Penso

CLOUD/SaaS
NÃO TEM BACKUP

→ Resiliência para M365

→ Salesforce, AWS, Azure

→ **e outras plataformas**

Entenda os riscos de ter **todos os ovos na mesma cesta** e saiba como **manter a resiliência do seu ambiente**

Apoio: veeam Adistec

Introdução

As grandes nuvens prometem o paraíso: escalabilidade infinita, disponibilidade 99,99% e zero dor de cabeça. Porém, outubro de 2025 mostrou, na prática, que as maiores nuvens do planeta também caem. Em menos de 45 dias, AWS US-East-1, Microsoft 365 e Cloudflare paralisaram milhões de usuários e empresas, gerando horas de indisponibilidade total e prejuízos que ainda estamos contando.

Criado pela Penso Tecnologia a partir do webinar realizado em 10 de dezembro de 2025, ministrado por Eric Moraes – cofundador e CEO da Penso, este e-book é o seu guia urgente e direto para deixar de confiar cegamente na "nuvem infalível" e começar a ter um plano B que realmente funciona quando tudo desabar.

Nas próximas páginas você vai acompanhar os casos reais que abalaram o mundo, os números que ninguém quer ouvir e as soluções Veeam + Penso que já estão garantindo restauração rápida e continuidade real para empresas brasileiras.

Apoio: veeam Adistec

Sobre a **Penso**

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

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

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

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

Protegemos seus dados para que sua empresa nunca pare.

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

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

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

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

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

ÍNDICE

SPEAKER

Erik Lopes Morais

COO e Cofundador da Penso

- Mais de 20 anos de trajetória técnica em segurança da informação, cloud e ferramentas de colaboração
- Lidera a Penso, a única nuvem soberana brasileira com o programa completo de competências Veeam

"Tecnologia é incrível, mas sem resiliência, é só um castelo de cartas esperando o vento."

Quando a teoria encontra a realidade

Em um intervalo de menos de 45 dias, três dos pilares mais críticos da internet moderna sofreram interrupções de escala global:

A região US-East-1 da AWS

O ecossistema completo do Microsoft 365

Infraestrutura da Cloudflare

Não foram minutos de degradação. Foram horas de indisponibilidade total seguidas de dias de recuperação parcial. Milhões de empresas, do pequeno varejo ao grande banco, acordaram sem acesso a e-mails, arquivos compartilhados, sistemas de colaboração ou sites institucionais.

O que esses incidentes revelaram não foi apenas a existência dos 0,01% que sobram no SLA, mas algo muito mais grave: a redundância física oferecida pelos grandes provedores protege contra falhas de hardware ou desastres localizados, porém não impede a propagação de falhas lógicas ou de serviços de controle compartilhados. Um único bug no DynamoDB, um problema no Azure Front Door ou uma atualização mal-sucedida de borda na Cloudflare foram suficientes para derrubar workloads que, em teoria, estavam “altamente disponíveis”.

A consequência prática é simples e cruel

Quando a nuvem primária para, o crédito de serviço devolvido pelo provedor cobre, no máximo, algumas horas de consumo. Ele não cobre a perda de produtividade de milhares de colaboradores, o atraso em fechamentos contábeis, o descumprimento de prazos regulatórios, as multas contratuais com clientes ou o dano reputacional que pode levar meses para ser reparado.

Mais preocupante ainda é o diagnóstico recorrente entre empresas brasileiras de médio e grande porte: a ampla maioria já transferiu seus workloads críticos para ambientes de nuvem pública, mas menos de um terço mantém cópias independentes, imutáveis e testadas fora do ambiente primário. Em outras palavras, terceirizou-se a operação, mas não a responsabilidade pela continuidade.
Esse descompasso transforma qualquer incidente global em um risco existencial para o negócio. A disponibilidade é responsabilidade do provedor; a recuperação, quando tudo falha, continua sendo responsabilidade exclusiva do controlador dos dados, ou seja, da própria organização.

Os capítulos seguintes detalham cada um desses três grandes eventos de 2025, expõem as limitações reais dos contratos de nuvem pública e apresentam as estratégias e soluções que já permitem eliminar essa vulnerabilidade de forma prática, regulatória e economicamente sustentável.

2025: o ano em que a internet quase parou

Outubro e novembro de 2025 ficará marcado como o período em que a infraestrutura digital global sofreu três interrupções consecutivas de escala inédita, todas em menos de 45 dias.

Três serviços considerados pilares da internet moderna falharam de forma independente, mas com consequências amplamente sobrepostas, afetando milhões de empresas e usuários simultaneamente.

OUTUBRO 2025

CRITICAL FAILURE DETECTED

AWS US-East-1 (Norte da Virgínia)

DOWNTIME
12h+

IMPACTO
GLOBAL

INDISPONIBILIDADE TOTAL
A maior região do mundo (N. Virginia) ficou offline, derrubando milhares de serviços

FALHA EM CASCATA
DynamoDB, DNS e serviços internos colapsaram, impedindo até o acesso ao painel de status.

DEPENDÊNCIAS OCULTAS
Empresas fora da região foram afetadas por dependências globais não mapeadas.

A região US-East-1 é a mais antiga e ainda a mais utilizada da AWS, concentrando o maior volume de workloads críticos do planeta. Apesar de contar com seis zonas de disponibilidade, uma falha interna no DynamoDB desencadeou erro em cascata que comprometeu o Route 53 (serviço de DNS da AWS).

O colapso tornou inacessíveis serviços que, mesmo hospedados em outras regiões, dependiam de componentes de controle centralizados na Virgínia. Netflix, Disney+, Slack, Robinhood, Twitch e centenas de aplicações SaaS corporativas ficaram fora do ar por mais de sete horas. No Brasil, o impacto começou às 4h da manhã e se estendeu por todo o dia útil, com lentidão residual por quase 48 horas adicionais devido à propagação de DNS.

OUTUBRO 2025

CRITICAL FAILURE DETECTED

AWS US-East-1 (Norte da Virgínia)

A região Norte da Virgínia (US-East-1) não é apenas a mais antiga da AWS; é, até hoje, a que concentra o maior volume absoluto de workloads críticos do planeta. Grandes bancos, plataformas de streaming, marketplaces, sistemas de pagamento e centenas de soluções SaaS corporativas ainda mantêm parte significativa de sua operação ali, mesmo com a existência de regiões mais modernas.

No dia 1º de outubro de 2025, essa concentração se transformou em vulnerabilidade global.

O que realmente aconteceu?

Uma alteração rotineira em um cluster interno do DynamoDB gerou um comportamento inesperado que sobrecarregou os servidores de metadados. O sistema de saúde automático interpretou erroneamente o evento e iniciou uma cascata de reinicializações que afetou o Route 53 (serviço de DNS da AWS). Em poucos minutos, nomes de domínio que resolviam para qualquer região da AWS começaram a retornar erros ou tempos de resposta proibitivos.

OUTUBRO 2025

CRITICAL FAILURE DETECTED

AWS US-East-1 (Norte da Virgínia)

O impacto foi imediato e abrangente

- Netflix, Disney+, Twitch e Fortnite ficaram completamente inacessíveis por mais de sete horas
- Slack, Robinhood, Coinbase e dezenas de fintechs paralisaram operações
- Milhares de aplicações SaaS que utilizam a Virgínia como região de controle (mesmo com dados replicados em outras zonas) perderam conectividade
- Serviços de autenticação, filas (SQS), notificações (SNS) e funções Lambda entraram em estado de degradação severa

No Brasil, onde muitas empresas utilizam a Virgínia por latência ou por decisões históricas de arquitetura, o efeito começou às 4h da manhã e se estendeu por todo o dia útil. Mesmo após a restauração oficial, a propagação de DNS continuou causando lentidão por quase 48 horas adicionais.

OUTUBRO 2025

CRITICAL FAILURE DETECTED

AWS US-East-1 (Norte da Virgínia)

Por que seis zonas de disponibilidade não foram suficientes?

A AWS anuncia que cada região possui no mínimo três zonas de disponibilidade (a US-East-1 tem seis), todas fisicamente separadas e com energia, rede e refrigeração independentes. Essa arquitetura protege contra desastres localizados (incêndio, inundação, falha de energia), mas não contra falhas lógicas que afetam serviços de plano de controle compartilhado.

O DynamoDB e o Route 53 são exemplos clássicos desses serviços: mesmo que os dados do cliente estejam replicados em várias zonas, os metadados e o roteamento passam por componentes centralizados. Quando esses componentes falham, toda a região (e, em alguns casos, outras regiões) sente o impacto.

Os aprendizados que ficam

A redundância física é essencial, mas insuficiente. Falhas lógicas, atualizações mal sucedidas ou bugs em serviços de controle podem ignorar completamente as zonas de disponibilidade e transformar uma região inteira em ponto único de falha.

Empresas que acreditavam estar protegidas por arquitetura multi-AZ ou multi-região descobriram, na prática, que ainda dependiam de um único ponto crítico. E, como a maioria não mantinha cópias externas e independentes, restou apenas esperar a AWS resolver (sete horas que, para muitos negócios, equivalem a perdas de milhões).

OUTUBRO 2025

SERVICE UNAVAILABLE (503)

Microsoft 365

Falha no Edge:
O Azure Front Door colapsou, derrubando a camada de autenticação global.

Blackout de Colaboração:
EntraID (Login), Teams, Exchange e SharePoint ficaram inacessíveis simultaneamente.

Paralisia Corporativa:
Empresas inteiras ficaram sem operar, incapazes de acessar arquivos ou e-mails críticos.

- Teams
- Exchange
- SharePoint
- EntraID

Apenas 14 dias depois, uma regressão no Azure Front Door, componente responsável pelo roteamento global do Microsoft Cloud, interrompeu autenticação e acesso ao ecossistema 365 em todos os continentes.

Teams, Outlook, OneDrive for Business e SharePoint ficaram inacessíveis ou extremamente lentos por mais de cinco horas.

No mercado corporativo brasileiro, onde o Microsoft 365 já responde por mais de 80% das soluções de colaboração e armazenamento, o efeito foi devastador: reuniões canceladas, aprovações travadas, caixas postais sem sincronização e milhares de colaboradores sem acesso a documentos críticos.

OUTUBRO 2025

SERVICE UNAVAILABLE (503)

Microsoft 365

Se a falha da AWS afetou principalmente serviços de consumo e aplicações de tecnologia, o incidente do Microsoft 365, ocorrido em 15 de outubro de 2025, atingiu diretamente o coração da operação de milhares de empresas: a produtividade diária.

O que realmente aconteceu?

- **Teams:** impossível iniciar ou ingressar em reuniões; mensagens não entregues
- **Outlook:** caixas postais sem sincronização, envio e recebimento bloqueados
- **OneDrive for Business e SharePoint:** arquivos inacessíveis ou em modo somente leitura
- **Power Platform, Dynamics 365 e outros serviços integrados:** indisponibilidade total

A paralisação durou oficialmente cinco horas e meia, mas a recuperação completa levou quase o dia inteiro em muitos casos, devido ao backlog de sincronização acumulado.

OUTUBRO 2025

SERVICE UNAVAILABLE (503)

Microsoft 365

Impacto no Brasil

No mercado brasileiro, onde o Microsoft 365 já responde por mais de 80% das soluções de e-mail e colaboração em empresas de médio e grande porte, o efeito foi devastador:

- Reuniões de conselho, aprovações financeiras e fechamentos mensais foram adiados
- Equipes comerciais perderam acesso a propostas e contratos armazenados no OneDrive
- Call centers que utilizam Teams como central telefônica ficaram mudos
- Empresas que migraram completamente do Exchange on-premise para o 365 descobriram que não tinham mais nenhum caminho alternativo de e-mail

Diferentemente da falha da AWS, que afetou principalmente aplicações de tecnologia e entretenimento, essa interrupção cortou a comunicação interna e externa de forma direta. Para muitas organizações, foi o primeiro momento em que perceberam que o 365 não é apenas “mais uma ferramenta”; tornou-se o sistema nervoso central do negócio.

Microsoft 365

Por que a alta disponibilidade do 365 não protegeu ninguém?

O Microsoft 365 é projetado com redundância geográfica: os dados são replicados entre múltiplos data centers em diferentes países. No entanto, o plano de controle (autenticação, roteamento e metadados) ainda depende de serviços compartilhados que, quando falham, afetam todos os tenants simultaneamente.

Além disso, a Microsoft trata disponibilidade e backup como conceitos distintos:

- Disponibilidade: garante que o serviço esteja no ar na maior parte do tempo.
- Backup: proteção contra exclusão acidental, ataques de ransomware ou indisponibilidade prolongada do próprio serviço.

O contrato padrão do Microsoft 365 não oferece garantia de recuperação de itens excluídos após determinados prazos (30 a 93 dias, dependendo da licença) e não cobre cenários nos quais o tenant inteiro fica inacessível (por exemplo, bloqueio geopolítico ou falha global de autenticação).

O próximo capítulo analisa o terceiro grande incidente de outubro de 2025: a falha da Cloudflare e como uma camada que deveria aumentar segurança e performance acabou se tornando o maior ponto único de falha da internet moderna.

Cloudflare

WAF/CDN mais abrangente do mundo indisponível.
A espinha dorsal de segurança de milhares de sites quebrou.

Dependências indiretas derrubaram serviços.
Mesmo quem não usava diretamente foi afetado por APIs de terceiros.

GPT/AI | Streaming | E-commerce | SaaS/APIS

O terceiro incidente envolveu a Cloudflare, responsável por CDN, WAF e DNS de milhões de sites e aplicações. Uma atualização de borda mal executada transformou a maior plataforma de performance e segurança da internet em ponto único de falha global.

Milhões de domínios simplesmente desapareceram. Muitas das mesmas empresas que já haviam sofrido com AWS e Microsoft 365 voltaram a cair, desta vez porque sua camada de proteção estava posicionada na frente da mesma região da Virgínia afetada semanas antes.

NOVEMBRO 2025

GLOBAL NETWORK FAILURE

Cloudflare

A Cloudflare é, para muitos, apenas um ícone verde no canto do navegador ou uma linha no DNS. Na prática, tornou-se a camada de segurança, performance e disponibilidade que milhões de empresas colocam na frente de suas aplicações, muitas vezes sem plena consciência das implicações.

Em outubro de 2025, essa camada se transformou no maior ponto único de falha da internet moderna.

O que realmente aconteceu?

Uma atualização de software nas rotas de borda (edge) continha uma regra de roteamento mal configurada que entrou em loop infinito. Em menos de três minutos, o problema se propagou para toda a rede global da Cloudflare. O resultado foi imediato:

- Milhões de domínios retornaram erro 500 ou simplesmente deixaram de responder
- Sites corporativos, lojas virtuais, portais de bancos e SaaS de todos os portes ficaram inacessíveis
- APIs protegidas por Cloudflare Workers e Access pararam de funcionar
- Mesmo aplicações com infraestrutura altamente redundante (containers, auto-scaling, multi-região) ficaram offline porque o tráfego nunca chegava até elas

NOVEMBRO 2025

GLOBAL NETWORK FAILURE

Cloudflare

A indisponibilidade durou cerca de quatro horas, mas a recuperação total levou mais de 12 horas em alguns casos, devido ao cache acumulado.

O paradoxo da camada de proteção

A Cloudflare é adotada exatamente para aumentar resiliência:

- **Proteção DDoS**
- **WAF gerenciado**
- **CDN global**
- **Zero Trust Access**

Porém, ao posicionar-se como front-end obrigatório, ela cria um novo single point of failure. Quando a própria Cloudflare cai, não importa quantas zonas de disponibilidade, regiões ou provedores existam atrás dela: o usuário final nunca chega ao destino.

Curiosamente, grande parte dos serviços afetados já havia sofrido com a AWS (US-East-1) e com o Microsoft 365 nas semanas anteriores. O motivo? Muitos utilizam Cloudflare como camada de segurança na frente de workloads hospedados exatamente na Virgínia, o que transformou três incidentes aparentemente distintos em uma sequência de quedas repetidas para os mesmos clientes.

NOVEMBRO 2025

GLOBAL NETWORK FAILURE

Cloudflare

A lição mais dura:

empresas que acreditavam estar protegidas por uma arquitetura “moderna e distribuída” descobriram que, na prática, dependiam de um único provedor de borda para funcionar.

A grande maioria não possuía configuração de DNS secundário ativo nem procedimento testado para bypass da Cloudflare em caso de falha global. Quando o serviço caiu, a única opção foi esperar, exatamente como nas falhas da AWS e do Microsoft 365.

Esse período do final de 2025, portanto, não foi apenas um momento de incidentes isolados. Foi o momento em que o mercado percebeu que alta disponibilidade, multi-região, multi-cloud e camadas de proteção externas podem, paradoxalmente, convergir para o mesmo resultado: paralisação total quando um serviço de controle compartilhado falha.

O próximo capítulo aborda a diferença crítica que ainda separa a maioria das empresas brasileiras da verdadeira resiliência: **disponibilidade não é backup.**

Lições que não podem mais ser ignoradas

Os três eventos apresentaram características comuns:

- Alta redundância física que se revelou ineficaz diante de falhas lógicas ou de serviços de controle compartilhado
- Propagação instantânea do problema para clientes que acreditavam estar protegidos por arquitetura multi-região ou multi-cloud
- Ausência generalizada de mecanismos independentes de recuperação rápida

O padrão por trás das quedas

REALIDADE TÉCNICA

- Nada é infalível. Clouds caem, e a redundância interna nem sempre salva o serviço.
- Quando a cloud cai, você perde totalmente o poder sobre o seu dado.
- Se o serviço volta faltando algo, qual é a sua garantia de integridade?

RISCO CONTRATUAL

Você já leu o contrato do seu SaaS?

A maioria deixa claro: o backup é responsabilidade do cliente.

- Qual a retenção real dos backups?
- Qual a política de restauração (RTO/RPO)?
- Se houver um ataque via seu login, de quem é a culpa?

PERGUNTA CRÍTICA:

VOCÊ TEM UM PLANO B CASO SEU SAAS PARE DE FUNCIONAR HOJE?

Outubro de 2025 não foi uma coincidência infeliz. Foi a demonstração prática de que a alta disponibilidade oferecida pelos grandes provedores não substitui uma estratégia autônoma de backup e restauração.

Redundância física não salva falhas lógicas

A arquitetura de nuvem moderna é construída sobre pilares de redundância física: múltiplos data centers dentro de uma mesma região, separação geográfica entre zonas de disponibilidade e replicação de dados em continentes diferentes.

Esses mecanismos protegem contra riscos tangíveis, como falhas de hardware, interrupções de energia ou desastres naturais localizados. No entanto, outubro de 2025 demonstrou que essa abordagem tem limites claros quando o problema reside em camadas lógicas ou de controle compartilhado.

O mito da redundância absoluta

Em teoria, uma região como a US-East-1 da AWS, com seis zonas de disponibilidade, deveria ser imune a paralisação total. Cada zona opera como um data center independente, com alimentação elétrica, rede e refrigeração isolados. **A Microsoft e a Cloudflare seguem princípios semelhantes: replicação síncrona de dados e balanceamento de carga automático para garantir que, se um componente falhar, o tráfego seja redirecionado instantaneamente.**

Na prática, esses incidentes revelaram que muitos serviços de nuvem dependem de um plano de controle centralizado (metadados, autenticação, roteamento de DNS e gerenciamento de configurações) que não seguem a mesma lógica de distribuição. Quando uma falha lógica ocorre, ela se propaga além das barreiras físicas, afetando não apenas a região principal, mas também workloads replicados em outras áreas.

Por exemplo, na falha da AWS, o DynamoDB e o Route 53 operam em um modelo híbrido: os dados do usuário podem estar distribuídos, mas os comandos de controle ainda passam por pontos de estrangulamento. **O resultado é que, mesmo com infraestrutura no ar, o acesso se torna impossível. É uma paralisação "funcional" que ignora completamente a redundância física.**

Consequências para as empresas

Falhas lógicas não respeitam SLAs de disponibilidade. Elas criam cenários onde o serviço está tecnicamente "disponível" (servidores ligados, dados intactos), mas inacessível para os usuários finais. Isso amplifica prejuízos:

- **Perda de receita direta:** e-commerces e fintechs perdem transações em minutos
- **Impacto na cadeia de suprimentos:** aplicações SaaS interdependentes param em cascata
- **Custos indiretos:** equipes de TI gastam horas em troubleshooting, enquanto a produtividade geral cai para zero

Relatórios globais de 2025 estimam que o **downtime médio em nuvem custa**

US$ 300 mil por hora

para empresas de médio porte

Esse valor ainda pode multiplicar em setores regulados como saúde e finanças, **onde multas por indisponibilidade somam milhões.**

Estratégias para mitigar riscos lógicos

A lição central é que resiliência verdadeira exige camadas independentes da nuvem primária:

> **Multi-cloud ou nuvem soberana:** Replique workloads críticos em ambientes de provedores diferentes, preferencialmente com operação local para evitar dependências geopolíticas

> **Backup off-tenant:** Mantenha cópias imutáveis fora do ecossistema do provedor principal, permitindo restauração granular mesmo se o plano de controle falhar

> **Testes regulares de failover:** Simule falhas lógicas em ambientes de staging para validar planos de contingência

Ferramentas como Veeam, integradas a nuvens soberanas, permitem replicação assíncrona que ignora as limitações lógicas dos hyperscalers, garantindo RTO (tempo de recuperação) em minutos em vez de horas.

Os capítulos seguintes exploram por que disponibilidade e backup são conceitos distintos e como confundir os dois pode transformar um incidente técnico em uma crise existencial para o negócio.

Disponibilidade não é backup: a diferença que decide o futuro da empresa

A confusão entre disponibilidade e backup é uma das armadilhas mais comuns e mais caras do mercado corporativo brasileiro atual.

Disponibilidade é a promessa do provedor (AWS, Microsoft, Google, etc.) de manter o serviço primário operacional na maior parte do tempo. Ela é medida em porcentagens (99,9%, 99,99%) e compensada, quando descumprida, por créditos de consumo.

Backup é a capacidade da própria empresa de recuperar dados e workloads de forma independente, rápida e íntegra quando o serviço primário deixa de estar disponível ou é comprometido (seja por falha técnica, ransomware ou bloqueio geopolítico).

São responsabilidades distintas, e a Microsoft deixa isso explícito no contrato do Microsoft 365. No documento "Microsoft Services Agreement" e no "Online Services Terms", a empresa é clara:

Itens excluídos

E-mails, arquivos, eventos de calendário e outros arquivos são mantidos na lixeira por até 93 dias (dependendo da licença). Após esse prazo, desaparecem permanentemente.

Sem plano B

Em caso de indisponibilidade prolongada do tenant inteiro (por exemplo, bloqueio por sanção internacional), a Microsoft não oferece alternativa automática de acesso aos dados.

Alto risco

Planos E5 incluem recursos avançados de retenção, mas o backup permanece no mesmo tenant. Ou seja, sujeito ao mesmo risco de acesso bloqueado.

Cenário de incerteza

Não há garantia de recuperação de dados corrompidos por ransomware ou por exclusão maliciosa após o período de retenção.

Em resumo: o Microsoft 365 garante alta disponibilidade, mas não garante a recuperação dos seus dados se eles forem excluídos, criptografados ou se o tenant ficar inacessível.

Ransomware no OneDrive: o cenário que já é rotina

Imagine que um colaborador clica em um link malicioso ou abre um anexo infectado. O ransomware criptografa arquivos localmente e, como o OneDrive sincroniza em tempo real, sobe as versões criptografadas para a nuvem. Em questão de minutos, milhares de documentos corporativos estão irrecuperáveis.

O recurso de "versões anteriores" do OneDrive permite restaurar arquivos individualmente, mas não foi projetado para ataques em massa. Em incidentes reais de 2025, empresas levaram dias para restaurar pastas críticas e muitas perderam dados permanentemente.

A única forma de reverter rapidamente esse tipo de ataque é possuir um backup externo, fora do tenant da Microsoft, com retenção configurável e imutabilidade.

Como isso acontece na prática?

Um colaborador abre um anexo malicioso ou clica em um link de phishing.

O ransomware criptografa arquivos na máquina local em minutos.

O OneDrive (ou SharePoint sincronizado) detecta as alterações e sincroniza automaticamente as versões criptografadas para a nuvem.

Em poucas horas, milhares (ou centenas de milhares) de documentos críticos estão criptografados em toda a estrutura corporativa.

O recurso nativo de “versões anteriores” do OneDrive permite restaurar arquivos individualmente, mas não foi projetado para ataques em massa. Empresas que sofreram esse tipo de incidente em 2025 levaram dias, ou até semanas, para tentar recuperar pastas inteiras manualmente, muitas vezes com perda definitiva de dados.

Porque o dano é tão grande?

- Sincronização bidirecional em tempo real: o que acontece localmente sobe imediatamente
- Permissões amplas: um único usuário com acesso a pastas compartilhadas contamina toda a empresa
- Ausência de imutabilidade nativa: o ransomware sobrescreve versões anteriores sem barreira
- Retenção limitada: após 93 dias, versões antigas desaparecem permanentemente

Relatórios globais de 2025 mostram que mais de 40% dos ataques de ransomware bem-sucedidos em empresas brasileiras **envolveram contaminação de ambientes Microsoft 365 via OneDrive ou SharePoint.**

Bloqueio geopolítico e a responsabilidade pelos dados: você é o controlador

Em 2025, o tenant do Microsoft 365 deixou de ser apenas uma ferramenta técnica. Tornou-se um ativo geopolítico que pode ser desligado por ordem judicial ou sanção internacional, sem aviso prévio e sem alternativa imediata.

Casos reais já ocorreram em vários continentes: empresas que prestavam serviço a países sob embargo ou que se envolveram em disputas transnacionais tiveram o acesso ao tenant bloqueado de uma hora para outra.

Quando isso acontece, o impacto é total

Login no Outlook, Teams, OneDrive e SharePoint desaparece

Backup nativo do plano E5 (se existir) fica igualmente inacessível, porque está no mesmo tenant

O suporte da Microsoft responde que se trata de questão jurídica, não técnica

No Brasil, esse risco está a uma decisão judicial de distância. Basta uma aplicação da Lei Magnitsky, uma investigação internacional ou uma ordem ampla para que o tenant de uma organização brasileira seja suspenso. O que poderia ser resolvido em horas transforma-se em semanas ou meses de processo, com a operação completamente paralisada.

A LGPD e o Marco Civil da Internet são claros: o controlador dos dados é a empresa que determina os fins e os meios do tratamento. Isso significa que multas da ANPD de até R$ 50 milhões, ações civis, processos trabalhistas e perda de contratos recaem exclusivamente sobre você, nunca sobre a Microsoft.

O contrato da Microsoft 365 que ninguém lê e que assusta

A maioria das empresas assina o Microsoft 365 acreditando que “está tudo coberto”. Na prática, o contrato é cristalino e assustadoramente restritivo sobre o que a Microsoft realmente garante e, principalmente, o que ela não garante.

As cláusulas que passam despercebidas

Responsabilidade compartilhada explícita:

“Você é responsável por proteger seus dados contra perda ou corrupção, incluindo exclusão acidental ou maliciosa.” (Microsoft Services Agreement – Seção 6.b)
(Microsoft Services Agreement – Seção 6.b)

Retenção limitada e sem garantia de restauração

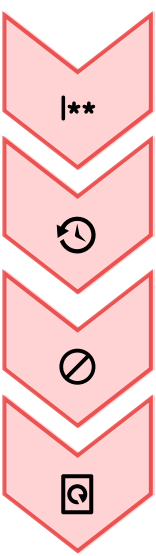
Lixeira: até 93 dias (E3/E5)	Após esse prazo, **exclusão definitiva e irrecuperável**	**Não há recurso técnico ou jurídico** para recuperar itens fora do período

Ransomware e corrupção não são cobertos

A Microsoft não se responsabiliza por restaurar arquivos criptografados ou corrompidos por malware. O recurso "versões anteriores" existe, mas foi projetado para erros humanos pontuais, não para ataques em massa.

O caso hipotético que não é mais hipotético

Imagine que uma sanção internacional (Lei Magnitsky ou equivalente) bloqueie o tenant da sua empresa no Brasil amanhã:



Você perde login no Microsoft 365

Você perde login no backup E5 (porque está no mesmo tenant)

Você perde e-mails, OneDrive, SharePoint, Teams e todo o histórico de colaboração

Não existe botão "recuperar" no portal da Microsoft

Esse cenário já aconteceu em outros países em 2025 e está a uma decisão judicial de distância de acontecer aqui.

A única solução que realmente funciona: ter um backup externo e imutável do Microsoft 365, armazenado fora do tenant da Microsoft.

Retenção configurável
1 ano, 3 anos, 7 anos ou ilimitada

Imutabilidade certificada
(WORM) que impede sobrescrição por ransomware

Restauração granular em minutos
Um arquivo, uma pasta, uma caixa postal inteira

Capacidade de restauração
em massa para cenários de contaminação total

Com esse tipo de backup, o procedimento é simples:

Isola-se o ambiente comprometido	Restaura-se a versão limpa (de 24h, 48h ou 7 dias antes) diretamente sobre o tenant ou em um novo ambiente	O negócio volta a operar em horas, não em semanas

Empresas que possuíam esse tipo de proteção em 2025 recuperaram 100% dos dados em menos de 24 horas. As que não tinham precisaram pagar resgates ou aceitar a perda definitiva de informações críticas.

A conclusão inevitável

A confusão entre disponibilidade e backup é uma das armadilhas mais comuns e mais caras do mercado corporativo brasileiro atual.

✕ **Disponibilidade**

Protege contra quedas curtas do serviço primário.

✔ **Backup**

protege contra exclusão, corrupção, ransomware e indisponibilidade prolongada do próprio provedor.

Empresas que tratam o Microsoft 365 (ou qualquer SaaS crítico) apenas como "altamente disponível" estão, na prática, operando sem rede de segurança.

A Microsoft é clara no contrato: Você mantém a propriedade dos seus dados e com isso vem **a responsabilidade de protegê-los**

Alta disponibilidade → responsabilidade Microsoft

Proteção e recuperação de dados → responsabilidade 100% sua

Empresas que ignoram essa divisão estão, na prática, operando sem backup real do seu ativo mais crítico: os dados corporativos.

Backup externo da Microsoft 365: sim, é possível e já funciona hoje

Felizmente, o risco que parecia inevitável já tem solução consolidada no mercado brasileiro.

O backup externo completo do Microsoft 365 não é um projeto experimental nem uma promessa para o futuro: é tecnologia madura, homologada pela própria Microsoft e em produção em centenas de empresas de médio e grande porte no país.

O que ele protege é absolutamente tudo que o Microsoft Graph expõe:

Caixas postais completas (e-mails, calendário, contatos, tarefas).

OneDrive for Business com todas as versões e permissões, sites SharePoint, canais do Teams, conversas, arquivos compartilhados, gravações de reuniões, grupos e Planner.

A cópia é feita diariamente ou na frequência que você definir para uma nuvem soberana brasileira, fora do tenant da Microsoft, em formato nativo e com imutabilidade certificada (WORM).

Isso significa que nem ransomware consegue apagar ou criptografar o backup.

A implantação é simples: um agente leve é instalado no tenant (sem impacto perceptível de performance) e inicia a cópia incremental diária para data centers Tier III no Brasil. Após o backup inicial, o portal web permite navegar pelo conteúdo como se você estivesse dentro do próprio 365, com busca instantânea e indexação completa.

A restauração é o verdadeiro diferencial:

Um e-mail perdido restaura em 30 segundos

Uma caixa postal apagada por hacker volta em poucos minutos

Contaminação total por ransomware permite restaurar o tenant inteiro para o estado de 24 h, 48 h ou 7 dias atrás

Bloqueio do tenant principal possibilita exportar tudo e subir em ambiente alternativo (Zimbra, Exchange local ou outro provedor) em poucas horas

Isso significa que nem ransomware consegue apagar ou criptografar o backup.

Empresas que já adotaram essa solução em 2025 relatam tempo médio de recuperação entre 4 e 8 horas em cenários críticos, contra semanas ou meses das que dependiam apenas dos recursos nativos da Microsoft.

O retorno é imediato: assim que o primeiro backup é concluído, o risco existencial desaparece.

Restauração granular e migração emergencial na prática

Quando o pior acontece, o que importa não é ter o backup; é conseguir colocar o negócio de pé novamente, rápido e com o mínimo de perda.

Restauração granular: do e-mail perdido ao arquivo crítico

O portal de backup externo permite navegar exatamente como no Microsoft 365 original.

Empresas que já usam a solução relatam que 90% dos incidentes do dia a dia são resolvidos em menos de cinco minutos, sem abrir chamado com a Microsoft.

Migração emergencial: o cenário “tudo caiu”

Esse é o teste de fogo: tenant bloqueado, ransomware total ou falha global prolongada do 365. O processo comprovado em produção é simples e rápido:

- Cria-se um novo domínio temporário (ou usa-se um já preparado)
- Levanta-se um ambiente de e-mail alternativo (Zimbra, Exchange local ou outro provedor) em nuvem brasileira
- Restaura-se prioritariamente as caixas críticas (CEO, financeiro, jurídico, comercial) com os últimos 30–90 dias de e-mails
- Ativa-se OneDrive/SharePoint em storage paralelo (pode ser até on-premise)
- Redireciona-se o fluxo de mensagens (MX) e o acesso aos arquivos

Tempo médio real em 2025: 4 a 12 horas para ter comunicação e arquivos essenciais rodando novamente.

Exemplo prático

Imagine o STF com o tenant bloqueado por sanção internacional. Sem backup externo, o país ficaria semanas sem e-mail oficial dos ministros e assessores.

Com a solução Penso + veeam

- **8h da manhã:** bloqueio confirmado
- **10h:** ambiente Zimbra já no ar com domínio temporário
- **14h:** caixas dos 11 ministros e gabinetes restauradas com os últimos 90 dias
- **18h:** OneDrive/SharePoint acessível via storage alternativo
- **Dia seguinte:** operação 100% normal enquanto a questão jurídica se resolve

Esse mesmo fluxo já foi executado com sucesso por empresas brasileiras em 2025, tanto em ataques de ransomware quanto em incidentes de exclusão em massa.

Por que isso funciona onde o nativo falha

- O backup está fora do tenant → não é afetado por bloqueio ou ransomware
- Os dados ficam em nuvem soberana brasileira → jurisdição nacional, sem interferência externa
- Formato nativo → não precisa de conversão complexa
- Suporte local em português 24×7 → decisão e execução em horas, não em dias

O resultado é claro: empresas com essa camada simplesmente não param. As que ainda dependem apenas do 365 original vivem na corda bamba.

O próximo capítulo mostra como Salesforce, Totvs e dezenas de outros SaaS críticos também não têm backup nativo e o que fazer quando o fornecedor diz “a responsabilidade é sua”.

Salesforce e outros SaaS sem backup nativo

O Microsoft 365 é apenas o caso mais famoso.

A grande maioria dos SaaS críticos que sustentam o dia a dia das empresas brasileiras segue exatamente o mesmo roteiro: alta disponibilidade na vitrine, mas zero garantia real de backup ou recuperação independente.

Salesforce, líder absoluto em CRM, já teve um módulo oficial de backup e o descontinuou anos atrás. Hoje o contrato é cristalino: a responsabilidade pela proteção dos dados é 100% do cliente.

Se um vendedor apagar contas por engano, se um ransomware criptografar registros ou se o tenant for bloqueado por qualquer motivo, não existe recurso nativo para restauração em massa. A única saída segura é a replicação via API para ambiente externo, exatamente o que a Veeam já faz em produção para dezenas de clientes brasileiros, permitindo restauração direta ou export em CSV/XML.

Totvs, RD Station, Zendesk, SAP SuccessFactors, Workday, PipeDrive e praticamente todos os ERPs e plataformas de marketing, RH e atendimento seguem a mesma lógica. A disponibilidade é alta, o SLA é bonito, mas o backup costuma ficar dentro do mesmo ambiente lógico do fornecedor.

Quando há indisponibilidade prolongada, ataque ou bloqueio, o acesso ao histórico financeiro, de leads, de tickets ou de folha de pagamento pode simplesmente sumir.

Em 2025, empresas que sofreram exclusão em massa ou ransomware em Salesforce perderam semanas tentando reconstruir dados manualmente. As que tinham replicação externa via API voltaram ao ar em horas.

A estratégia que já resolve tudo isso é simples e consolidada:

- **Backup imutável (WORM)** – cópias que ransomware não consegue apagar nem criptografar
- **BaaS completo para Microsoft 365** – fora do tenant, com retenção configurável e restauração granular
- **Proteção para +25 workloads** – incluindo Salesforce, Kubernetes, bancos Oracle/SQL, Nutanix, VMware, Hyper-V e ambientes físicos
- **Infraestrutura 100% brasileira** – 5 data centers Tier III em São Paulo e Rio de Janeiro, sob jurisdição nacional e conformidade total com LGPD
- **Replicação automática** via API ou export estruturado para nuvem soberana
- **Retenção configurável e imutabilidade contra ransomware**
- **Plano de restauração testado e documentado**

Empresas que adotaram esse modelo deixaram de ser reféns e passaram a ter controle real sobre seus dados, independentemente da plataforma.

Penso + veeam

Quando o assunto é proteção de dados crítica, não existe mais espaço para promessas ou experimentos. Existe apenas o que já foi testado centenas de vezes e funciona na hora do caos e é exatamente isso que a combinação Veeam + Penso entrega: a tecnologia número 1 mundial em backup integrada à única nuvem soberana brasileira com o programa completo de competências Veeam.

- **Backup imutável (WORM)** – cópias que ransomware não consegue apagar nem criptografar
- **BaaS completo para Microsoft 365** – fora do tenant, com retenção configurável e restauração granular
- **Proteção para +25 workloads** – incluindo Salesforce, Kubernetes, bancos Oracle/SQL, Nutanix, VMware, Hyper-V e ambientes físicos
- **Infraestrutura 100% brasileira** – 5 data centers Tier III em São Paulo e Rio de Janeiro, sob jurisdição nacional e conformidade total com LGPD
- **Replicação automática** via API ou export estruturado para nuvem soberana
- **Retenção configurável e imutabilidade contra ransomware**
- **Plano de restauração testado e documentado**

Próximos passos: seu plano B começa agora

Você acompanhou, capítulo a capítulo, que as maiores nuvens do planeta falham em cascata, que redundância física não protege contra falhas lógicas nem geopolíticas, que o contrato do Microsoft 365 e de praticamente todos os SaaS críticos deixa a recuperação de dados como responsabilidade exclusiva da sua empresa. Além disso, ransomware, exclusão acidental ou bloqueio de tenant já custaram milhões a organizações que acreditavam estar protegidas.

A boa notícia é que a solução não exige projetos de meses nem investimentos milionários. Ela já existe, está madura, roda em produção em centenas de empresas brasileiras e pode ser ativada em dias, muitas vezes em horas.

O caminho mais curto para sair da corda bamba é simples: faça um assessment gratuito de 60 minutos com um especialista Penso + Veeam.

1. Mapeamos todos os seus workloads críticos (Microsoft 365, Salesforce, Totvs, AWS, Azure ou outros)

2. Entregamos um relatório claro mostrando exatamente o que está protegido e o que ainda está exposto.

A partir daí, ativamos o primeiro backup externo completo dos seus dados em nuvem soberana brasileira, com a primeira cópia concluída em até 48 horas. O último e mais importante passo é o teste real de restauração, feito junto com você, para que tenha certeza absoluta de que funciona.

Resultados que comprovam a eficácia da Penso:

- Empresas que sofreram ransomware em 2025 restauraram o Microsoft 365 inteiro em menos de 8 horas
- Clientes com DRaaS ativaram ambientes AWS ou Azure na Penso em menos de 15 minutos após falhas regionais
- Salesforce de grandes varejistas foi recuperado em massa após exclusão acidental, sem perda de uma única oportunidade

A estratégia que já resolve tudo isso é simples e consolidada:

- **Backup imutável (WORM)** – cópias que ransomware não consegue apagar nem criptografar
- **BaaS completo para Microsoft 365** – fora do tenant, com retenção configurável e restauração granular
- **Proteção para +25 workloads** – incluindo Salesforce, Kubernetes, bancos Oracle/SQL, Nutanix, VMware, Hyper-V e ambientes físicos
- **Infraestrutura 100% brasileira** – 5 data centers Tier III em São Paulo e Rio de Janeiro, sob jurisdição nacional e conformidade total com LGPD

Tudo com suporte 24×7 em português, operação local e sem depender de decisão de big tech estrangeira. Porque, no final do dia, a disponibilidade é responsabilidade do provedor primário.

Como a Penso pode garantir a segurança dos seus dados?

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

O que é o BIA? Business Impact Analysis

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

Implementar Estratégia de Resiliência de Dados Global e Contínua

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

Resiliência de Processos e Sistemas (DR)

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

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

Mas o que é RPO e RTO ?

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

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

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

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

Estratégia de Resiliência de Dados

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

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

Como a Penso pode ajudar você agora

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

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

Soluções Sob Medida:

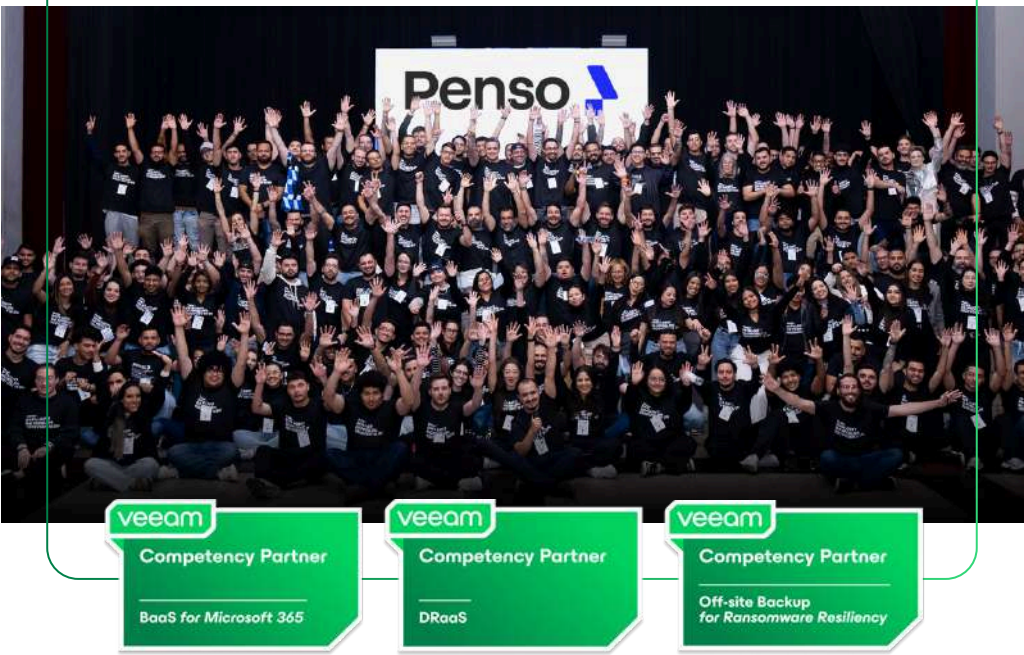
- **Backup Imutável Veeam:** Proteção contra ransomwares, com storage soberano.
- **DR Soberano:** Continuidade em minutos, não dias, em data centers brasileiros.
- **Criptografia S/MIME:** Blindagem contra phishing IA-potencializado.
- **RMM e Treinamento:** Gestão de updates e educação para fechar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

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

Experiência comprovada

A Penso foi a primeira nuvem brasileira a conquistar o programa completo de competências Veeam e foi reconhecida em 2025 como Impact Cloud & Service Provider Partner of the Year Brasil.

Isso não é marketing: significa que nossa infraestrutura foi auditada e aprovada pela própria Veeam para entregar os serviços mais críticos do portfólio.



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.

O cenário de tecnologia mudou de forma irreversível.

A nuvem deixou de ser sinônimo de tranquilidade e passou a ser reconhecida como componente crítico que exige uma camada externa de proteção. Continuidade de negócios, soberania de dados e recuperação rápida deixaram de ser temas exclusivos da TI e tornaram-se parte da agenda estratégica de qualquer organização.

Cada decisão de arquitetura e orçamento agora precisa considerar a resiliência independente como fundamento da operação. O risco não está apenas em perder minutos de serviço, mas em perder semanas de acesso ao que realmente move o negócio.

O desafio é permanente, mas a solução já existe e está ao alcance de qualquer empresa brasileira.

Entender o risco é o primeiro passo. Agir com a estrutura certa é o que garante que, independentemente do próximo incidente, o essencial continue funcionando.

Seguimos juntos, transformando vulnerabilidade em continuidade real.

Penso

CLOUD/SaaS
NÃO TEM BACKUP

#Obrigado

Apoio: veeam Adistec