WHITEPAPER //

3STRUCTURE

_Parte 2

Backup Corporativo:

Como gerenciar os dados da sua empresa?

Pagar o resgate não garante a recuperabilidade

O que significa que toda a infraestrutura de TI está tão perfeitamente disponível para o invasor quanto é facilmente acessível aos usuários. A maioria das organizações corre o risco de reintroduzir infecções: de forma alarmante, quase dois terços (63%) das organizações correm o risco de reintroduzir infecções enquanto se recuperam de ataques de ransomware ou desastres significativos de TI.

Pressionadas a restaurar as operações de TI rapidamente e influenciadas por executivos, muitas organizações pulam etapas vitais, como a reverificação de dados em quarentena, causando a probabilidade de as equipes de TI restaurarem inadvertidamente dados infectados ou malware.

Pelo terceiro ano consecutivo, a maioria (81%) das organizações pesquisadas pagou o resgate para encerrar um ataque e recuperar dados.

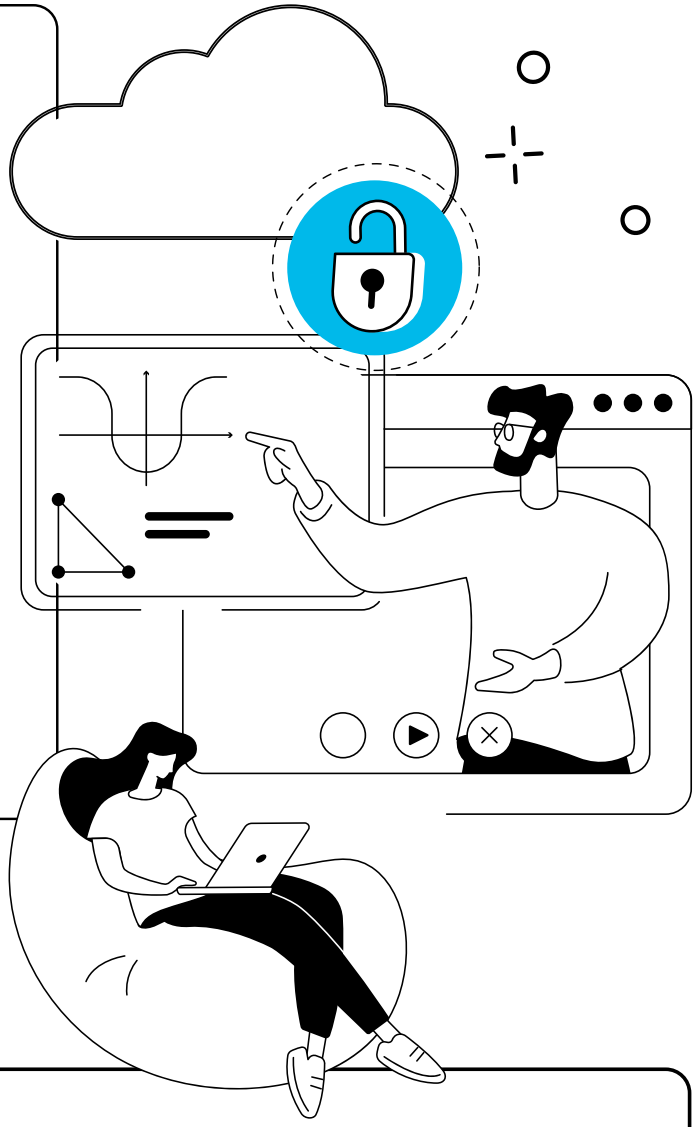
Uma em cada três dessas organizações que pagou o resgate ainda não conseguiu se recuperar mesmo depois de pagar. E pelo terceiro ano consecutivo, mais organizações “pagaram, mas não conseguiram recuperar” do que as organizações que “recuperaram sem pagar”.

Os dados na Nuvem e no local são facilmente passíveis de ataque: surpreendentemente, não houve variação significativa entre a quantidade de dados afetados dentro do Data Center versus dados dentro de escritórios remotos/filiais ou mesmo em dados hospedados em uma Nuvem pública, ou privada.

As organizações devem garantir dados recuperáveis:

Como uma “lição aprendida”, os entrevistados que já enfrentaram ataques cibernéticos agora reconhecem a importância da imutabilidade.

Atualmente, 75% das organizações utilizam discos locais com proteção contra alterações, e 85% recorrem ao armazenamento em nuvem com recursos de imutabilidade. Na prática, metade de todo o armazenamento de backup já é imutável, o que demonstra avanços significativos, embora ainda haja trabalho a ser feito.



A importância do backup para segurança de dados

O ano era 2013, quando a IBM declarou que os dados seriam para o século XXI o que a energia a vapor foi para o século XVIII, a eletricidade para o século XVI e os hidrocarbonetos para o século XX.

Em uma conferência em 2015, a então presidente executiva da IBM Corp., Ginni Rometty, afirmou que os dados são o novo recurso natural do mundo, sendo uma base de vantagem competitiva, mas uma grande ameaça para todos os setores e empresas do mundo, devido ao crime cibernético.

A perda de dados é ainda mais preocupante sob o ponto de vista das organizações.

Isso porque os dados são recursos valiosos e com as novas leis que os protegem, nunca foi tão necessário prezar pela segurança desses ativos digitais. Em termos de negócio, perder dados pode significar um grande prejuízo para quem os detêm.

Nesse cenário, onde “os dados são o novo petróleo”, as empresas precisam definir os ambientes em que serão armazenados e como garantir a segurança para evitar violações e perdas de dados.

Como sua empresa lida com a segurança de dados?

Sobretudo, **uma empresa que não investe em segurança de dados está exposta a riscos e ameaças cibernéticas.**

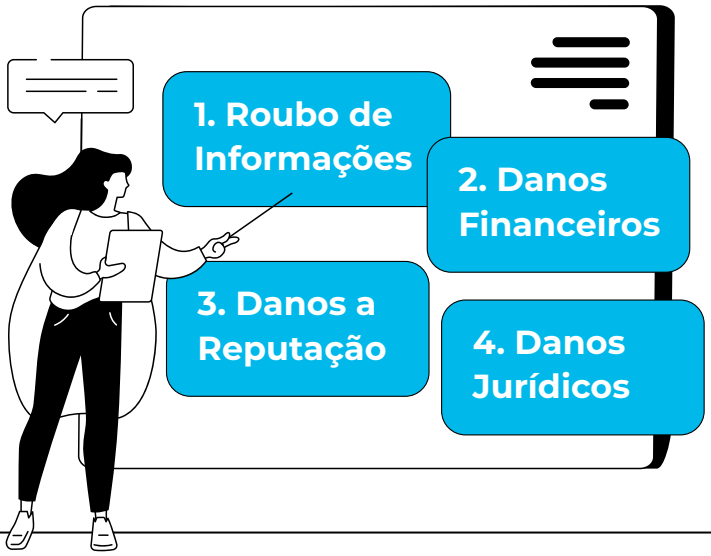
O mais recente levantamento da Kaspersky revela números preocupantes: **o custo médio de um incidente por perda de dados atinge a impressionante marca de US$ 1,23 milhão para grandes empresas e US$ 120 mil para pequenas organizações.**

Outra pesquisa, da Information Technology Intelligence Consulting (ITIC), descobriu que 98% das organizações afirmam que uma única hora de inatividade pode custar em média US$ 100.000.

Contudo, o impacto financeiro causado às empresas em decorrência de um ciberataque não é a única preocupação com a perda de dados. Na era digital em que vivemos, as informações pessoais, dados financeiros e a reputação online são ativos valiosos. Por isso, os ataques cibernéticos representam uma ameaça real para a segurança dessas informações e as consequências são desastrosas.

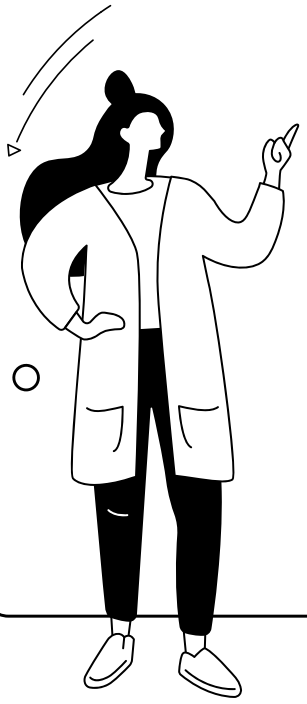
Os ciberataques resultam em prejuízos, tanto para os indivíduos quanto para as empresas. Nesse caso, **como anda o seu investimento em estratégias de segurança?**

Impactos causados pela violação e perda de dados



Uma organização que sofreu perda de dados devido a uma falha de hardware, pode contar com o backup de dados para restaurar as operações rapidamente.

Assim como, uma empresa com medidas robustas de segurança cibernética está mais bem preparada para suportar ataques cibernéticos, minimizando a interrupção de suas operações.



Ainda segundo as pesquisas, 79% dos líderes só aprovam orçamentos de soluções de segurança depois que a violação ou perda de dados acontece. Enquanto isso, o número de organizações que sofrem ataques chega a 92%. O relatório “Cost of a Data Breach”, da IBM, aponta que **o custo médio de uma violação de dados no Brasil é de R$ 6,75 milhões.**

Dessa forma, a criação de backups de dados corporativos se mostra como uma medida básica e uma grande aliada para qualquer protocolo de segurança. Além disso, a prática de armazenamento é essencial para evitar interrupções operacionais, multas e danos à reputação da empresa.

8 motivos para investir em backups corporativos:

1. Previne a perda de dados sensíveis
2. Garante a conformidade regulatória
3. Facilita a recuperação de desastres
4. Protege contra ataques de malware e ransomware
5. Garante a consistência e a integridade dos dados
6. Certifica a disponibilidade dos dados
7. Otimiza tempo e reduz custos
8. Certifica a continuidade das operações e dos negócios

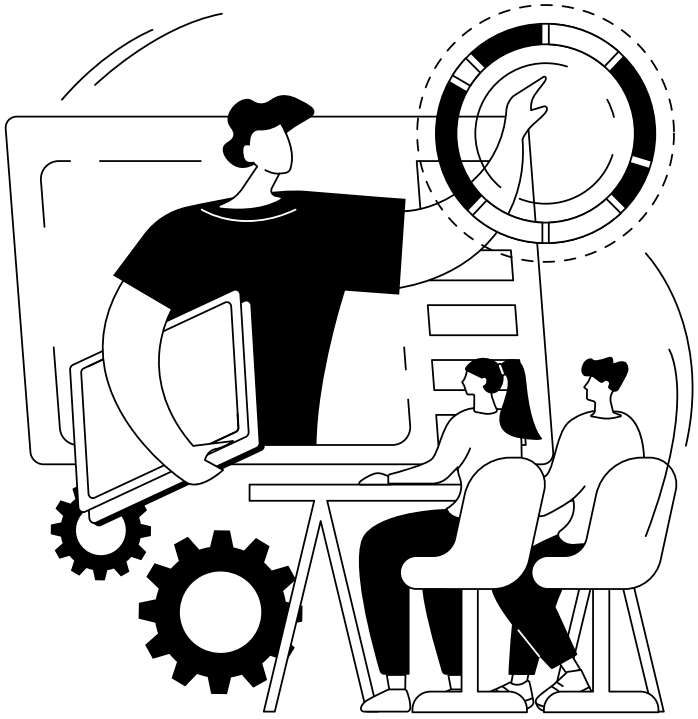
Portanto, com um backup de dados sua empresa tem a garantia de que caso algum incidente aconteça de maneira repentina, como uma falha no hardware ou seu sistema seja comprometido, os seus registros de negócio podem ser recuperados facilmente.

Ter estratégias de backup e recuperação de dados no protocolo de segurança cibernética é crucial para garantir a integridade e a disponibilidade das informações diante de perdas acidentais ou maliciosas

Ambiente de armazenamento local, em nuvem pública, privada e híbrida

Tão importante quanto realizar as cópias de dados, é o local de armazenamento desses dados. A escolha do local deve levar em conta fatores como nível de proteção, acessibilidade e custo, o que vai variar de acordo com o que cada empresa procura.

Nuvem privada: refere-se a serviços no local, onde uma estrutura é montada no próprio ambiente da empresa, onde seus dados ficam sob controle e protegidos permitindo soluções personalizadas que atendem as necessidades específicas de cada organização. Entre as vantagens está maior flexibilidade, controle e escalabilidade em comparação a infraestrutura local.



Entre as opções de armazenamento local, destacam-se:

Nuvem pública: abrange serviços de nuvem terceirizados em que a infraestrutura de TI, como servidores, redes e recursos de armazenamento é oferecida como recursos virtuais acessíveis pela internet. Entre os benefícios estão a redução de custos, escalabilidade quase ilimitada e não há necessidade de manutenção.

Nuvem hibrida: é a combinação entre o armazenamento local com o armazenamento em nuvem permitindo que os dados e aplicativos se movam entre dois ambientes. Oferece maior flexibilidade, mais opções de implantação, segurança e conformidade.

Backup como ferramenta de segurança

Antes de tudo, fazer backups dos dados da sua empresa é como ter uma cópia extra da chave de casa, caso a original seja perdida.

O mesmo se aplica aos dados corporativos, criar backup de dados é uma medida básica e essencial para qualquer protocolo de segurança que busca proteger informações críticas como registros financeiros, propriedade intelectual, dados de clientes, funcionários e parceiros. Afinal, quando sua organização é vítima de um ataque cibernético ou um desastre natural, ela acaba sendo impactada em três principais vertentes: financeira, reputacional e jurídica.

Entretanto, é o impacto na reputação da organização devido aos incidentes cibernéticos o que mais pode perdurar, afetando relacionamentos com clientes, parceiros e investidores. Segundo uma pesquisa da AMO Strategic Advisors, 35,3% do valor de uma empresa é referente à sua reputação.

Por esse motivo, o backup de dados é mais do que uma estratégia eficaz de resiliência cibernética, mas uma ferramenta robusta para garantir a proteção dos ativos digitais.

Contudo, para que os backups possam atingir o objetivo desejado, é preciso que eles sejam atualizados constantemente. Sendo assim, é recomendado criar rotinas e procedimentos claros e bem definidos, além de acompanhar seu cumprimento de acordo com os prazos necessários.

Melhores práticas de backup para proteger dados

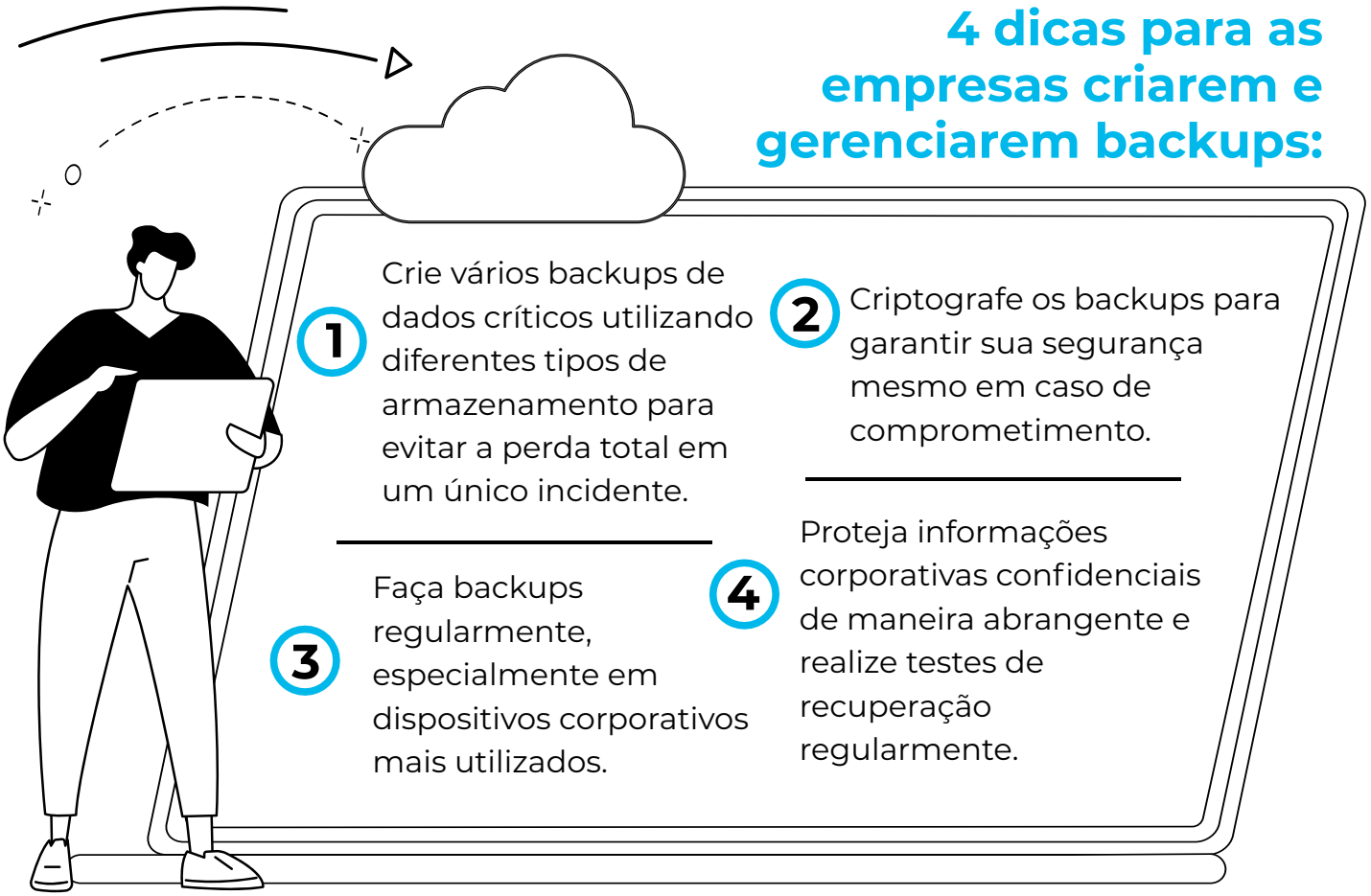
A precaução é o ativo mais importante diante da segurança de dados. Empresas que compreendem a importância em manter seus servidores de armazenamento sempre seguros se antecipam aos imprevistos.

Portanto, é essencial incorporar um plano de backup eficaz na estratégia de segurança cibernética, pois a questão não é mais se sua empresa será alvo de um ataque, mas quando isso ocorrerá.

As melhores práticas devem estar alinhadas com as necessidades da sua organização ao estruturar um planejamento coerente para continuidade dos negócios. Ter um plano de recuperação de desastres garante que a recuperação dos dados seja rápida em restabelecer todo o sistema operacional da empresa.

Outro ponto importante é a diversificação dos métodos de armazenamento, combinar soluções locais com nuvem, proporciona uma recuperação ágil, além de adicionar uma camada extra de segurança, protegendo os ativos contra desastres físicos, por exemplo. Afinal, manter uma cópia em um único local de backup já não é mais o suficiente.

4 dicas para as empresas criarem e gerenciarem backups:



1. Crie vários backups de dados críticos utilizando diferentes tipos de armazenamento para evitar a perda total em um único incidente.
2. Criptografe os backups para garantir sua segurança mesmo em caso de comprometimento.
3. Faça backups regularmente, especialmente em dispositivos corporativos mais utilizados.
4. Proteja informações corporativas confidenciais de maneira abrangente e realize testes de recuperação regularmente.

Portanto, com essas dicas, fica mais claro como sua empresa pode garantir a segurança dos dados por meio do gerenciamento de backup.

Agora, vamos falar sobre a Regra 3-2-1 de backup e no que consiste essa estratégia.

O que é a regra 3-2-1 de backup?

A Regra 3-2-1 é uma estratégia de proteção de dados que recomenda ter três cópias dos seus dados, armazenadas em dois tipos diferentes de mídia, com uma cópia mantida fora do local.

Como uma estratégia de backup de dados amplamente adotada, a Regra 3-2-1 consiste em:

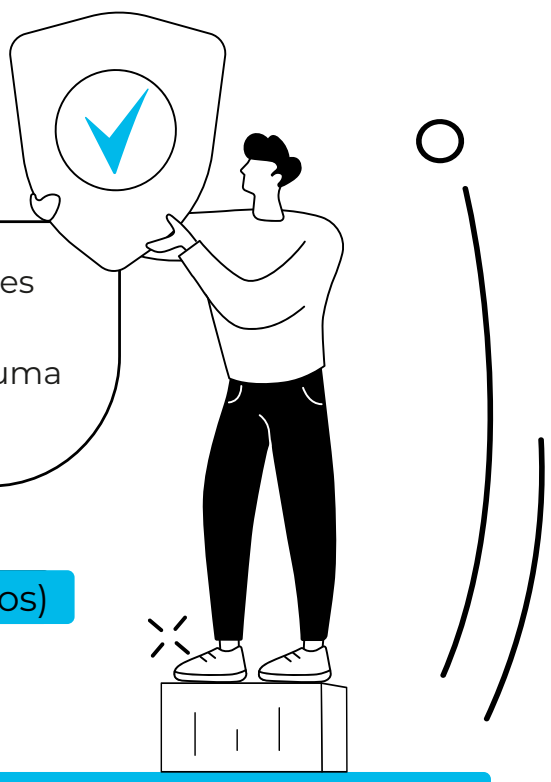
- **Manter três cópias dos seus dados:** isso inclui os dados originais e pelo menos duas cópias.
- **Usar dois tipos diferentes de mídia para armazenamento:** armazene seus dados em duas formas distintas de mídia para aumentar a redundância.
- **Manter pelo menos uma cópia fora do local:** para garantir a segurança dos dados, tenha uma cópia de backup armazenada em um local externo, separada dos seus dados principais e dos backups locais.

Esta regra é uma diretriz robusta para proteção de dados, garantindo redundância, resiliência e a capacidade de recuperar dados mesmo diante de eventos inesperados ou desastres. Ao mitigar pontos únicos de falha, aumentar a disponibilidade de dados e proteger contra corrupção, a redundância garante a segurança de informações críticas.

Ela desempenha um papel fundamental na recuperação de desastres, adaptando-se a tecnologias em evolução e atendendo aos requisitos de conformidade. Armazenamento diversificado e backups externos, conforme recomendado pela regra, mitigam efetivamente vários riscos, contribuindo para a segurança geral e a confiabilidade de dados críticos.

A regra 3-2-1-1-0 com Veeam

A Veeam pode configurar inúmeras combinações seguindo a Regra 3-2-1. Essa versatilidade é evidente nas seguintes implementações, cada uma contribuindo para a adesão a essa diretriz:



- Backups em disco (DAS, SAN, NAS e dispositivos)
- Backups em fita
- Backups em armazenamento removível
- Snapshots de armazenamento (cuidado ao separar mídia da produção)
- Backups em armazenamento de objetos, como na nuvem pública com a camada de capacidade do Repositório de Backup de Escalabilidade Horizontal
- Backups em armazenamento de arquivo frio na nuvem pública com a camada de arquivo do Repositório de Backup de Escalabilidade Horizontal
- Backups hospedados ou gerenciados por um provedor de serviços, incluindo Veeam Cloud Connect
- Replicação para outro host ou site com replicação Veeam
- Trabalhos de cópia de backup para outro local de armazenamento

A Veeam pode configurar inúmeras combinações seguindo a Regra 3-2-1. Essa versatilidade é evidente nas seguintes implementações, cada uma contribuindo para a adesão a essa diretriz:

3

Três cópias dos dados

Certifique-se de ter três cópias dos seus dados, seguindo o aspecto tradicional da regra.

2

Dois tipos diferentes de mídia

Mantenha a redundância de dados usando dois tipos distintos de mídia, mas agora considere o armazenamento em nuvem como uma dessas opções (ou seja, instantâneos em volumes e backups em armazenamento de objetos).

1

Uma cópia fora do local

Tenha uma cópia dos seus dados armazenada fora do local, o que pode ser facilmente obtido com soluções de backup em nuvem (por exemplo, AZ, região ou provedor de nuvem alternativo).

1

Uma cópia offline, air-gapped ou imutável

Reconheça a importância de ter uma cópia que seja offline, air-gapped ou imutável. Esse aspecto é crítico, especialmente no contexto de proteção contra ransomware, onde uma cópia offline, air-gapped ou imutável pode ser um salva-vidas.

0

Zero erros com a verificação de recuperação do SureBackup

Reconheça a importância de ter uma cópia que seja offline, air-gapped ou imutável. Esse aspecto é crítico, especialmente no contexto de proteçãocontra ransomware, onde uma cópia offline, air-gapped ou imutável pode ser um salva-vidas.

veeam

Soluções de backup corporativo

Software de Backup Veeam

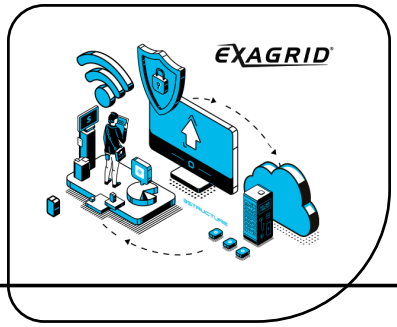
Essa solução oferece uma gama de recursos que garantem a proteção e recuperação de dados corporativos de forma eficaz. Com funcionalidades como recuperação instantânea, backup para armazenamento em nuvem, segurança integrada, portabilidade de dados e suporte robusto.

Capacidade de gerenciar grandes volumes de dados e infraestruturas complexas com eficiência

Restauração imediata de máquinas virtuais e arquivos com segurança

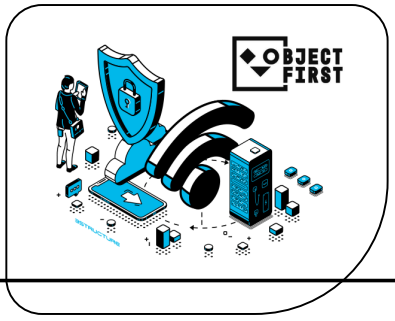
Backup e restauração de dados em ambientes de nuvem pública, privada e híbrida p/ maior resiliência

Armazenamento para Backup



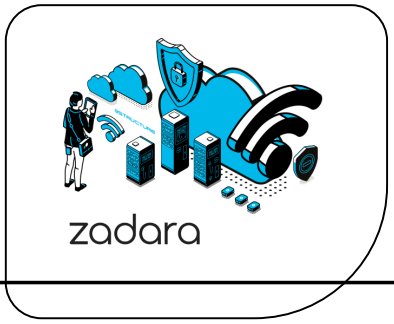
O ExaGrid oferece backup em camadas com uma zona de aterrissagem em cache de disco para backups rápidos e restaurações instantâneas de VM.

Seu repositório de retenção tem o menor custo para armazenamento a longo prazo, e sua arquitetura escalável garante uma janela de backup fixa, evitando atualizações caras.



O armazenamento de backup seguro, simples e poderoso para clientes Veeam agora é uma realidade com o Object First OOTBI.

Em apenas 15 minutos, esse objeto revolucionário pode ser acumulado, empilhado e alimentado, oferecendo desempenho de backup e recuperação imbatível, resistente a ransomware.



O Zadara se destaca como um dispositivo SAN na nuvem, combinando a familiaridade de um SAN tradicional com o dinamismo do provisionamento em tempo real e cobrança por hora.

Oferece recursos avançados e segurança robusta, ideal para enfrentar os desafios do crescimento de dados com eficiência e proteção melhoradas.

3STRUCTURE

Fontes

DataCenterDynamics. Perda de dados pode custar às empresas mais de US$ 1 milhão. Abril, 2024. Disponível em: https://www.datacenterdynamics.-com/br/not%C3%ADcias/perda-de-dados-pode-custar-as-empresas-mais-de-us-1-milhao/ #:~:text=Novo%20levantamento%20realizado%20pela%20em-presa,120%20mil%20para%20pequenas%20organiza%C3%A7%C3%B5es Acesso em: 17 marc. 2025. Cyber Security Ventures. Os danos colaterais dos ataques cibernéticos: danos à reputação. Califórnia, 2025. Disponível em: https://cybersecurityventures.com/the-collateral-damage-of--cyberattacks-reputational-harm/. Acesso em: 17 marc. 2025. Forbes. Empresas brasileiras perdem em média R$ 6,75 milhões por violação de dados. Setembro, 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/09/empresas-brasileiras-perdem-em-media-r-675- milhoes-por-violacao-de-da-dos/. Acesso em: 17 marc. 2025. Fortinet. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/data-security#:~:text= Por%20que%20a%20-seguran%C3%A7a%20de,de%20perda%20de%20dados%20confidenciais. Acesso em: 17 marc. 2025. Matheus Bracco. Security Report. Custo de vazamen-to de dados no Brasil é de R$ 6,2 milhões. Agosto, 2023. Disponível em: https://securityleaders.com.br/media-de-custo-de-vazamento-de--dados-no-brasil-oscila-para-r-62-milhoes-em-2023/#:~:text=De%20acordo%20com%20o%20estudo,R%24%206%2C2%20milh%C3%B5es. Acesso em: 17 marc. 2025. Meu Positivo. Qual é o volume de dados criados todos os dias e qual é o futuro dos dados? Disponível em: https://www.meupositivo.com.br/do-seujeito/tecnologia/qual-o-volume-de-dados-criados-todos-os-dias-e-qual-e-o-futuro-dos-dados/. Acesso em: 17 marc. 2025. Microsoft. O que são nuvens públicas, privadas e híbridas? Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-are- private-public-hybrid--clouds. Acesso em: 17 marc. 2025. MIT Tecnology Review. Data Literazy: a importância da alfabetização em dados em mundo Big Data. Outubro, 2024. Disponível em: https://mittechreview.com.br/data-literacy-a-importancia-da-alfabetizacao-em-dados-em-um-mundo-big-data/. Acesso em: 17 marc. 2025. Secureway. Gerenciamento avancado e prevencao para reducao de riscos. Disponível em: Acesso em: 17 marc. 2025. Terra. Cibercrime irá faturar US$ 10 trilhões por ano até 2025, revela estudo. Abril, 2023. Disponível em: https://www.terra.com.br/noticias/cibercrime-ira-faturar-us--10-trilhoes-por-ano-ate-2025-revela-estudo,bcb2fc9aa10371ab85c721eb1768adfck1lll5wh.html?utm_source=clipboard. Acesso em: 17 marc. 2025. Veeam. Qual é a regra de backup 3-2-1. Fevereiro, 2024. Disponível em: https://www.veeam.com/blog/321-backup-rule.html. Acesso em: 17 marc. 2025.