Penso

Disaster Recovery para sistemas TOTVS

Seu sistema está realmente protegido por uma **estratégia sólida** de Disaster Recovery?

Segunda-feira, 7h30 da manhã.

Tudo indica que será mais um dia produtivo.

Enquanto você toma seu café e revisa mentalmente os compromissos, **o telefone toca. Do outro lado da linha, alguém do time de infraestrutura. A voz vem tensa:**

Você respira aliviado, mas
a má notícia vem em seguida:

“A PREVISÃO DE RECUPERAÇÃO É DE SETE DIAS...”

Introdução

Milhares de empresas estruturam operações inteiras em torno do ambiente TOTVS. Ainda assim, é comum que equipes de TI e cibersegurança tenham dúvidas críticas sobre responsabilidades de backup, continuidade e recuperação. **Em muitos casos, essas perguntas só surgem quando já é tarde demais.**

Este conteúdo foi criado para ajudar você a tomar decisões com clareza, antes que um incidente coloque seu ambiente em risco. Reunimos, em um só lugar, os principais pontos que devem ser avaliados em planos de Disaster Recovery para ambientes TOTVS, com explicações técnicas, riscos comuns e alternativas viáveis para resposta rápida diante de cenários críticos.

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

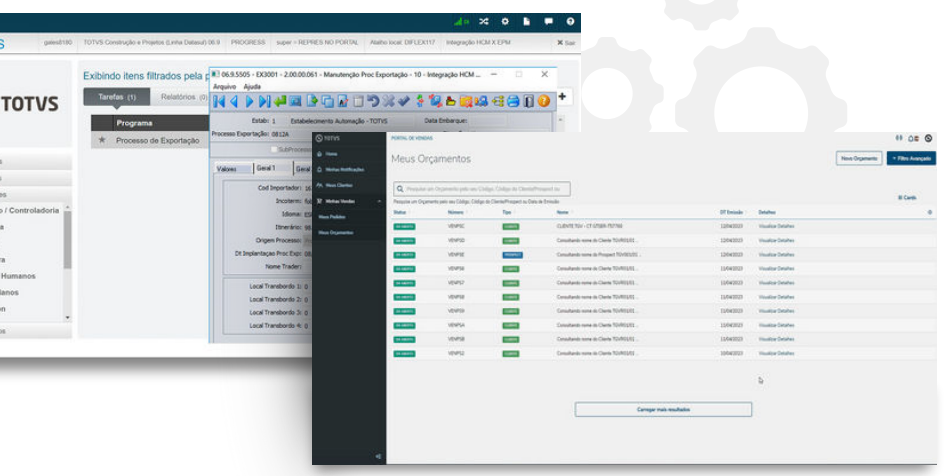
veeam
Competency Partner
DRaaS
BaaS *for 365*
Off-site Backup

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

Entenda a diferença entre Backup e Disaster Recovery

É comum ouvir frases como “temos backup, então estamos protegidos”. Mas será que isso basta?

Essa é uma das confusões mais recorrentes quando se fala em continuidade de operação. Backup e Disaster Recovery são conceitos complementares, mas completamente diferentes em objetivo, escopo e resultado.

Entender essa diferença é essencial, e pode definir a continuidade da sua empresa.

Backup é como um cofre. Ele guarda dados.

Você pode recuperar um arquivo perdido, uma base apagada ou mesmo reconstituir documentos de anos atrás. Mas cofres não garantem funcionamento. **Eles protegem a memória, não a operação.**

Backup:

- **Objetivo:** Preservar dados específicos (arquivos, bancos de dados).
- **Escopo:** Focado em dados individuais, como uma pasta ou um banco.
- **RTO (Recovery Time Objective):** Alto, geralmente dias (ex.: restaurar 10 TB pode levar 1-3 dias).
- **RPO (Recovery Point Objective):** Perda de dados entre o último backup e a falha (ex.: 8 horas se o backup roda à meia-noite e a falha ocorre às 8h).
- **Retenção:** Múltiplas versões, armazenáveis por anos.

Disaster Recovery (DR) é o plano de ação.

É o motor reserva. É a estrutura que permite manter o negócio funcionando, mesmo quando tudo dá errado.

proteger o negócio vai além de ter uma cópia. É saber, com precisão, em quanto tempo você volta ao ar. E quanto de dado você está disposto a perder.

DR Disaster Recovery:

- **Objetivo:** Garantir a continuidade operacional de sistemas inteiros, como o TOTVS.
- **Escopo:** Abrange sistemas completos, incluindo servidores e aplicações.
- **RTO (Recovery Time Objective):** Baixo, geralmente minutos ou poucas horas.
- **RPO (Recovery Point Objective):** Perda mínima, com replicação em tempo real ou em janelas curtas (ex.: 15 minutos).
- **Retenção:** Poucas versões, geralmente até sete dias, dependendo da estratégia (replicação ou snapshots).

Os riscos reais que paralisam empresas

Você pode ter firewalls de ponta. Equipes treinadas. Infraestrutura robusta. E mesmo assim, ficar sete dias parado.

É assim que desastres reais acontecem. Sem aviso. A causa do problema pode ser um erro humano, um disco queimado, uma enchente ou até mesmo um botão clicado por engano.

A seguir, veja alguns riscos que toda empresa conectada ao TOTVS deveria considerar com seriedade:

Falha de hardware (ainda acontece)

Em 2025, uma falha em um simples switch foi suficiente para paralisar o Banco Central Europeu e interromper trilhões de euros em transações. Nenhum ataque. Nenhum vazamento. Apenas um componente de rede que parou de funcionar, e levou com ele um dos sistemas financeiros mais estruturados do mundo.

O hardware evoluiu, mas não é infalível. E, quando o ambiente depende de disponibilidade contínua, uma única falha física pode ser o suficiente para interromper tudo.

Casos como esse mostram que indisponibilidade não depende de ameaças externas. Muitas vezes, começa dentro da infraestrutura — em pontos que pareciam sob controle.

Ataques cibernéticos

A **Braspress,** uma das maiores transportadoras do Brasil, teve sua operação paralisada por sete dias após um ataque ransomware. Isso já seria grave o suficiente. Mas o mais alarmante é que, segundo pesquisas de mercado, a média de tempo para recuperação completa após um ataque como esse é de 21 dias.

Os ataques são silenciosos, rápidos e altamente destrutivos. Um simples clique pode comprometer seu ambiente TOTVS inteiro. E, ao contrário do que muitos pensam, ter backup não é o suficiente. É preciso ter um plano de ação. E ele precisa funcionar.

Eventos climáticos e desastres naturais

A enchente que atingiu o Rio Grande do Sul em 2024 causou a paralisação de centenas de empresas. Data centers foram alagados. Ambientes inteiros ficaram inacessíveis.

Em paralelo, o incêndio ocorrido na Equinix SP4, um dos maiores data centers do Brasil, exigiu o desligamento de parte da infraestrutura por medida de segurança.

Segundo dados da Data Center Dynamics, um data center médio sofre ao menos uma paralisação a cada oito anos. Isso não significa que falhas são frequentes, mas sim que não podem ser descartadas.

Se o seu ambiente de produção está localizado em apenas um local, o risco de indisponibilidade existe — mesmo que a estrutura física seja considerada de alto padrão.

Erro humano: ainda é uma causa recorrente de paralisação

O Google Cloud apagou acidentalmente a conta de um fundo de pensão de **R$ 125 bilhões por falha operacional.** A empresa só conseguiu se recuperar porque um backup externo havia sido feito manualmente por um administrador.

Esse tipo de ocorrência não depende de tecnologia ultrapassada ou falta de investimento. Erros acontecem mesmo em empresas que operam com padrões de excelência.

O problema está na ausência de plano. Quando não existe um processo formal para lidar com falhas humanas, elas tendem a se multiplicar em momentos de crise.

Google Cloud accidentally dele

business-standard.com/world-news/google-cloud-accidentally-deletes-1...

BS LAR NOTÍCIAS DO MUNDO E-PAPER DECODIFICADO OPINIÃO NOTÍCIAS DA ÍNDIA ÚLTIMAS NOTÍCIAS Inscrever-se

Página inicial / Notícias do mundo / Google Cloud apaga acidentalmente US$ 125 bilhões de fundo de pensão australiano

Google Cloud apaga acidentalmente fundo de pensão australiano de US$ 125 bilhões

A 'configuração incorreta única' afetou mais de meio milhão de membros que não conseguiram acessar suas contas de pensão por uma semana

Mais de meio milhão de membros do UniSuper não conseguiram acessar suas contas depois que o Google Cloud acidentalmente excluiu a conta de nuvem privada do fundo de pensão australiano no valor de US$ 125 bilhões.

A interrupção de uma semana resultou em frustração e preocupação generalizadas. Embora o restabelecimento do serviço tenha começado na quinta-feira, pode levar algum tempo para que os saldos de investimento reflitam os números precisos.

A UniSuper, uma importante empresa do setor de previdência complementar da Austrália, atende às necessidades de poupança para a aposentadoria de funcionários do ensino superior e de pesquisa. A interrupção, que afetou funcionários de universidades, faculdades e instituições de pesquisa, teve origem em uma configuração incorreta específica no Google Cloud.

Sem um plano funcional, qualquer interrupção pode se tornar uma crise maior do que precisa ser.

Esses riscos vão muito além da teoria. Eles foram registrados, documentados e publicados por grandes veículos. A maioria das empresas que sofre interrupções longas não foi pega de surpresa por ameaças inéditas. Foi surpreendida pela ausência de preparo.

Por isso, quando falamos de planos de **Disaster Recovery,** não estamos propondo proteção contra o improvável. Estamos falando sobre responder rapidamente ao inevitável.

O impacto financeiro da paralisação

Sete dias de paralisação representam 1,92% do ano.

esse tempo parado pode consumir até

18,5% do lucro anual.

*Em empresas com margens líquidas próximas da média brasileira — 10,43%, segundo a B3

Essa conta considera um cenário regular. Em datas-chave, como Dia das Mães ou Black Friday, o volume de vendas pode ser duas a três vezes maior que a média semanal. Nesses casos, a perda se torna ainda mais difícil de recuperar.

O prejuízo também atinge comissões, metas de trimestre, repasses e contratos com cláusulas de performance. O impacto se espalha pela operação.

Mesmo após a retomada dos sistemas, a empresa leva semanas para restabelecer ritmo, fluxo de caixa e previsibilidade. Uma semana fora do ar não afeta só o mês. Desregula o ano inteiro.

Consequências de uma falha

Sete dias fora do ar são suficientes para comprometer o lucro do ano, expor a empresa a sanções, abalar relações comerciais e desorganizar times inteiros.

Enquanto a equipe tenta restaurar sistemas, vendas são perdidas, pedidos não saem, notas não são emitidas e prazos deixam de ser cumpridos. O prejuízo financeiro cresce a cada hora, e a capacidade de reação diminui cada vez mais, criando uma verdadeira bola de neve.

A confiança de clientes e parceiros começa a enfraquecer

Durante a paralisação, a empresa deixa de entregar, perde prazos e falha em obrigações básicas. Mesmo após a retomada, a percepção de instabilidade já está instalada.

Em cadeias de fornecimento sensíveis, isso costuma resultar em rebaixamento de prioridade ou substituição por fornecedores mais confiáveis. A operação continua, mas com menos espaço e mais exigências.

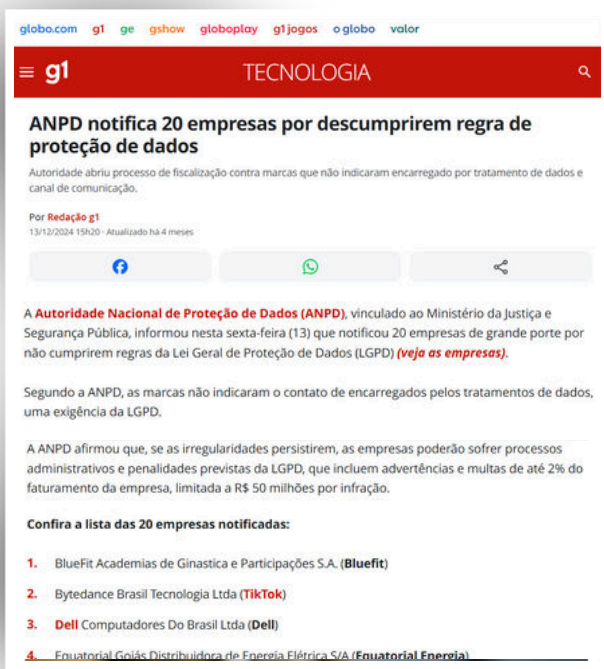
Reconquistar essa posição pode levar meses. Em muitos casos, não há segunda chance.

Órgãos reguladores exigem continuidade. E aplicam sanções quando ela falha.

Empresas que não conseguem emitir nota fiscal no momento da venda estão sujeitas a multas da Secretaria da Fazenda.

Se houver vazamento ou indisponibilidade de dados pessoais, a LGPD também impõe sanções. **A ANPD já começou a aplicar penalidades em casos de falhas não tratadas adequadamente.**

Durante auditorias, o que se espera é a apresentação de evidências: plano de contingência formal, testes realizados, métricas aferidas. Sem esses elementos, a empresa assume o risco por omissão.



globo.com g1 ge gshow globoplay g1 jogos o globo valor

≡ g1 TECNOLOGIA

ANPD notifica 20 empresas por descumprirem regra de proteção de dados

Autoridade abriu processo de fiscalização contra marcas que não indicaram encarregado por tratamento de dados e canal de comunicação.

Por Redação g1
13/12/2024 15h20 · Atualizado há 4 meses

A **Autoridade Nacional de Proteção de Dados (ANPD)**, vinculado ao Ministério da Justiça e Segurança Pública, informou nesta sexta-feira (13) que notificou 20 empresas de grande porte por não cumprirem regras da Lei Geral de Proteção de Dados (LGPD) ***(veja as empresas)***.

Segundo a ANPD, as marcas não indicaram o contato de encarregados pelos tratamentos de dados, uma exigência da LGPD.

A ANPD afirmou que, se as irregularidades persistirem, as empresas poderão sofrer processos administrativos e penalidades previstas da LGPD, que incluem advertências e multas de até 2% do faturamento da empresa, limitada a R$ 50 milhões por infração.

Confira a lista das 20 empresas notificadas:

1. BlueFit Academias de Ginastica e Participações S.A. (**Bluefit**)
2. Bytedance Brasil Tecnologia Ltda (**TikTok**)
3. **Dell** Computadores Do Brasil Ltda (**Dell**)
4. Equatorial Goiás Distribuidora de Energia Elétrica S/A (**Equatorial Energia**)

A crise operacional se transforma em desgaste interno

Enquanto os sistemas estão fora do ar, a TI opera sob pressão máxima. Além das tarefas técnicas, a equipe precisa lidar com cobranças da diretoria, respostas a usuários e suporte a outras áreas da empresa.

A consequência costuma ser o desgaste extremo. Após incidentes como esse, é comum que a rotatividade na área de tecnologia aumente, especialmente entre os profissionais mais experientes.

É comum que colaboradores impactados por esse tipo de incidente deixem a empresa em até 12 meses após a falha.

As demais áreas também sofrem. Vendas param, atendimento falha, metas são comprometidas. Isso gera frustração, sobrecarga e retração de desempenho, mesmo após a retomada.

Recuperar é sempre mais caro do que prevenir

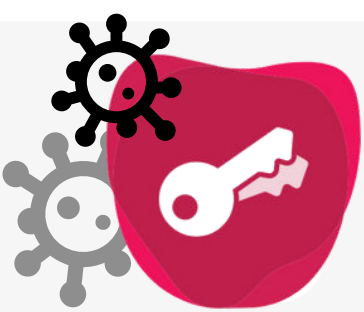
Quando a operação volta, o problema não está resolvido. O tempo perdido precisa ser compensado, a imagem reconstruída, os clientes reengajados e os processos reorganizados.

Toda paralisação impõe uma dívida operacional que se acumula rapidamente. E quanto mais tempo demora para ser contida, maior ela se torna.

Como ataques ransomware comprometem o ambiente TOTVS

Ambientes baseados em TOTVS não estão imunes a ataques ransomware. Pelo contrário: a alta concentração de dados financeiros, fiscais, operacionais e de RH torna o sistema um alvo frequente. Quando comprometido, o impacto vai muito além da indisponibilidade: envolve paralisação de faturamento, perda de produtividade, risco regulatório e quebra de confiança com parceiros.

A seguir, alguns tipos de ataque comuns que afetam diretamente a integridade e a continuidade do sistema:



Criptografia da base de dados (SQL Server, Oracle, etc.):

Criminosos ganham acesso à infraestrutura e criptografam os bancos que alimentam o TOTVS. O sistema pode até abrir, mas não processa, consulta ou grava informações, tornando o ERP completamente inoperante.

Sequestro dos arquivos de aplicação e parametrização:

Arquivos essenciais do Protheus, RM ou Datasul são criptografados ou corrompidos. Mesmo com a estrutura de banco preservada, o ambiente não inicializa ou apresenta erros em série.

Contaminação de servidores de aplicação (ex: appserver, license server):

Serviços responsáveis pela lógica de negócio ou licenciamento são paralisados. Nesses casos, o sistema pode parecer disponível, mas usuários não conseguem autenticar ou realizar transações.

Ataques em cadeia com movimentação lateral

O ransomware se espalha dentro da rede, comprometendo servidores de TOTVS e sistemas integrados, como TEF, BI ou emissão fiscal. Isso causa falhas em processos interdependentes e impede a retomada da operação de forma isolada.

Corrupção de dados críticos após execução silenciosa

Alguns ataques permanecem ativos por dias antes da criptografia. Durante esse período, registros são alterados ou excluídos silenciosamente. Mesmo que o backup seja restaurado, há risco de inconsistência ou perda de integridade.

Como a Penso entrega Disaster Recovery de verdade

Benefícios do Nosso Serviço

2. **Testes Periódicos:**

Realizamos testes semestrais (ou mensais/trimestrais, se necessário) para validar o RTO e RPO, envolvendo usuários de negócios para garantir a funcionalidade completa.

3. **Certificação ISO 27001:**

Nossa operação é certificada, assegurando segurança e conformidade.

4. **Plano de Continuidade de Negócios (PCN):**

Elaboramos um PCN detalhado, com processos, políticas, escalations e métricas, impresso para uso em emergências, garantindo execução por qualquer equipe.

5. **Monitoramento ativo e suporte**

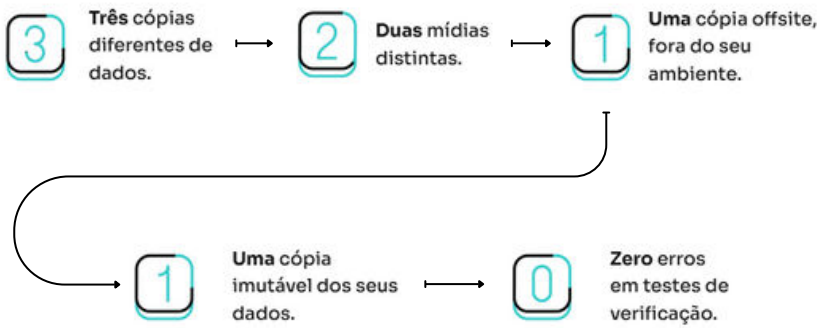
A equipe da Penso monitora o ambiente de DR em tempo integral. O cliente não precisa operar nem gerenciar a replicação. A estrutura já está pronta para responder quando necessário.

6. **Acesso garantido**

Incluímos até sete dias por ano de uso das máquinas no DR sem custo adicional, seja para testes ou desastres reais, eliminando preocupações com orçamento emergencial.

Estratégia de Resiliência de Dados

- **Políticas de Backup:** Adotamos uma política robusta, a **"Golden Rule" 3-2-1-1-0 (3 cópias, 2 mídias diferentes, 1 off-site, 1 imutável, 0 erros)** que deve ser testada regularmente para garantir a recuperação dos dados.



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

- 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 sua infraestrutura atual

O que é o BIA? Business Impact Analysis

Análise de impacto de negócio capaz de identificar sistemas e processos críticos, definindo tempos aceitáveis de interrupção do seu negócio.

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 dados da empresa, mesmo em ambientes multicloud.

Resiliência de Processos e Sistemas (DR)

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

- **Plano de Disaster Recovery:** Defina 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

A Oferta de DR da TOTVS e Suas Limitações

O ambiente TOTVS tem características que exigem atenção especial na hora de planejar um plano de Disaster Recovery. Não basta replicar servidores e dados. É preciso considerar licenças, integrações, acessos e limitações técnicas específicas da plataforma.

Empresas que não conhecem esses detalhes tendem a descobrir falhas no momento mais crítico: durante a tentativa de recuperação.

A seguir, veremos os principais pontos de atenção que precisam estar previstos, testados e resolvidos.

Principais fragilidades do sistema

- **Escopo:** Cobre apenas sistemas TOTVS, excluindo integrações como TEF, BI ou sistemas de terceiros.

- **Infraestrutura:** Fornece apenas recursos, deixando a implantação, elaboração do PCN e testes sob responsabilidade do cliente, exigindo know-how interno ou consultoria externa.

- **RPO Único:** Baseada em replicação em tempo real, não oferece versionamento, deixando o ambiente vulnerável a problemas lógicos (ex.: ransomware ou erros humanos, como um update que zera preços).

- **Dependência do Mesmo Fornecedor:** Concentrar produção e DR no mesmo provedor aumenta o risco em caso de ataque ao fornecedor, como uma paralisação em ambos os ambientes.

TOTVS ID precisa ser reemitido

O TOTVS ID é uma chave de ativação vinculada ao hardware do ambiente original. Em caso de desastre, não é possível simplesmente ligar uma réplica e retomar a operação. A chave precisa ser reemitida no portal da TOTVS e inserida no ambiente de recuperação.

Se esse processo não estiver documentado e previsto no plano, a retomada pode ser bloqueada logo na primeira etapa.

Arquiteturas baseadas em IP fixo exigem ajustes

Muitas empresas ainda utilizam clientes pesados (fat clients) conectados por IP direto. Em um cenário de contingência, essa estrutura não se replica automaticamente.

É preciso prever o uso de DNS, balanceamento, VDI ou outras formas de redirecionamento. Sem isso, o usuário não consegue acessar o sistema, mesmo que o servidor já esteja no ar.

Integrações externas precisam estar mapeadas

O TOTVS costuma operar conectado a diversos sistemas: BI, TEF, gateways fiscais, ferramentas de logística ou faturamento. Esses elementos nem sempre estão no mesmo ambiente ou dentro da mesma estrutura técnica. No momento do acionamento, se o ambiente de DR não incluir essas integrações, a aplicação até pode subir, mas não funcionará como esperado.

Ambiente de produção precisa ter recursos disponíveis

Replicação em janelas curtas exige CPU, memória e disco disponíveis no ambiente de origem. Quando os servidores estão constantemente operando no limite, a cópia incremental falha ou atrasa.

É comum que ambientes TOTVS não tenham folga suficiente, especialmente em bancos de dados. Sem esse espaço, não é possível manter uma replicação estável e funcional.

Licenciamento do banco de dados pode impedir a replicação

Ambientes TOTVS utilizam diferentes bancos de dados, como SQL Server, Oracle ou Progress. Cada um tem exigências específicas de licenciamento para permitir replicação, backup contínuo ou clusterização.

Se o licenciamento não permitir uso em ambiente paralelo, o DR pode até funcionar tecnicamente, mas estará irregular — ou legalmente inviável em caso de auditoria.

Sistema TOTVS exige plano de DR sob medida.

TOTVS não é um sistema isolado. Ele se conecta com o negócio, com a operação e com uma série de dependências que não aparecem em um diagrama técnico padrão.

Por isso, o plano de recuperação não pode seguir um modelo genérico.

Cada implantação exige análise específica, documentação precisa e testes completos, incluindo todas as camadas que tornam o sistema funcional.

Ignorar esses pontos transforma qualquer plano de DR em uma promessa que não se cumpre quando mais se precisa dela.

Escolhendo a estrutura certa para o seu ambiente TOTVS

A TOTVS oferece uma solução de Disaster Recovery para seus clientes, mas que se limita àqueles que operam dentro do T-Cloud.

Embora essa opção possa atender a alguns cenários, ela possui limitações importantes, principalmente quando o ambiente exige flexibilidade, integrações externas ou múltiplos pontos de restauração.

Neste capítulo, vamos explorar em detalhes os limites da cobertura oferecida pela solução da TOTVS e apresentar alternativas mais completas e robustas para cada uma das lacunas identificadas.

Abrangência da solução

✗ **TOTVS:** Cobre apenas os sistemas TOTVS hospedados no T-Cloud.

Penso: cobre todo o ambiente, incluindo integrações com TEF, BI, gateways fiscais e outros sistemas externos.

Empresas com estruturas híbridas ou sistemas complementares precisam de um DR que contemple todos os componentes críticos, não apenas o ERP.

Escopo do serviço

✗ **TOTVS:** A responsabilidade pela implantação, documentação e testes é do cliente.

Penso: entrega completa, incluindo a configuração do ambiente de DR, testes periódicos, plano de continuidade e suporte técnico.

Isso significa que, com a TOTVS, a empresa precisa contratar ou manter uma equipe interna para montar e validar o plano. Na Penso, esse processo já está incluso na operação.

RPO (Ponto de Recuperação)

❌ **TOTVS:** Oferece apenas um ponto de restauração, com replicação contínua.

Penso: Oferece múltiplas versões, com possibilidade de restauração em diferentes momentos.

Esse ponto é crítico. Um único RPO não protege contra falhas lógicas, como ransomware ou exclusões acidentais. Se o erro for replicado, o ambiente de DR também será comprometido.

Proteção contra falhas lógicas

❌ **TOTVS:** Como trabalha com replicação contínua, não possui versionamento. Qualquer alteração destrutiva é imediatamente replicada.

Penso: Mantém cópias em múltiplas janelas, com possibilidade de recuperar versões anteriores à falha.

Em um ataque ransomware, por exemplo, isso define se a empresa vai conseguir voltar com segurança, ou se precisará reconstruir todo o ambiente a partir de backups manuais.

Dependência do mesmo fornecedor

❌ **TOTVS:** Produção e recuperação ficam sob o mesmo provedor.

Penso: O ambiente de recuperação está fora da estrutura principal, em uma nuvem privada isolada.

Ter produção e contingência sob a mesma gestão pode representar um ponto único de falha.

Em um incidente que afete o próprio fornecedor, os dois ambientes podem ser comprometidos simultaneamente.

Escolhendo a estrutura certa para o seu ambiente TOTVS

Aspecto	TOTVS (T-Cloud)	Penso
Escopo	Apenas sistemas TOTVS	**Ambientes completos e híbridos**
Implantação e testes	Por conta do cliente	**Incluídos no serviço**
Versionamento	Não possui	**Múltiplas versões disponíveis**
Proteção contra falhas lógicas	Limitada	**Sim**
Plano de continuidade	Cliente precisa elaborar	**Entrega e mantém**
Equipe de suporte	Limitado à infraestrutura	**Acompanhamento técnico completo**
Localização do ambiente de DR	Mesmo fornecedor	**Nuvem isolada, gerenciada pela Penso**

Cada ambiente exige um nível diferente de resposta. Entender as limitações técnicas de cada modelo é o primeiro passo para fazer uma escolha segura.

O modelo da TOTVS pode atender empresas com estrutura simples, totalmente centralizada no T-Cloud. Mas em ambientes mais complexos, com dependências externas, requisitos de compliance e exigência de recuperação rápida e segura, essas limitações precisam ser consideradas com atenção.

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.

ESCOLHA A MELHOR SOLUÇÃO.

Construímos confiança com testes, resultados e transparência.

Conclusão

Confiança se Constrói com Resiliência.

Uma paralisação no ambiente TOTVS pode custar caro, seja financeiramente, reputacional e operacionalmente. Com a solução de *Disaster Recovery* da Penso Tecnologia, baseada na plataforma Veeam e apoiada pela Adstec, sua empresa estará preparada para enfrentar qualquer interrupção, garantindo a continuidade do negócio em minutos, não dias. Nossos testes periódicos, governança robusta e expertise certificada constroem a confiança que você precisa para proteger seu ambiente TOTVS.

Penso

Disaster Recovery para sistemas TOTVS

#Obrigado

Apoio: veeam Adistec