Penso

Disaster Recovery:

a única defesa contra ransomware

Apoio: veeam Adistec

Introdução

Nos últimos anos, o avanço dos ataques cibernéticos mostrou que nenhuma empresa está imune. Organizações de todos os portes, segmentos e estruturas passaram a enfrentar ameaças antes restritas a grandes corporações.

Neste cenário, o backup deixou de ser um diferencial e passou a ser o mínimo. O que define o futuro de uma empresa diante de um desastre é sua capacidade de reagir com rapidez, segurança e previsibilidade.

E é exatamente sobre isso que trata este e-book: como o **Disaster Recovery (DR)** evoluiu para se tornar a última linha de defesa das organizações, e por que ele é essencial para a continuidade dos negócios. Ao longo das próximas páginas, vamos desmistificar conceitos, expor os riscos atuais, apresentar soluções acessíveis e mostrar como a Penso, em parceria com a Veeam, entrega proteção real aos dados corporativos.

Além deste material que você tem agora em mãos, a Penso promoveu o webinar **"Disaster Recovery: A Única Garantia Real Contra Ransomware"**, no qual esse tema foi abordado com profundidade. Este e-book é baseado nos insights do evento, trazendo aqui seus direcionamentos técnicos e estratégicos.

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

O cenário atual de ameaças e por que o backup tradicional não basta

Vivemos em uma economia 100% digitalizada. Não importa o porte ou o setor da empresa, todos os negócios dependem de tecnologia para funcionar: do faturamento ao atendimento ao cliente. Até operações remotas e tradicionais, como a de um canoeiro numa vila de pescadores isolada, hoje dependem de celular, internet e PIX para receber pagamentos.

Nesse contexto, a perda de acesso a sistemas ou dados pode significar, literalmente, parar de operar. E os riscos são globais: **ataques cibernéticos atingem empresas de todos os tamanhos, setores e países.** O Brasil figura entre os dez países mais visados do mundo, segundo dados da CrowdStrike.

O ransomware, hoje um negócio bilionário, é a maior ameaça. Ele não escolhe vítimas, atinge desde hospitais até pequenas empresas e cresce tanto em ambientes locais quanto em nuvens públicas. Os ataques nessas plataformas aumentaram 110% entre 2023 e 2024, criando um panorama alarmante.

O impacto não é só financeiro: reputação, conformidade e até a sobrevivência da empresa ficam em jogo.

O impacto do ransomware: uma ameaça silenciosa

O ransomware deixou de ser um ataque isolado para se tornar uma indústria bilionária do crime digital. Hoje, grupos organizados operam como verdadeiras empresas clandestinas, explorando vulnerabilidades com precisão e paralisando serviços críticos em questão de horas.

Para compreender como chegamos ao cenário atual, é fundamental observar a evolução dessa prática criminosa ao longo da última década:

2010

Popularização do **Bitcoin** cria um meio de pagamento **anônimo e global,** abrindo caminho para extorsões digitais.

2013

Surge o **Cryptolocker**, combinando criptografia avançada e pagamento em Bitcoin.

2016

Aparece o modelo de **Ransomware as a Service (RaaS),** permitindo que grupos desenvolvam ferramentas e as "aluguem" para outros criminosos.

2020

O ransomware se torna a maior ameaça tecnológica global, com plataformas como **LockBit** liderando o mercado criminoso.

Backup ≠ Continuidade: os mitos que colocam empresas em risco

Um dos maiores enganos é achar que ter backup garante continuidade. **Na prática:**

97%
dos ataques visam atingir os backups

75%
conseguiram comprometer pelo menos um repositório

Mesmo backups bem protegidos podem falhar em um ponto crítico: a velocidade. Restaurar um ambiente inteiro pode ser um processo lento e doloroso, incapaz de acompanhar a urgência de serviços que não podem parar.

Backup serve para recuperar dados. Continuidade exige restaurar rapidamente sistemas e serviços: algo que só um plano de Disaster Recovery (DR) bem estruturado entrega.

O tempo médio de
recuperação após um ataque é de

21 DIAS

504 horas | **30.240 min.** | **15 dias úteis**

De acordo com o Veeam Ransomware Trends Report 2023, organizações levam em média 3,4 semanas para restaurar totalmente seus ambientes após um ataque. Esse intervalo pode ser devastador para serviços públicos e empresas que dependem de disponibilidade contínua.

Disaster Recovery é a última linha de defesa

Nenhuma infraestrutura é impenetrável. Ransomware, falhas de configuração e credenciais comprometidas conseguem ultrapassar até as defesas mais avançadas. Em ambientes corporativos heterogêneos, que combinam nuvem, data centers e aplicações críticas, cada vulnerabilidade se transforma em um ponto de entrada.

O backup, embora essencial, resolve apenas parte do problema: garante os dados, mas não a continuidade. Restaurar sistemas inteiros a partir de backups pode levar dias ou até semanas, tempo em que operações ficam paradas, clientes desassistidos e perdas financeiras se acumulam.

O Disaster Recovery (DR) é o elo que transforma o caos em retomada. Ao replicar ambientes completos e garantir que aplicações críticas voltem ao ar em horas, o DR protege receita, reputação e continuidade do negócio.

O que diferencia uma empresa resiliente de uma vulnerável?

Resiliência não é sobre ter mais tecnologia, é sobre ter o plano certo.

Empresas resilientes:

Assumem que serão atacadas e planejam a resposta.

Segmentam prioridades com base em análise de **impacto no negócio (BIA).**

Testam o plano periodicamente, **corrigindo falhas** e ajustando ao ambiente atual.

Contam com **parceiros especializados** para suporte no momento crítico.

A vulnerabilidade, por outro lado, nasce da falsa sensação de segurança, de confiar apenas no backup ou em soluções de proteção de borda.

Como saber se sua empresa está preparada para um desastre?

Algumas perguntas-chave ajudam a medir a prontidão:

- **Qual o tempo máximo que cada sistema pode ficar indisponível (RTO)?**
- **Qual a perda máxima aceitável de dados (RPO)?**
- **Há um plano de continuidade documentado e validado com as áreas de negócio?**
- **Os testes de recuperação são realizados com que frequência?**
- **Há recursos humanos e técnicos preparados para execução em caso real?**

Se as respostas não forem claras, rápidas e baseadas em evidências de testes, a empresa provavelmente não está preparada.

Mesmo com firewalls, EDRs, backups e políticas de segurança bem estabelecidas, sempre haverá brechas: sejam técnicas, humanas ou operacionais. Por isso, o Disaster Recovery se torna a última linha de defesa.

Mas, para funcionar de verdade, o DR precisa sair do papel. Precisa ser planejado, implementado, testado e operado com excelência. E é justamente nesse ponto que a Penso se diferencia, entregando não apenas uma infraestrutura robusta, mas um modelo de serviço orientado a resultados.

Por dentro de uma operação de Disaster Recovery moderna

O DR moderno é muito mais acessível e eficiente que o tradicional. Entre as principais diferenças:

Localização – antes exigia dois data centers físicos; hoje pode rodar em nuvem sob demanda.

Hardware e software – no passado, exigia duplicação de servidores e licenças; hoje, licenças podem ser reaproveitadas, e a infraestrutura é elástica.

Gestão – de replicações manuais por serviço para rotinas automatizadas e monitoradas centralmente.

Custo – caiu de 170% do custo do ambiente principal para algo em torno de 60% ou menos.

O DR moderno combina snapshots frequentes, ambientes isolados, versões históricas, detecção de ameaças e integração multicloud. Mais do que tecnologia, envolve processos: implementação, testes semestrais, atualização contínua e suporte especializado.

Como a Penso entrega Disaster Recovery como serviço

Na prática, garantir a continuidade dos negócios em meio a desastres exige mais do que tecnologia: exige experiência, estrutura e responsabilidade. É exatamente isso que a Penso entrega com os planos de Disaster Recovery como Serviço (DRaaS), combinando a plataforma premiada da Veeam com uma operação local altamente especializada.

> ***A gente acredita que proteger o dado é o mínimo. O que a empresa realmente precisa é garantir que o negócio continue, mesmo sob ataque.***
>
> *Thiago Madeira de Lima*

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 seu negócio:

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.

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.

RPO e RTO: Parte essencial do DR

- **Plano de Disaster Recovery:** Define tempos de recuperação (RTO) e pontos de recuperação (RPO) para sistemas críticos, negociando com o 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

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.

Estratégia de Resiliência de Dados

- **Políticas de Backup:** 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.

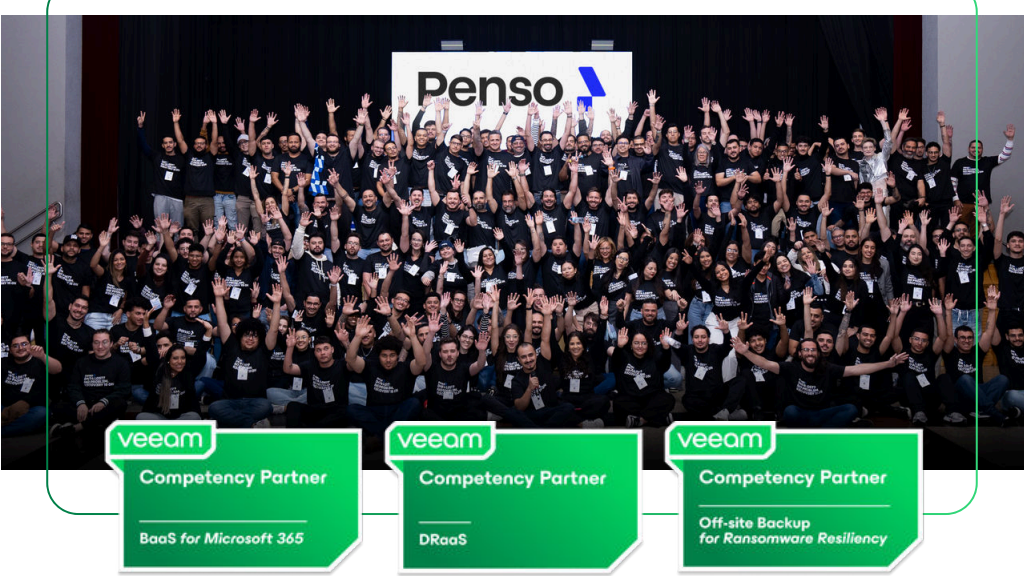
Se você deseja se aprofundar na Regra 3-2-1-1-0, acesse o conteúdo completo no nosso blog.

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 e backups imutáveis, recuperando sistemas em horas e evitando prejuízos e paralisações.



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

Vivemos em um cenário onde a digitalização deixou de ser uma vantagem competitiva para se tornar uma condição básica de existência. Não importa o tamanho da empresa ou o setor em que atua, todos os negócios hoje são, de alguma forma, digitais. E, portanto, todos estão expostos aos riscos cibernéticos, especialmente ao ransomware.

> ***A pergunta não é mais se você será atacado, mas quando. E, principalmente, o que fará quando isso acontecer.***
>
> *Thiago Madeira de Lima*

Se você chegou até aqui, provavelmente já entendeu: **resiliência é questão de estratégia.**

E, quando o assunto é continuidade de negócios, **escolher o parceiro certo faz toda a diferença**.

Penso

Disaster Recovery:

a única defesa contra ransomware

#Obrigado

Apoio: veeam Adistec