Penso

Cibersegurança e Recuperação de Desastres:

Um chamado urgente para proteger os dados do setor público brasileiro

Apoio: veeam Adistec

Introdução

Quando a Cibersegurança se Torna um Pilar da Soberania Digital

Imagine um Brasil onde serviços públicos digitais são impenetráveis, onde cidadãos confiam plenamente em sistemas como o Gov.br e onde **a soberania digital é inabalável**. Esse futuro é possível, mas exige coragem e ação imediata.

Cada ataque evitado representa uma vitória para **212 milhões de brasileiros**. Cada falha ignorada, porém, abre espaço para riscos inaceitáveis que podem comprometer a confiança da população e a integridade do Estado.

Neste eBook, baseado no webinar exclusivo apresentado por Thiago Lima, CEO da Penso, vamos explorar os desafios da cibersegurança no setor público e a importância da **recuperação de desastres como um chamado urgente** para proteger os dados e a soberania do Brasil.

Descubra como blindar o setor público contra ataques cibernéticos.

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 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

Thiago Lima

CEO na Penso

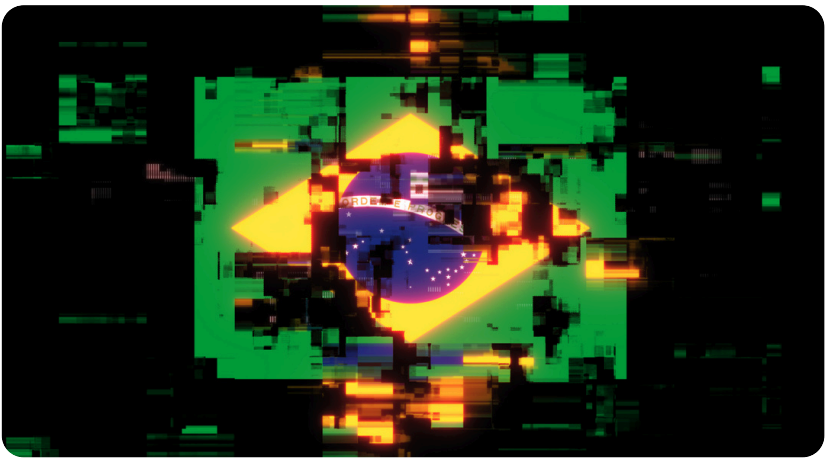
+ 1.600 clientes corporativos ativos

+ 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

O Brasil está sob ataque



Em 2024, o Tribunal de Contas da União (TCU) revelou que o país enfrenta a quarta maior superfície de ataque cibernético do mundo, com **5.302 incidentes de segurança** registrados em órgãos públicos, um **aumento alarmante de 55%** em relação aos 3.402 casos de 2022.

Esses números expõem uma realidade preocupante: a infraestrutura digital brasileira que sustenta serviços essenciais, como Gov.br, folha de pagamento e emissão de documentos, está vulnerável. A ausência de estratégias robustas de **cibersegurança e recuperação de desastres** ameaça a soberania digital do país e a continuidade dos serviços essenciais.

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 cibersegurança com Disaster Recovery, serviços críticos podem parar por semanas.

Por que o setor público está na mira?

O setor público brasileiro é um alvo irresistível para cibercriminosos. Digitalização em larga escala, dados de alto valor, baixo investimento em segurança e ataques movidos por ativismo criam um cenário de risco sem precedentes.

Digitalização: O avanço que virou risco

A transformação digital do Brasil trouxe mudanças impressionantes que também abriram portas para o caos. Com **450 milhões de dispositivos conectados** e 161,6 milhões de brasileiros acessando a internet, serviços como Gov.br, Declaração de Imposto de Renda e emissão de carteiras de identidade dependem de infraestruturas digitais frágeis.

Informações como folhas de pagamento, cadastros de contribuintes ou registros do INSS têm valor inestimável no mercado do cibercrime. Por exemplo, comprometer a base da Fazenda Estadual, com milhões de contribuintes, é infinitamente mais lucrativo do que atacar uma construtora.

Em 2021, por exemplo, um vazamento expôs 220 milhões de CPFs e CNPJs, incluindo nomes, endereços, fotos e números do INSS, com parte dos dados vendidos na dark web. Ataques como esse não buscam apenas lucro: muitos são motivados por ativismo político ou ideológico, mirando a desestabilização de instituições.

Falta de orçamento compromete a segurança dos dados públicos

Processos licitatórios complexos e orçamentos limitados dificultam a adoção de tecnologias modernas. O TCU destaca que, nos últimos quatro anos, os recursos para segurança da informação foram inadequados.

O Brasil é o 7º país mais visado por ransomware globalmente. **Sem investimento, essa posição só piora.**

Enquanto no setor privado, o lucro é o principal motivador para os atacantes, o governo também é visado por criminosos que agem por ativismo político e buscam **desestabilizar as instituições,** interrompendo serviços ou expondo dados sensíveis. Esses ataques amplificam o impacto, **afetando a confiança pública** e a governança.

Exemplo prático:

Ataques DDoS, que somaram **372.825 incidentes** no primeiro semestre de 2024, frequentemente visam paralisar serviços como o SEI ou sistemas de saúde, muitas vezes com motivações políticas ou de protesto.

Por que isso importa? O setor público não pode ser reativo. Digitalização em massa, exposição de dados valiosos, falta de investimento e ativismo criam um risco extremo.

Adesão a práticas básicas de segurança no Brasil

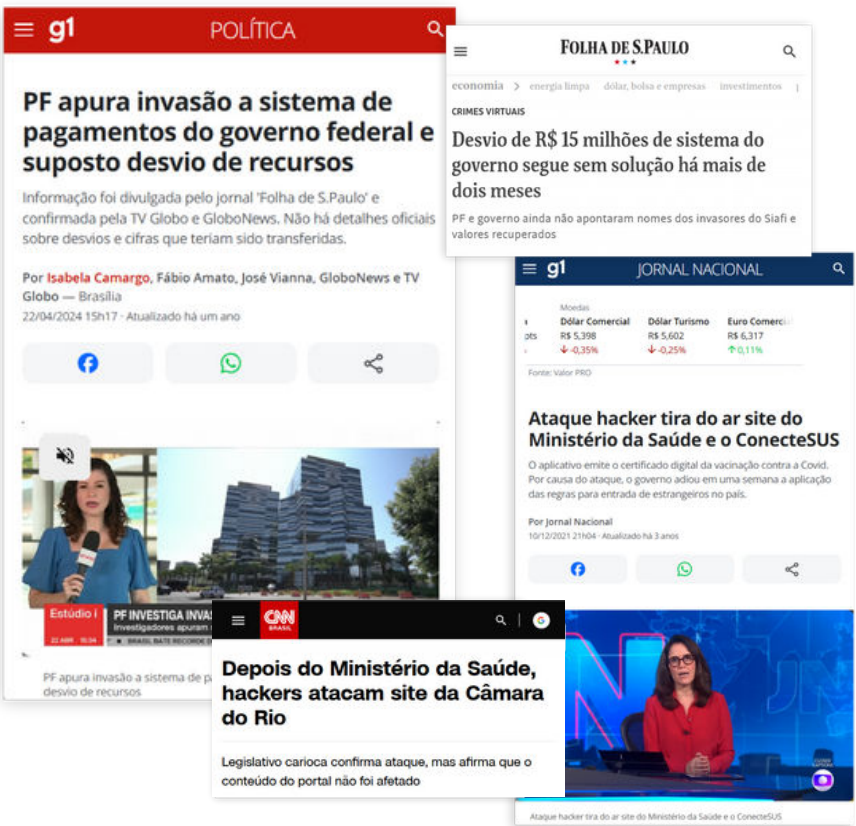
O Tribunal de Contas da União (TCU) aponta que a falta de processos robustos, orçamentos insuficientes e baixa adesão a práticas básicas de segurança criam brechas perigosas.

Com sistemas críticos em risco, a ausência de preparação pode levar a paralisações devastadoras.

Processos de Recuperação Inexistentes

A maioria dos órgãos públicos não está preparada para recuperar dados após um ataque. O TCU revela que **69% dos órgãos auditados não possuem processos claros de recuperação de dados.** Isso significa que, mesmo com backups, não há garantia de restauração rápida ou confiável. Sem um plano testado, sistemas críticos podem ficar fora do ar por semanas, comprometendo serviços essenciais.

Em 2024, ataques como o **desvio de recursos via Siafi** e a **paralisação** da emissão de cartões de vacina contra Covid-19 mostram **o impacto devastador da negligência.**



Relatórios indicam que a recuperação após um ataque leva, em média, 21 dias, afetando serviços críticos e a confiança da população.

Fonte: Veeam Ransomware Trends Report 2023

Negligência em práticas fundamentais

Práticas básicas, como criptografia robusta e autenticação em dois fatores (2FA), são amplamente ignoradas. Muitos órgãos não implementam controles essenciais, como segmentação de redes ou monitoramento contínuo. Essa negligência facilita a ação de criminosos que exploram vulnerabilidades simples, como senhas fracas ou sistemas desatualizados.

Em 2024, por exemplo, o vazamento de dados do INSS expôs informações sensíveis de beneficiários, como números de benefícios e endereços, devido à falta de criptografia adequada. Esses dados alimentaram **atividades criminosas na dark web**, mostrando o custo da inação.

Governança frágil amplifica o problema

A falta de coordenação e governança em cibersegurança é um obstáculo desafiador. A Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto 11.856/2023, é limitada ao Executivo Federal e carece de implementação unificada. Muitos órgãos não possuem equipes dedicadas à segurança ou planos de continuidade de negócios (PCN), deixando a gestão de riscos à deriva.

Enquanto os cibercriminosos utilizam ferramentas avançadas, como inteligência artificial para phishing, os órgãos públicos operam com tecnologias defasadas, ampliando o risco de colapso.

Ransomware: A ameaça que paralisa

O ransomware não é apenas um software malicioso. É uma arma sofisticada que **sequestra dados, paralisa serviços e explora vulnerabilidade**s com precisão cirúrgica.

A Evolução do Ransomware

Diferente dos ataques tradicionais, o ransomware moderno invade sistemas, criptografa dados e exige resgate para liberá-los.

Segundo o Veeam Ransomware Trends Report 2024, 97% dos ataques miram backups antes dos dados de produção.

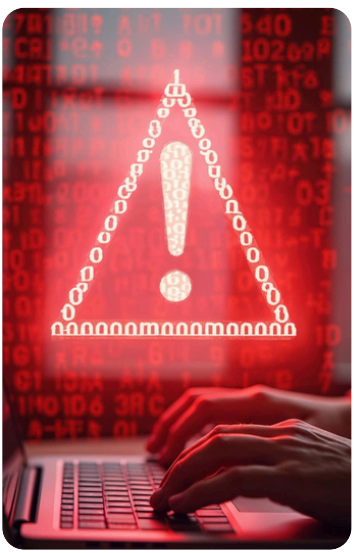
Por quê? Sem backup, a vítima não tem alternativa senão pagar, algo inviável para órgãos públicos devido a restrições legais. Essa tática garante que serviços como SEI, folha de pagamento ou sistemas de saúde fiquem fora do ar por semanas.

Escala e sofisticação no Brasil

O Brasil é um alvo prioritário. Em 2024, 73% das organizações brasileiras sofreram pelo menos um ataque de ransomware, com 1.827 incidentes no último trimestre.

O setor público representa 10,65% das atividades na dark web, onde dados roubados são vendidos. Grupos como LockBit 3.0 e BlackCat utilizam inteligência artificial e técnicas avançadas, como phishing direcionado, para explorar credenciais legítimas, que são a maior porta de entrada para ataques.

A maioria dos ataques de ransomware começa com credenciais legítimas roubadas. Senhas fracas, reutilizadas ou expostas em vazamentos permitem que criminosos acessem sistemas internos sem enfrentar defesas externas. Funcionários clicando em links maliciosos ou usando a mesma senha em redes sociais e sistemas públicos também são portas de entrada fáceis para os atacantes.



Impacto além dos dados

O ransomware não apenas rouba informações, ele paralisa operações. A média de recuperação é de 21 dias, tempo suficiente para interromper serviços essenciais, como emissão de documentos ou acesso a sistemas de saúde. Esses ataques também alimentam a desconfiança pública, minando a credibilidade de instituições e afetando a governança.

Com 16 mil tentativas de ataque na saúde pública em 2024, a paralisação de sistemas médicos pode custar vidas, enquanto ataques financeiros, como o desvio via Siafi, impactam diretamente o orçamento público.

Sem estratégias robustas, como **backups imutáveis e Disaster Recovery,** o setor público enfrenta paralisações que custam caro, em tempo, dinheiro e confiança.

97% dos ataques visam backups

73% das organizações brasileiras foram atingidas

Recuperação de Desastres: A Última Linha de Defesa Contra Ataques

Com ataques cibernéticos cada vez mais sofisticados, o setor público brasileiro não pode depender apenas de defesas tradicionais para proteger serviços essenciais. Enquanto defesas tradicionais e backups falham em ambientes complexos e vulneráveis, o DR assegura continuidade onde outras soluções não chegam.

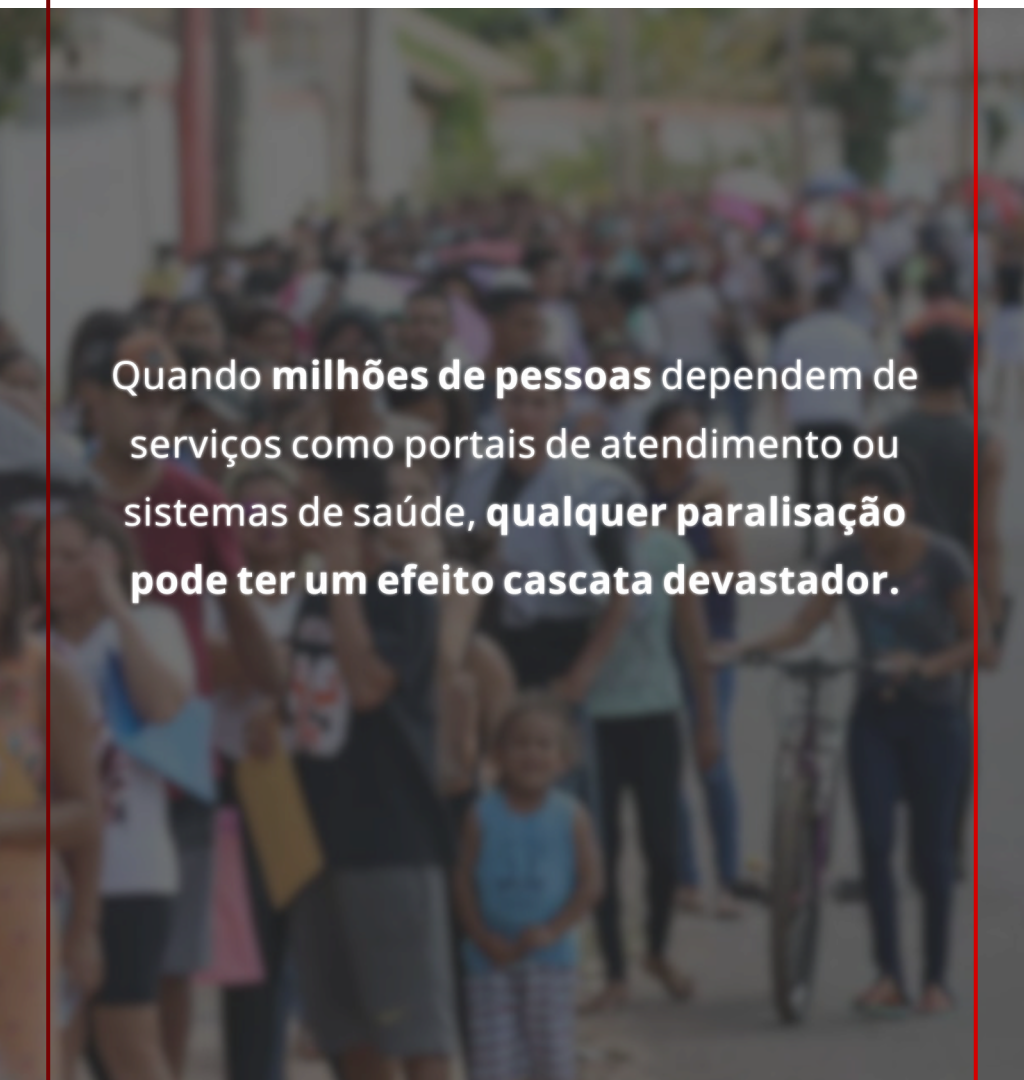
O Disaster Recovery é a barreira final que garante a continuidade de operações críticas, como sistemas de licitação, saúde ou atendimento ao cidadão, em questão de horas.

Ataques sofisticados exploram brechas sutis, como sistemas desatualizados ou configurações erradas, que até as melhores ferramentas não conseguem prever. Em ambientes públicos, onde múltiplas tecnologias coexistem, essas falhas são ainda mais difíceis de evitar.

Diferente de soluções convencionais, o Disaster Recovery enfrenta as complexidades e vulnerabilidades dos ambientes modernos, oferecendo resiliência onde outras barreiras falham.

Sistemas complexos: Um campo minado para a cibersegurança

Os sistemas de TI do setor público são um quebra-cabeça: Linux, Windows, VMware, Hyper-V, roteadores Cisco e Fortinet convivem em redes interconectadas. Essa heterogeneidade complica as atualizações e cria pontos cegos nas interconexões. Um único erro em uma configuração pode expor sistemas críticos, tornando defesas externas insuficientes.


Quando **milhões de pessoas** dependem de serviços como portais de atendimento ou sistemas de saúde, **qualquer paralisação pode ter um efeito cascata devastador.**

Backup vs Disaster Recovery

Backup e Disaster Recovery (DR) são comumente confundidos, mas são soluções complementares com propósitos bem diferentes.

Backup

É um processo de cópia de dados, onde você armazena versões dos dados em um ponto específico no tempo. **O objetivo do backup é ter uma cópia recuperável** caso os dados originais se percam ou se corrompam.

Disaster Recovery

É uma estratégia e um **conjunto de processos e tecnologias que asseguram a continuidade operacional** da infraestrutura de TI. Isso pode envolver, por exemplo, a recuperação de todo o ambiente do ERP, incluindo configurações, customizações, integrações, e não apenas os dados em si.

A diferença crítica entre eles está no objetivo final:

Enquanto o backup é uma solução pontual, o DR garante que o sistema de recuperação seja eficiente e rápido para que a operação não seja interrompida por longos períodos, atendendo aos requisitos de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).

⚠ Nenhuma defesa é infalível

Ferramentas avançadas, como firewalls ou EDRs, falham diante de ameaças sofisticadas e ambientes de TI complexos, que misturam Linux, Windows, VMware e Nutanix.

O TCU destaca que 71,2% dos órgãos com servidores próprios não possuem planos de backup específicos para seus principais sistemas.

Backups são essenciais para salvar dados, mas não asseguram a disponibilidade imediata de serviços. Restaurar um ambiente comprometido pode ser lento, especialmente em sistemas públicos interdependentes.

O Disaster Recovery, por outro lado, replica ambientes inteiros, permitindo que operações voltem em horas, minimizando interrupções. Ou seja, é a solução que garante resiliência onde antivírus, firewalls e backups falham, mantendo o setor público em pé diante de crises.

O Preço da Inação: Riscos que o Brasil Não Pode Ignorar

Cada dia sem investir em cibersegurança e recuperação de desastres expõe serviços essenciais a paralisações, vazamentos e **perdas financeiras que ameaçam milhões de cidadãos** e a soberania digital do país.

Com 1.449 ataques de phishing direcionados ao setor público em 2024, as consequências de ficar parado são devastadoras.

Serviços Interrompidos

Sem estratégias como DR, ataques cibernéticos podem travar serviços críticos, como portais de atendimento, sistemas de educação ou finanças públicas, por semanas. Essas interrupções geram transtornos para milhões de cidadãos, atrasam operações e sobrecarregam equipes de TI despreparadas.

Dados Expostos

Vazamentos de dados corroem a credibilidade do setor público. Em 2024, por exemplo, 309 bancos de dados foram comprometidos, alimentando fraudes na dark web.

Informações sensíveis, como cadastros de benefícios ou dados fiscais, quando expostas, abalam a confiança da população e geram crises de imagem.

Custos Financeiros

A inação drena recursos públicos. Ataques DDoS, que atingiram 4 Tbps em 2024, e **incidentes de ransomware geram perdas bilionárias,** desviando verbas de áreas como saúde e infraestrutura.

Com um orçamento federal de cerca de R$ 5,6 trilhões, cada paralisação ou recuperação lenta representa um custo inaceitável.

Soberania Digital em Risco

A falta de priorização da cibersegurança ameaça a autonomia do Brasil sobre seus dados e serviços. Sistemas vulneráveis abrem portas para interferências externas, comprometendo a governança nacional. O TCU alerta que a inação pode minar a soberania digital, deixando o país refém de criminosos.

Bloqueie brechas com controles essenciais

A**dotar práticas como criptografia robusta, autenticação em dois fatores (2FA) e segmentação de redes é o primeiro passo para proteger dados sensíveis.**

Essas medidas dificultam o acesso de criminosos, especialmente em ataques que exploram senhas fracas ou phishing. Monitoramento contínuo garante que ameaças sejam detectadas antes que causem danos.

Como proteger o futuro digital do Brasil

O Brasil enfrenta uma guerra cibernética, e o setor público está na linha de frente. Com 1.449 ataques de phishing em 2024 e um aumento de 340% em contas violadas, **a cibersegurança é uma necessidade imediata, não uma escolha.** Cada dia sem ação expõe serviços essenciais, como saúde, educação e administração, a riscos que podem custar bilhões.

Disaster Recovery é a única saída

O Disaster Recovery é a chave para manter serviços no ar após ataques ou falhas. Um plano robusto, com testes regulares e um **Plano de Continuidade de Negócios (PCN),** reduz o tempo de inatividade e assegura conformidade com as exigências do **TCU e da PNCiber.**

Como o DR moderno transforma a resiliência de dados

No passado, o DR exigia investimentos pesados: data centers duplicados, hardware idêntico e licenças triplicadas, com custos médios de 1,7x o ambiente principal.

Cada sistema como SEI ou folha de pagamento, precisava de uma solução específica, tornando a gestão um pesadelo. Órgãos públicos, com orçamentos apertados, raramente podiam arcar com isso.

Longe das soluções caras e complexas, o Disaster Recovery moderno é acessível, eficiente e indispensável.

Com tecnologias como **snapshots, multi-cloud e isolamento seguro,** ele garante que serviços essenciais, como sistemas de educação, transporte ou atendimento ao cidadão, voltem ao ar em horas, não semanas.

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.

Sua parceira na Resiliência Digital

A Penso Tecnologia, eleita Provedor de Serviços do Ano pela Veeam em 2024, oferece o Disaster Recovery as a Service (DRaaS), uma solução sob medida para o setor público.

Backups Imutáveis

Nossos backups imutáveis protegem contra exclusão maliciosa, incluindo dados do Office 365, que muitas vezes ficam desprotegidos. Armazenados em cinco data centers Tier III no Brasil, com tecnologia S3, garantimos segurança e acessibilidade. Além disso, monitoramos rotinas e corrigimos falhas, eliminando preocupações para sua equipe.

Disaster Recovery as a Services (DRaaS)

O Disaster Recovery as a Service (DRaaS) da Penso replica sistemas críticos para a nuvem, garantindo recuperação em horas. Nosso processo começa com um dimensionamento simplificado, mapeando servidores e armazenamento, seguido pela criação de um Plano de Continuidade de Negócios (PCN) assinado por TI e gestores. Testes semestrais com usuários reais asseguram que tudo funciona, com ativação prevista de 7 dias por ano para testes ou crises.

Conformidade com TCU e PNCiber

Nossas soluções atendem às exigências do TCU e da Política Nacional de Cibersegurança (PNCiber, Decreto 11.856/2023). Nosso health check baseado no padrão NIST identifica vulnerabilidades, fortalecendo a segurança.

Com certificações ISO 27001 e competências Veeam em DR, backup offsite e Office 365, garantimos que órgãos públicos passem em auditorias e evitem sanções.

Suporte e flexibilidade para todos os tamanhos de negócios

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 do setor público?

- ✓ 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

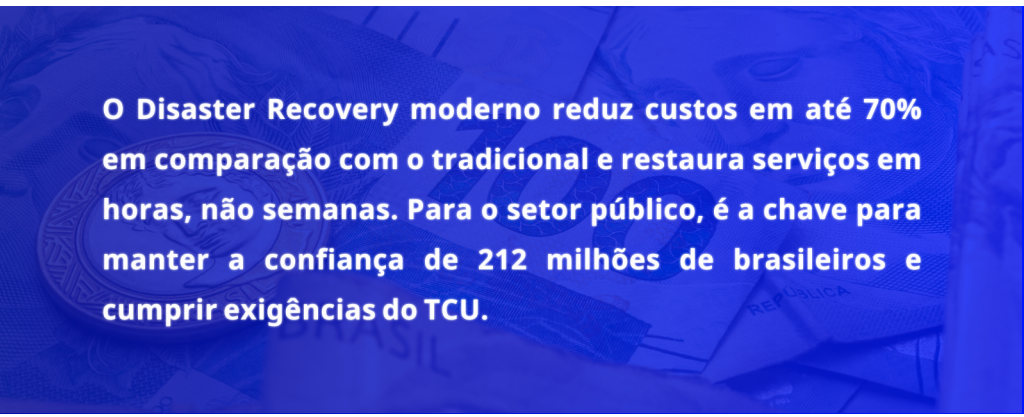
Estratégia de Resiliência de Dados

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.

Gestão centralizada e simplificada

Diferente do DR tradicional, que exigia gerenciamento sistema por sistema, o DR moderno usa painéis centralizados para monitorar replicações. Testes semestrais, com participação de TI e usuários, garantem que tudo funcione. Isso reduz custos operacionais para cerca de 0,6x o ambiente principal.

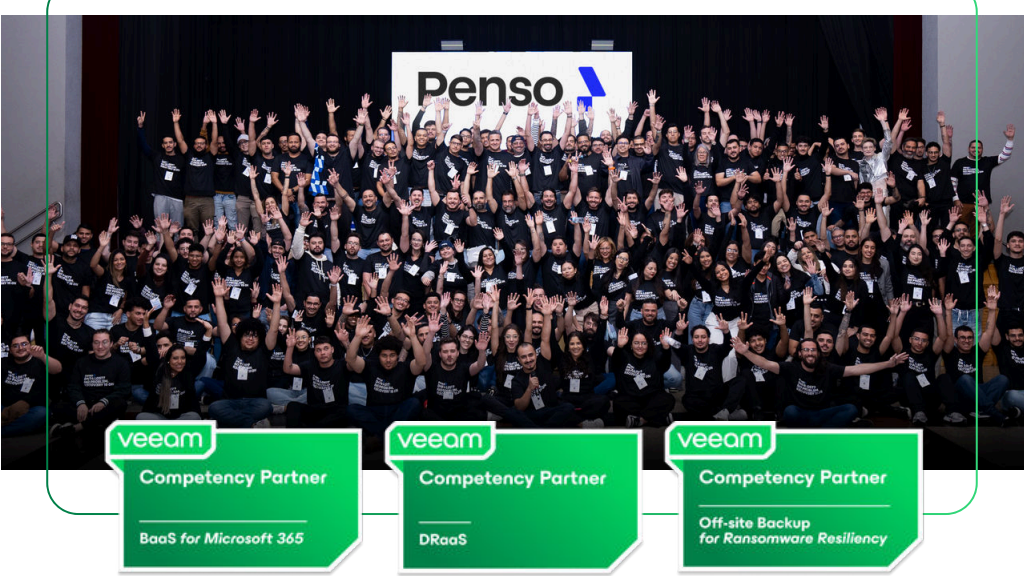


Experiência comprovada

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 TCU e PNCiber, 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

O cenário de ameaças é claro: o setor público brasileiro está sob constante ataque, e a continuidade dos serviços que sustentam milhões de cidadãos depende de escolhas feitas hoje. Vazamentos, paralisações e prejuízos bilionários já não são hipóteses. São realidades que comprometem a confiança da população e a soberania digital do país.

Investir em práticas de segurança, adotar controles básicos e implementar estratégias modernas de Disaster Recovery não é apenas uma medida técnica, mas um compromisso com a cidadania. Cada órgão que se prepara reduz não só o risco de interrupções, mas garante a preservação da credibilidade das instituições.

O futuro digital do Brasil será definido pela capacidade de proteger e recuperar seus sistemas diante de crises. Com parceiros especializados, como a Penso, o setor público pode transformar vulnerabilidade em resiliência e assegurar que os serviços essenciais permaneçam disponíveis, mesmo diante das ameaças mais sofisticadas.

Penso

Cibersegurança e Recuperação de Desastres:

Um chamado urgente para proteger os dados do setor público brasileiro

#Obrigado

Apoio: veeam Adistec