1)O que é Backup?

Já imaginou perder todos seus registros financeiros, banco de dados de clientes ou até mesmo lançamentos do seu estoque? Isso geraria muita dor de cabeça! A notícia boa é que a automação dos Backups minimiza expressivamente estes riscos.

Considera-se Backup qualquer cópia de segurança, quer seja feita em outro dispositivo, como HDs externos, pendrives ou na nuvem. A finalidade do Backup é a recuperação de dados para restaurar informações em caso de perda dos arquivos originais, ou em caso de acidentes operacionais com os equipamentos.

 Por essa razão, é recomendado que façamos Backups recorrentes tanto no ambiente profissional o quanto em nossos arquivos de uso pessoal (documentos de computador, fotos do celular, entre outros).

Qual a importância do Backup para os negócios?

A importância do Backup está na proteção contra o risco de perda de dados e informações. Essa importância aumenta proporcionalmente em relação ao valor das informações a serem protegidas. Assim, os Backups passam a ter relevância muito maior em empresas que trabalham com dados e informações sensíveis, como dados bancários e dados pessoais de clientes.  
Atualmente, realizar cópias de segurança é uma atividade muito mais simples e acessível, devido à diversidade de recursos que a tecnologia disponibiliza. Nesse tocante, a estratégia de centralizar os Backups em um único ambiente pode trazer muitas vantagens para seu negócio, pois o acesso às cópias de segurança torna-se mais ágil, otimizando o tempo de restauração em casos emergenciais.  
Outro fator importante a considerar, é a proteção das cópias de segurança. Levando em conta os crescentes casos de ataques virtuais e a nova LGPD (Lei Geral de Proteção de Dados), que entra em vigor em 2020, proteger os dados salvos com recursos como criptografia ou com Blockchain são estratégias importantíssimas.

2) Backups Full, Incremental e Diferencial

Para identificar qual o melhor método para sua empresa, é preciso avaliar a política de backups que você escolheu implementar. Cada metodologia possui suas vantagens específicas, e você deve considerar quais são as mais importantes para o tipo de dados e informações que trata e para o seu modelo de negócio.  
Há, basicamente, três as metodologias para armazenamento de cópias de segurança, Full (completo), Incremental e diferencial. Vamos falar um pouco sobre cada um deles.

Backup Full (completo)  
É o mais simples e comum de ser usado, consiste em criar uma cópia completa dos dados. Todos os arquivos da sua empresa são atualizados e não apenas os novos ou modificados. Essa metodologia possui a vantagem de haver sempre uma cópia completa de todos os dados do seu negócio, possibilita a recuperação total dos arquivos de maneira ágil. A desvantagem aqui é que ele demanda muito mais tempo para ser feito e muito mais capacidade de armazenamento.

Backup Incremental  
É o tipo de backup recomendado para empresas que possuem grande volume de dados. Geralmente ele é realizado após um Backup completo, salvando apenas os arquivos novos ou alterados. É um método que permite maior velocidade na criação de cópias de segurança, levando muito menos tempo que o Backup completo. A sua desvantagem é de que para restaurar o sistema ele necessita, recuperar antes os dados completos e em seguida os incrementais e só então realizar a restauração dos arquivos, levando mais tempo

Backup Diferencial  
Esse método é muito semelhante ao Incremental, visto que ele também cria uma cópia dos arquivos alterados. A diferença aqui é que ele realiza uma cópia desde o Backup completo de tudo que foi alterado desde então. Dessa forma, ele armazena mais dados do que o incremental e exige mais espaço e tempo para ser realizado. Sua vantagem é que para restaurar os arquivos ele o faz de forma mais rápida visto que ele usa como referência o último Backup completo. Esse método é ideal para pequenas e médias empresas, devido ao custo de armazenamento dos dados.  
Em suma, fica clara a importância de um método adequado de backup instituído junto ao sistema de gestão do negócio, afinal alguns dados são muito valiosos e perdê-los pode gerar muitos prejuízos e até complicações legais. Gostou do artigo? Quer saber mais sobre como proteger seus dados? Conte com a Acadi-TI!

3) A frequência de backup é uma consideração crucial ao desenvolver um plano de backup por várias razões. Aqui estão alguns motivos pelos quais a frequência de backup é tão importante:

Minimização da Perda de Dados:

Quanto mais frequentemente você realiza backups, menor é a quantidade de dados perdidos em caso de falha do sistema ou perda de dados. Se os backups são realizados com pouca frequência, há um risco maior de perder informações valiosas se ocorrer um problema entre os backups.

Recuperação Rápida:

Backups frequentes permitem uma recuperação mais rápida em caso de falha. Se ocorrer um problema, você pode restaurar os dados a partir do backup mais recente, minimizando o tempo de inatividade e impacto nas operações.

Mudanças Significativas nos Dados:

Se os dados em seu sistema estão sujeitos a mudanças significativas com frequência, é crucial realizar backups frequentes para capturar essas alterações. Isso é especialmente importante em ambientes onde os dados são atualizados regularmente.

Manutenção da Integridade dos Dados:

Backup frequente ajuda a manter a integridade dos dados. Se ocorrer uma corrupção de dados ou um erro humano, você pode voltar a um estado anterior que não foi afetado por esses problemas.

Conformidade com Regulamentações:

Algumas regulamentações e políticas de segurança podem exigir backups frequentes como parte das práticas recomendadas para garantir a proteção e a disponibilidade dos dados.

Minimização de Riscos Operacionais:

Ao realizar backups com frequência, você reduz os riscos operacionais associados à perda de dados. Isso é especialmente crítico em ambientes onde a perda de dados pode resultar em impactos financeiros significativos ou danos à reputação.

Crescimento Controlado do Volume de Dados:

Se os backups são realizados com frequência, o volume de dados a serem copiados em cada backup individual é menor. Isso facilita o gerenciamento do armazenamento e reduz os requisitos de largura de banda necessários para a transferência de dados.

Tecnologia de Deduplicação Eficiente:

Com backups frequentes, as tecnologias de deduplicação podem ser mais eficientes, pois elas identificam e eliminam dados redundantes ou duplicados entre os backups.

Ao desenvolver um plano de backup, é importante avaliar a natureza dos dados, os requisitos de recuperação, a frequência de mudanças nos dados e outros fatores para determinar a melhor estratégia de backup. Em muitos casos, uma combinação de backups completos e incrementais é usada para otimizar a eficiência e a segurança do processo de backup.

Parte superior do formulário

4) A escolha da frequência de backup depende de vários fatores, incluindo o tipo de dados, a criticidade das informações, os requisitos de recuperação, os recursos disponíveis e a aceitação de riscos. Aqui estão exemplos de situações em que uma frequência mais alta ou mais baixa pode ser apropriada:

Frequência Mais Alta:

Ambientes de Transações Financeiras:

Em setores financeiros, onde as transações ocorrem rapidamente e com frequência, backups mais frequentes são essenciais para garantir a integridade dos dados financeiros e para atender a regulamentações rigorosas.

Sistemas de E-Commerce:

Em plataformas de comércio eletrônico, onde as transações são realizadas continuamente, backups frequentes são necessários para capturar as atualizações constantes do inventário, informações do cliente e registros de transações.

Ambientes de Desenvolvimento e Teste:

Em ambientes de desenvolvimento de software, onde as alterações no código-fonte e nos dados são frequentes, backups regulares são cruciais para evitar a perda de trabalho significativo em caso de falha.

Bancos de Dados de Sistemas Críticos:

Sistemas que suportam operações críticas para o negócio, como bancos de dados de sistemas de gestão empresarial (ERP), podem exigir backups mais frequentes para minimizar a perda de dados em caso de falha.

Frequência Mais Baixa:

Dados Estáticos ou de Arquivo:

Para dados que mudam com pouca frequência, como arquivos estáticos ou referências históricas, backups menos frequentes podem ser apropriados, desde que a perda de dados entre os backups seja aceitável.

Sistemas com Recursos Limitados:

Em ambientes com recursos limitados, como largura de banda ou capacidade de armazenamento, pode ser mais prático realizar backups com menor frequência, equilibrando os requisitos de proteção de dados com os recursos disponíveis.

Dados Menos Críticos:

Para dados que são menos críticos para as operações diárias ou cuja perda não teria um impacto significativo, backups menos frequentes podem ser suficientes. Isso pode ser aplicável a dados de teste, por exemplo.

Custos Associados:

Em situações em que os custos associados aos backups frequentes (como armazenamento em nuvem) são proibitivos, pode ser necessário reduzir a frequência dos backups, equilibrando a proteção de dados com considerações financeiras.

Ambientes Menos Dinâmicos:

Em ambientes onde as mudanças nos dados ocorrem raramente e de maneira previsível, backups menos frequentes podem ser adequados, desde que ainda atendam aos requisitos de recuperação.

Em muitos casos, a combinação de diferentes tipos de backups, como backups completos e incrementais, pode ser uma abordagem eficaz para equilibrar a frequência com a eficiência e os recursos disponíveis. É crucial avaliar as necessidades específicas do ambiente e dos dados ao criar um plano de backup.

Parte superior do formulário

5) Existem várias opções comuns de armazenamento para backups, cada uma com suas vantagens e desvantagens. A escolha da solução de armazenamento depende de fatores como a quantidade de dados, a sensibilidade dos dados, os requisitos de recuperação, o orçamento disponível e a infraestrutura existente. Aqui estão algumas opções comuns:

1. Dispositivos de Armazenamento Locais:

Vantagens:

Rápido acesso aos dados.

Controle direto sobre a segurança e privacidade dos dados.

Menos dependência de conexões de rede.

Desvantagens:

Susceptível a danos físicos (incêndio, inundação).

Menor escalabilidade comparado a soluções em nuvem.

Menos prático para backup remoto.

2. Nuvem Pública:

Vantagens:

Alta escalabilidade e flexibilidade.

Acesso remoto aos dados de qualquer lugar.

Geralmente, opções de recuperação rápida.

Desvantagens:

Dependência de conectividade de internet.

Custos contínuos, especialmente para grandes volumes de dados.

Menos controle direto sobre a segurança.

3. Nuvem Privada:

Vantagens:

Maior controle sobre a segurança e privacidade.

Pode ser configurada para atender a requisitos específicos de conformidade.

Flexibilidade na configuração da infraestrutura.

Desvantagens:

Pode ser mais caro de implementar e manter.

Menor escalabilidade em comparação com nuvens públicas.

4. Dispositivos de Armazenamento em Rede (NAS):

Vantagens:

Acesso rápido aos dados em uma rede local.

Pode ser configurado para backup automático.

Oferece alguma redundância e proteção contra falhas de disco.

Desvantagens:

Vulnerável a eventos que afetam toda a rede.

Menos escalável do que soluções em nuvem.

Pode exigir configuração e manutenção especializadas.

5. Tape Backup:

Vantagens:

Baixo custo por gigabyte em comparação com algumas alternativas.

Boa durabilidade e resistência física.

Desconectado quando não em uso, o que pode melhorar a segurança.

Desvantagens:

Recuperação pode ser mais lenta do que em dispositivos de armazenamento mais modernos.

Menos prático para acesso rápido a dados específicos.

Requer cuidado no manuseio físico das fitas.

6. Armazenamento Hiperconvergente:

Vantagens:

Combinação de computação, armazenamento e virtualização em uma única plataforma.

Escalabilidade e flexibilidade.

Recuperação rápida devido à integração próxima com a infraestrutura.

Desvantagens:

Custo inicial pode ser elevado.

Requer habilidades específicas de gerenciamento.

7. Armazenamento em Disco Dedicado para Backup:

Vantagens:

Rápido acesso aos dados.

Configuração simplificada em comparação com algumas opções.

Opções de recuperação rápida.

Desvantagens:

Pode ser mais caro por capacidade de armazenamento do que algumas alternativas.

Menos escalável em comparação com soluções em nuvem.

A escolha da opção de armazenamento dependerá das necessidades específicas de cada organização, levando em consideração fatores como tamanho dos dados, requisitos de recuperação, orçamento, e políticas de segurança e conformidade. Em muitos casos, uma abordagem híbrida que utiliza várias dessas opções pode ser a mais eficaz para garantir redundância e atender a diversos requisitos.

Parte superior do formulário

6) As políticas de retenção em um plano de backup referem-se às diretrizes e práticas que determinam por quanto tempo os dados de backup devem ser mantidos antes de serem removidos ou substituídos. Estas políticas definem a durabilidade e o ciclo de vida dos backups. As políticas de retenção são importantes por várias razões:

1. Otimização do Espaço de Armazenamento:

Políticas de retenção ajudam a otimizar o uso do espaço de armazenamento, evitando que backups antigos e desnecessários ocupem espaço valioso. Isso é crucial para ambientes que têm limitações de armazenamento ou para reduzir custos em soluções de armazenamento em nuvem.

2. Conformidade com Regulamentações:

Em muitos setores, existem regulamentações que ditam por quanto tempo certos tipos de dados devem ser retidos. As políticas de retenção garantem que a organização esteja em conformidade com essas regras e evitem possíveis penalidades legais.

3. Eficiência na Recuperação:

Manter backups desnecessários por longos períodos pode tornar a recuperação de dados mais demorada e complexa. Ao definir políticas de retenção apropriadas, as organizações podem garantir uma recuperação mais eficiente, focando apenas nos dados essenciais.

4. Gerenciamento de Riscos e Segurança:

Reduzir a retenção de dados diminui o risco associado à exposição prolongada de informações sensíveis. Isso é especialmente importante em casos de violações de segurança, onde a exposição de dados deve ser minimizada.

5. Gestão do Ciclo de Vida dos Dados:

As políticas de retenção fazem parte da gestão do ciclo de vida dos dados, ajudando a organizar e controlar o fluxo de informações desde a criação até a destruição ou arquivamento.

6. Economia de Recursos e Custos:

Retirar backups mais antigos que não são mais necessários reduz os requisitos de armazenamento, levando a economias de custo, especialmente em soluções de armazenamento em nuvem que podem ser baseadas em uso.

7. Preservação da História Operacional:

Políticas de retenção permitem que uma organização mantenha um histórico operacional significativo sem acumular uma quantidade excessiva de dados antigos. Isso é útil para análises históricas e para compreender a evolução dos sistemas e dados ao longo do tempo.

8. Ajuste Dinâmico às Necessidades de Negócios:

As políticas de retenção podem ser ajustadas dinamicamente para atender às mudanças nas necessidades de negócios, como novos requisitos de conformidade ou alterações nas prioridades de recuperação.

Ao desenvolver políticas de retenção, é importante considerar os requisitos regulatórios específicos, as características dos dados, as metas de recuperação e as políticas internas da organização. Uma abordagem equilibrada e bem planejada para as políticas de retenção ajuda a garantir a eficácia do plano de backup e a conformidade com as necessidades do negócio.

Parte superior do formulário

7) Garantir a segurança do backup é crucial para proteger os dados contra acesso não autorizado. Aqui estão algumas práticas e medidas que podem ser adotadas para fortalecer a segurança do processo de backup:

1. Criptografia:

Durante a Transferência:

Utilizar protocolos de transferência seguros, como SSL/TLS, para criptografar dados durante a transferência entre sistemas.

Em Repouso:

Armazenar backups criptografados para proteger os dados armazenados contra acesso não autorizado, mesmo se o meio de armazenamento físico for comprometido.

2. Controle de Acesso:

Implementar controles rigorosos de acesso aos sistemas e armazenamento de backup, garantindo que apenas pessoal autorizado tenha permissão para acessar, modificar ou excluir dados de backup.

3. Autenticação Forte:

Utilizar autenticação forte, como autenticação de dois fatores (2FA), para proteger o acesso a sistemas e ferramentas de backup, reduzindo o risco de acesso não autorizado.

4. Monitoramento e Auditoria:

Implementar ferramentas de monitoramento e auditoria para rastrear atividades relacionadas a backups. Isso inclui o monitoramento de acessos, alterações nos dados de backup e eventos de sistema que possam indicar atividades suspeitas.

5. Segregação de Deveres:

Adotar a segregação de deveres para garantir que as responsabilidades relacionadas a backups sejam distribuídas entre várias pessoas, reduzindo assim o risco de abusos de privilégios.

6. Proteção Física:

Garantir a proteção física dos dispositivos de armazenamento de backup para prevenir o acesso não autorizado. Isso inclui restrições de acesso físico às instalações onde os backups estão armazenados.

7. Atualizações e Patches:

Manter sistemas operacionais, software de backup e outras ferramentas atualizados com as últimas correções de segurança e patches para evitar vulnerabilidades conhecidas.

8. Backup Offline:

Manter cópias de backup offline, especialmente para dados críticos. Isso protege contra ataques cibernéticos, como ransomware, que podem mirar em backups online.

9. Testes de Recuperação:

Realizar testes regulares de recuperação para garantir que os dados podem ser restaurados de maneira eficaz e que os procedimentos de segurança associados estão funcionando conforme o esperado.

10. Políticas de Senhas Fortes:

Exigir senhas fortes para contas associadas a sistemas de backup e alterá-las regularmente. Isso ajuda a evitar o acesso não autorizado devido a senhas fracas ou comprometidas.

11. Treinamento e Conscientização:

Educar os usuários e a equipe envolvida nos processos de backup sobre as práticas de segurança, ameaças cibernéticas e os procedimentos adequados para proteger os dados.

12. Firewalls e Segurança de Rede:

Implementar firewalls e medidas de segurança de rede para controlar o tráfego de dados entre sistemas e garantir que apenas comunicações autorizadas ocorram.

13. Contingência e Recuperação de Desastres:

Desenvolver planos de contingência e recuperação de desastres que incluam procedimentos específicos para lidar com violações de segurança nos dados de backup.

A abordagem eficaz à segurança do backup envolve uma combinação dessas práticas para criar camadas de defesa e mitigar riscos. É importante adaptar as estratégias de segurança às necessidades específicas da organização, levando em consideração a sensibilidade dos dados e os requisitos de conformidade.

Parte superior do formulário

8) Realizar testes regulares de restauração de backup é crucial para garantir a eficácia de um plano de backup por várias razões importantes:

1. Validação da Integridade dos Dados de Backup:

Os testes de restauração confirmam se os dados de backup estão íntegros e podem ser recuperados com sucesso. Isso é crucial para garantir que, em caso de falha ou perda de dados, os backups serão realmente eficazes na restauração dos sistemas e informações críticas.

2. Verificação da Consistência dos Backups:

Os testes garantem a consistência dos backups ao longo do tempo. À medida que os dados e os sistemas são alterados, é vital confirmar que os backups continuam a refletir com precisão o estado desejado dos dados em diferentes pontos no tempo.

3. Identificação de Problemas e Inconsistências:

Realizar testes de restauração ajuda a identificar problemas potenciais antes de uma situação de emergência real. Pode revelar falhas nos procedimentos de backup, erros de configuração, ou até mesmo problemas nos próprios dados de backup.

4. Aprimoramento do Processo de Recuperação:

A prática regular de restauração permite que a equipe de TI se familiarize com o processo de recuperação, tornando-o mais eficiente e eficaz em situações de emergência. Isso inclui a compreensão dos procedimentos, o tempo necessário para a recuperação e a resolução de quaisquer obstáculos que possam surgir.

5. Avaliação do Tempo de Recuperação (RTO):

Os testes de restauração ajudam a avaliar e ajustar o Tempo de Recuperação (RTO), que é o período de tempo aceitável para restaurar serviços após uma interrupção. Isso é crucial para garantir que os objetivos de tempo de recuperação sejam atendidos durante uma situação real.

6. Conformidade com Requisitos de Negócios e Regulamentações:

Muitas regulamentações e padrões de segurança, como PCI DSS e GDPR, exigem testes regulares de recuperação de dados para garantir que as organizações estejam em conformidade. A falha em atender a esses requisitos pode resultar em penalidades significativas.

7. Prevenção de Surpresas Desagradáveis:

A realização de testes de restauração regularmente ajuda a evitar surpresas desagradáveis durante situações de emergência. Descobrir que os backups não são restauráveis ou que o processo de recuperação não funciona adequadamente durante uma crise pode ser desastroso.

8. Garantia da Disponibilidade dos Dados Críticos:

Garantir a disponibilidade de dados críticos é vital para as operações comerciais. Os testes regulares garantem que, em caso de falha, os dados necessários estarão prontamente disponíveis para a recuperação.

9. Treinamento e Conscientização da Equipe:

Os testes de restauração proporcionam uma oportunidade para treinar a equipe de TI e outros envolvidos nas práticas de recuperação. Isso aumenta a conscientização sobre o plano de backup e recuperação, melhorando a prontidão da equipe.

Ao realizar testes regulares de restauração, as organizações podem ter confiança na capacidade de seu plano de backup para proteger dados críticos e minimizar o impacto de potenciais eventos adversos. Essa prática é fundamental para manter a resiliência dos sistemas de informação e garantir a continuidade das operações.

Parte superior do formulário