brasileiras, incluindo riscos jurídicos, geopolíticos e operacionais. Apresentado por Erik de Lopes Morais, cofundador e COO da Penso, o conteúdo destaca casos reais recentes e estratégias práticas para mitigar esses perigos, garantindo resiliência e conformidade com a LGPD.

Saiba como se proteger.

Apoio: veeam Adistec

Penso

A PENSO GARANTE QUE SEUS DADOS SEJAM

SOBERANOS, NÃO SUBMISSOS.

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

Erik Lopes Morais

COO e Cofundador da Penso

- Especialista em resiliência de dados e soberania digital

"Acredito que a soberania de dados é a base da autonomia empresarial moderna. **É isso que entregamos todos os dias.**"

Apoio: veeam Adistec

Você é capaz de dizer se seus dados estão **sob controle brasileiro ou expostos a leis estrangeiras?**

É por isso que esse conteúdo é tão necessário

Você sabia?

A adoção de infraestrutura nacional cresceu de

45% PARA **68%**

entre 2024 e 2025, impulsionada por leis como a Magnitsky.

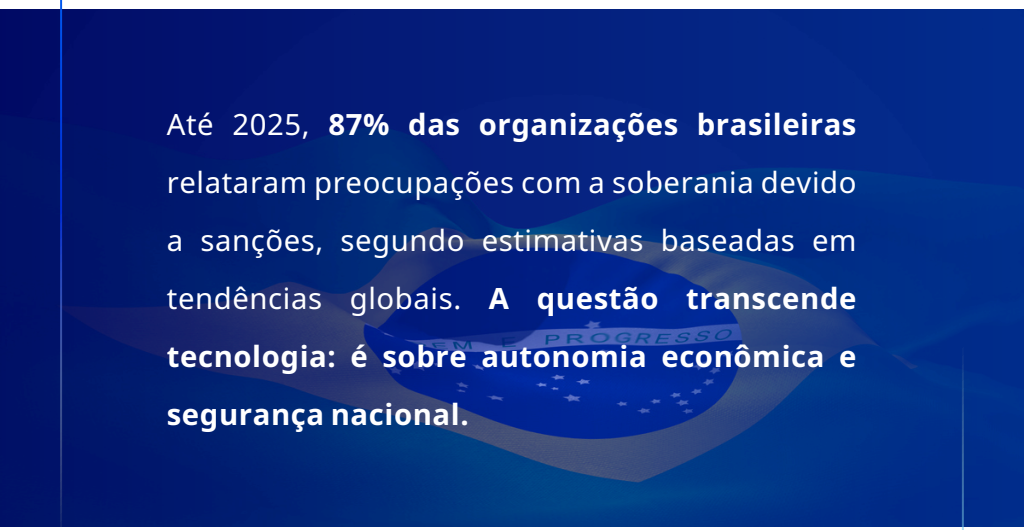
A soberania de dados está presente em todos os lugares. Inclusive em riscos jurídicos internacionais.

O Conceito de Soberania de Dados

Soberania de dados refere-se ao controle de uma nação ou empresa sobre suas informações, garantindo que estejam protegidas por jurisdição local e imunes a interferências externas.

No Brasil, esse conceito ganhou relevância com a LGPD (Lei Geral de Proteção de Dados), que exige transparência sobre onde dados são armazenados. Porém, **a dependência de big techs como Microsoft, Google e AWS expõe empresas a riscos**, especialmente em cenários geopolíticos tensos.

Imagem gerada por Inteligência Artificial



Até 2025, **87% das organizações 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

- Erik de Lopes Morais, COO da Penso

Contexto Global e Desafios Jurídicos

O cenário global de 2025 revela um aumento de 200% em riscos jurídicos relacionados a dados, impulsionado por tensões entre potências como EUA, UE e China. **Empresas brasileiras, dependentes de nuvens estrangeiras, enfrentam interrupções por sanções** que sobrepõem leis de privacidade, como a LGPD, à segurança nacional.

Esse conflito cria um dilema: enquanto a LGPD protege dados locais, leis como o Cloud Act permitem acessos unilaterais dos EUA, afetando 75% das organizações que usam big techs. A escalada inclui sanções secundárias, onde bancos globais evitam transações para não perder acesso ao sistema financeiro americano, isolando empresas.

O que aconteceria hoje se a Microsoft, Google ou AWS **interrompessem seus serviços abruptamente?**

Interrupções por questões não técnicas

Imagine **87% das organizações brasileiras afetadas por dependência de big techs** estrangeiras, a maioria não preparada, enfrentando colaterais geopolíticos como tensões EUA-China.

Até 2025, interrupções eram raras e técnicas, mas agora, sanções judiciais e políticas causam paradas em escala global. Em 2024, casos eram quase inexistentes; em 2025, o aumento expressivo em riscos jurídicos deixou **empresas inoperantes por até uma semana.**

É urgente reavaliar: sem soberania, sua operação pode parar sem aviso.

Essa vulnerabilidade é agravada pela crescente sofisticação dos ataques cibernéticos.

O Ransomware Trends Report 2024 da Veeam indicou que **94% dos incidentes miram backups para impedir recuperações,** afetando diretamente empresas que dependem de infraestruturas não controladas localmente.

Além disso, a **latência e os custos imprevisíveis de nuvens estrangeiras**, combinados com o shadow IT que atinge 60% das empresas, criam um cenário onde a continuidade depende de ações proativas.

Leis que ameaçam a soberania

Diante dos desafios globais e jurídicos expostos, **as leis que regem as big techs emergem como catalisadoras diretas das ameaças à soberania de dados.** Elas transformam a dependência de infraestruturas estrangeiras em pontos de vulnerabilidade crítica, conectando os riscos geopolíticos mencionados ao impacto prático nas operações:

Cloud Act (EUA)

Promulgada para garantir segurança nacional, obriga empresas americanas (Microsoft, Google, AWS) a fornecer dados globais sob demanda governamental. Sem lei federal de privacidade, interpretações amplas sobrepõem a LGPD, expondo 75% das organizações dependentes a vazamentos sem notificação. Relatórios Veeam indicam que 92% das empresas em multi-cloud enfrentam riscos de dados espalhados, agravados por esse acesso unilateral.

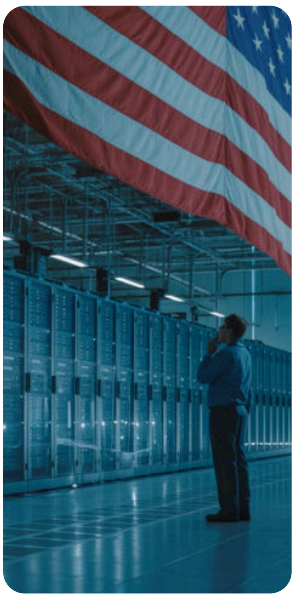
Evidence Act (UE)

Similar, exige que big techs na Europa entreguem dados para investigações, criando pontes para sanções extraterritoriais que afetam operações como a da Nayara que contaremos no capítulo 5.

A interação Brasil-China, com 80% das exportações em jogo, pode gerar colaterais em tensões EUA, como discutido em nosso blog sobre IA chinesa e conflitos regulatórios com LGPD.

Essas leis subvertem a privacidade, exigindo estratégias de mitigação urgentes.

Origem e Impacto da Lei Magnitsky



Curiosidade sobre a Lei Magnitsky

Sergei Magnitsky, advogado e auditor russo, descobriu em 2008 um esquema de corrupção envolvendo autoridades do governo que desviaram 230 milhões de dólares em impostos. Após denunciar, foi preso pelos próprios acusados e, sem condenação, passou 11 meses detido. Morreu na prisão com sinais de negligência e possível tortura.

Essa tragédia levou os Estados Unidos a criar, em 2012, a Lei Magnitsky, que **impõe sanções globais contra indivíduos ou entidades** envolvidas em violações de direitos humanos ou corrupção significativa, incluindo o congelamento de bens e proibições de entrada nos EUA, sem necessidade de processo judicial prévio no país sancionado.

Mas atenção: sua importância transcende o âmbito original, impactando diretamente o setor tecnológico.

Embora não projetada para regular dados ou serviços digitais, a aplicação da lei em 2025 a figuras como o ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), revelou seu alcance inesperado.

A sanção gerou tensões em serviços de e-mail e sistemas críticos do STF, levantando a possibilidade de bloqueios totais que poderiam **paralisar operações judiciais por até 21 dias**, conforme estimativas baseadas em tendências Veeam.

Migalhas

Tensão diplomática

Lei Magnitsky, dos EUA, já puniu 672 e pode atingir Moraes; entenda

Norma norte-americana permite sanções unilaterais por corrupção e abusos de direitos humanos, com efeitos reputacionais e patrimoniais.

Da Redação
terça-feira, 29 de julho de 2025
Atualizado em 30 de julho de 2025 13:53

Relatórios da Veeam indicam que 97% das sanções recentes miraram backups, expondo vulnerabilidades cibernéticas em infraestruturas dependentes de big techs.

No Brasil, a relevância da Magnitsky amplifica-se com a decisão do ministro Flávio Dino, em 2025, de declarar que sanções estrangeiras como essa não têm validade automática, alinhando-se à Constituição e à LINDB (Lei de Introdução às Normas do Direito Brasileiro). Essa postura visa proteger a soberania nacional, mas pode isolar o país financeiramente se bancos globais, pressionados por sanções secundárias, recusarem transações – **um risco que afeta 80% das exportações brasileiras ligadas a mercados como a China.**

Embora voltada a direitos humanos, **a Lei Magnitsky tornou-se um catalisador de interrupções tecnológicas,** exigindo estratégias de resiliência como backups imutáveis e DRaaS para mitigar impactos, como discutido em nosso blog sobre adequação à LGPD.

Para saber mais, acesse nossa matéria

Acontecimentos Reais

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.**

STF e Ministro Alexandre de Moraes

O caso do Supremo Tribunal Federal (STF) e do ministro Alexandre de Moraes mostra como a Lei Magnitsky pode atingir instituições públicas no Brasil.

Em 2025, a sanção contra Moraes gerou tensão nos serviços de e-mail do STF, com risco de bloqueio total e migrações custosas, embora o serviço tenha se mantido ativo. A ameaça persiste, revelando vulnerabilidades em sistemas dependentes de big techs, com downtime potencial de até 21 dias, conforme tendências Veeam.

A decisão do ministro Flávio Dino de invalidar sanções estrangeiras, alinhada à Constituição e LINDB, protege a soberania, mas expõe o risco de isolamento financeiro se bancos globais evitarem transações por sanções secundárias.

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.

Mitos de neutralidade

Casos como o do TPI e do STF expõem uma vulnerabilidade crítica, desafiando a confiança nas promessas de neutralidade das big techs e revelando que soberanias estrangeiras prevalecem, sujeitando dados a riscos imprevisíveis.

Anton Carniaux, Diretor de Assuntos Públicos e Jurídicos da Microsoft França, foi questionado sob juramento pelos senadores em 2025 sobre a possibilidade da entrega de dados franceses ao governo americano sem autorização.

"Eu não posso garantir isso, mas posso dizer que nunca aconteceu antes."
- Disse Carniaux.

Essa admissão fragiliza o mito da neutralidade, especialmente com a escalada de 2025, quando a sede nos EUA acessou dados sem notificar filiais. O risco cresce com tarifas de Trump contra o Brasil por regulação de plataformas, refletindo pressões geopolíticas.

Backups imutáveis Veeam mitigam lock-ins, como destacado em nosso blog sobre Veeam v13. **CLIQUE AQUI para explorar soluções híbridas que protegem contra essas vulnerabilidades.**

Riscos locais: LGPD e outros

A desmistificação da neutralidade das big techs, como visto na declaração na França, revela como a dependência externa agrava riscos locais no Brasil, onde leis como a LGPD demandam controle rigoroso sobre dados, mas colidem com interferências estrangeiras. Essa tensão amplifica vulnerabilidades internas, tornando essencial uma análise dos impactos na conformidade e operações cotidianas:

LGPD e Responsabilidade do Controlador: A lei exige transparência sobre dados armazenados fora do Brasil, responsabilizando o controlador por vazamentos via Cloud Act, com multas que podem atingir milhões de reais.

Interrupções Políticas e Geopolíticas: Tensões EUA-China afetam 80% das exportações brasileiras, gerando sanções secundárias que paralisam serviços, similar aos casos reais discutidos.

Lock-in e Custos Ocultos: Dependência de nuvens estrangeiras eleva custos de saída em até 5 vezes, limitando migrações e ampliando exposições a bloqueios.

Latência e Desempenho: Armazenamento externo pode piorar a latência em até 200ms, impactando eficiência operacional e experiência do usuário.

Shadow IT e Exposições Não Mapeadas: 60% das empresas enfrentam SaaS contratados sem supervisão de TI, aumentando riscos de vazamentos e inconformidades.

Desafios Regulatórios do STF: O STF regula plataformas, mas sanções Magnitsky desafiam isso, como em investigações de práticas comerciais, expondo colisões jurídicas.

Vantagens da Soberania de Dados

Quando a infraestrutura está no país, decisões judiciais ocorrem dentro de um sistema legal conhecido, com jurisdição clara, previsibilidade e direito ao contraditório. Você sabe o que está acontecendo, pode acompanhar de perto e tem meios para reagir, caso ocorra qualquer medida arbitrária.

Além disso, soluções brasileiras já entregam níveis de desempenho e disponibilidade comparáveis aos das big techs internacionais, com menor latência, resposta mais rápida e sem os riscos associados a sanções externas ou conflitos geopolíticos.

Ao centralizar dados no Brasil, sua empresa ganha controle jurídico, estabilidade operacional e proximidade técnica, sem abrir mão de performance.

Segurança jurídica
Conformidade com a legislação Brasileira e menor exposição a conflitos legais internacionais

Desempenho
Menor latência para acessos e melhor experiência para usuários Brasileiros

Disponibilidade
Redução de riscos de interrupção e perdas por fatores geopolíticos

Backup soberano: proteja seus dados nas big techs

Mesmo em plataformas robustas e consolidadas como Salesforce ou Office 365, a sua empresa não tem controle total sobre os dados, principalmente quando eles estão sob jurisdição estrangeira.

Esses serviços podem ser interrompidos por fatores políticos, sanções ou decisões judiciais externas, e o acesso aos seus próprios dados pode ser bloqueado de forma repentina.

Para mitigar esse problema, realizamos backups completos dessas plataformas e os armazenamos em infraestrutura brasileira, com proteção legal, controle local e restauração garantida.

Através de soluções homologadas, como a integração da Veeam com a Microsoft, é possível fazer o download de e-mails, cadastros, contratos e históricos comerciais. Esses dados podem ser restaurados tanto em ambientes Microsoft como em outras soluções compatíveis, com segurança e integridade.

Essa camada de proteção é rápida de implementar e evita perdas operacionais, jurídicas ou comerciais caso haja qualquer interrupção no serviço original.

Você não precisa esperar um desastre ou planejar uma grande migração. Pode começar agora, com uma medida simples, estratégica e soberana.

Estratégias de mitigação e continuidade

Tendo explorado os riscos locais da LGPD e outros desafios internos que se agravam com a falta de soberania, como vazamentos, lock-in e shadow IT, surge a necessidade de estratégias concretas para mitigar esses perigos e garantir a continuidade das operações.

Essas abordagens não apenas neutralizam as vulnerabilidades identificadas nos capítulos anteriores, mas transformam a soberania de dados em uma vantagem competitiva, promovendo resiliência em ambientes híbridos:

Inicie com Assessment Detalhado

Mapeie todos os dados e combata o shadow IT, que afeta 70% das organizações, identificando criticidade via BIA (Business Impact Analysis) para definir RTO (Recovery Time Objective) e RPO (Recovery Point Objective) ideais. Quanto mais crítico for o sistema, menores devem ser o RPO e o RTO.

RTO E **RPO** 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 de E-mail	12 horas	6 horas

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

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.

Adote Soluções Rápidas de Proteção

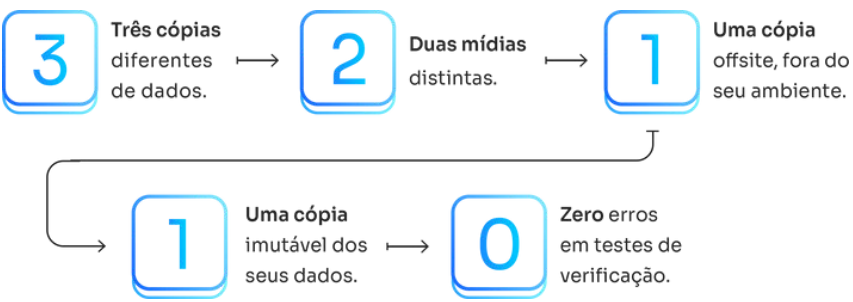
Implemente backups de SaaS, permitindo exportações em horas, e DRaaS para réplica instantânea, reduzindo o impacto de interrupções geopolíticas.

Aproveite Vantagens Locais no Brasil

Priorize segurança jurídica com discussões em jurisdição nacional, disponibilidade de 99.99% e latência abaixo de 50ms, superando limitações de nuvens estrangeiras.

Incorpore Tecnologias Avançadas

Utilize Veeam v13 para simplificar backups híbridos, alinhando à regra **“Golden Rule” 3-2-1-1-0 (3 cópias, 2 mídias diferentes, 1 off-site, 1 imutável, 0 erros)**



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

Realize Testes Periódicos

Evite downtime de 21 dias em sanções, simulando cenários para validar planos e ajustar estratégias, implementando uma rotina de testes regular, que garante a eficácia de seu plano de **Disaster Recovery** diante de qualquer cenário.

Essas medidas, enraizadas nos insights dos capítulos anteriores, convertem ameaças em oportunidades de fortalecimento.

A Solução da Penso

Ampliando as estratégias de mitigação e continuidade apresentadas, a Penso oferece serviços especializados de **Backup e Disaster Recovery** que respondem diretamente aos riscos de sanções e vulnerabilidades, com soluções Veeam que asseguram resiliência.

Análise e Planejamento Inicial

- Realizamos Business Impact Analysis (BIA) para mapear processos críticos, definindo **RTO e RPO** ideais (<15 minutos), como na **recuperação de 70 TB em 10 minutos para a Andra.**

- Desenvolvemos estratégias personalizadas com **Veeam Cloud Connect**, assegurando **conformidade LGPD em multi-cloud contra acessos unilaterais como os do Cloud Act.**

Backup as a Service (BaaS)

- Protege servidores físicos e virtuais **(VMware, Hyper-V, Linux VM), bancos de dados, Microsoft 365, AWS, Azure e Google Cloud com armazenamento imutável.**

- Oferece recuperação granular para restaurar arquivos específicos, reduzindo downtime, **com testes semestrais garantindo integridade.**

- Hospedado em data centers Tier III no Brasil, **com faturamento em real e suporte local,** eliminando riscos cambiais.

Disaster Recovery as a Service (DRaaS)

- Garante continuidade em crises, com restauração em até 30 minutos via replicação de VMs.
- Inclui Infrastructure as a Service (IaaS) para ambientes VMware prontos, minimizando gaps de backup.
- Planos testados e simulações regulares asseguram alta disponibilidade, como destacado em nossa página de DRaaS.

Gestão e Suporte Contínuo

- Realizamos simulações periódicas para validar backups, evitando downtime de 21 dias em crises.
- Oferecemos diagnóstico de vulnerabilidades como lock-in e shadow IT, propondo migrações para Penso Cloud Corporativo.

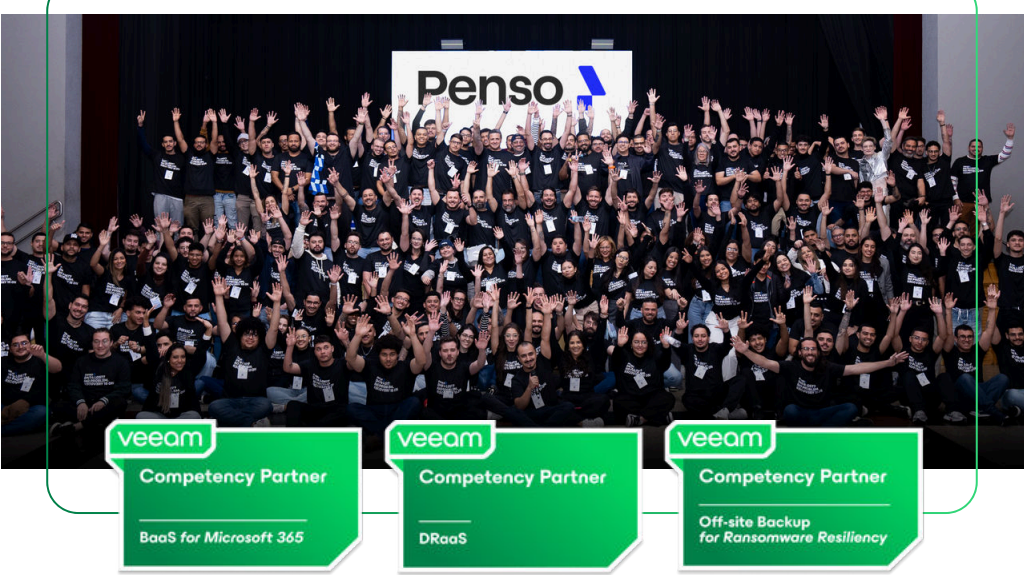
Essas soluções, integradas à Veeam Data Platform, combatem dependências externas e asseguram conformidade LGPD. Acesse nossas páginas de Veeam Backup e DRaaS para detalhes e agende um diagnóstico com nossos especialistas.

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.

Eleita **Provedor do Ano Veeam 2024,** a Penso entrega **DRaaS, backups imutáveis** e conformidade com **LGPD**, recuperando sistemas em horas e protegendo a confiança de 212 milhões de brasileiros.



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

A jornada deste eBook destila uma lição crucial: a soberania de dados no Brasil está sob cerco, com a Lei Magnitsky e o Cloud Act impondo sanções que paralisam operações por semanas e desafiam a LGPD, atingindo 75% das empresas.

Dos fundamentos de autonomia aos alertas dos casos da Nayara, STF e TPI, passando pela desmistificação dos mitos de neutralidade e os riscos locais como lock-in e shadow IT, aprendemos que a dependência de big techs amplifica vulnerabilidades em 200% desde 2024. O insight central é transformador: esses riscos podem se converter em força com resiliência ativa, como backups imutáveis e recuperações em minutos.

O momento de agir é agora, antes que uma interrupção revele sua fragilidade.

Com a Penso, você encontra uma parceira com mais de 22 anos de expertise e certificações ISO-27001, pronta para blindar seus dados e garantir continuidade com soluções testadas.

Soberania de dados no Brasil e a lei Magnitsky

#Obrigado

Apoio: veeam Adistec