ConversationalGeek®

Infográfico de backup para Microsoft Teams

Por: Brien M. Posey, MVP da Microsoft

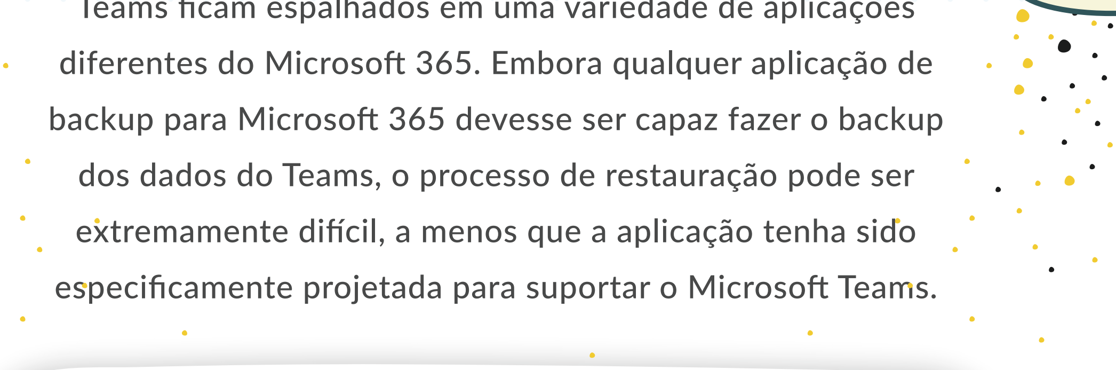
#1 Certifique-se de que você está *fazendo o backup do Microsoft Teams*

Embora pareça completamente óbvio, a melhor prática nº 1 em relação aos backups do Microsoft Teams é se certificar que você está mesmo fazendo o backup do Microsoft Teams (e do resto das aplicações do Microsoft 365).

Um aumento de 18%
no backup terceirizado para o Office 365, que saltou de 27% em 2020 para 45% em 2021.
http://vee.am/DPR21report

50% dos dados perdidos
têm como causa principal os erros humanos, de acordo com a Netwrix Research.
https://hostingtribunal.com/blog/data-loss-statistics/#gref

35% da perda de dados
podem ser atribuídos a falhas de hardware, de acordo com a Netwrix Research
https://hostingtribunal.com/blog/data-loss-statistics/#gref



#2 Adotar uma *solução de backup* que compreenda o Teams

Diferente de aplicações como o Exchange Online ou SharePoint Online, o Teams não armazena todos os seus dados no mesmo lugar. Em vez disso, os dados do Microsoft Teams ficam espalhados em uma variedade de aplicações diferentes do Microsoft 365. Embora qualquer aplicação de backup para Microsoft 365 devesse ser capaz fazer o backup dos dados do Teams, o processo de restauração pode ser extremamente difícil, a menos que a aplicação tenha sido especificamente projetada para suportar o Microsoft Teams.

De acordo com a Tech Radar, a Microsoft revelou em julho de 2021 que tinha 250 milhões de usuários mensais ativos no Teams. Esse é um aumento de mais de 100 milhões, dos 145 milhões informados em abril do mesmo ano.
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

"Mais de 500.000 organizações usam o Microsoft Teams como sua plataforma padrão de mensagens"
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 Usar a *ferramenta certa* para a tarefa

A melhor prática nº 3 para os backups do Microsoft Teams é se certificar de que você esteja usando a ferramenta certa para a tarefa. Há recursos dentro do ecossistema do Microsoft 365, como as políticas de retenção e de retenção de litígio, que podem agir como um pseudobackup. Porém, essas ferramentas existem para fins de conformidade e não para proteção de dados. Assim sendo, elas não protegem adequadamente os dados do Microsoft Teams.

60%
De acordo com a Avast, "60% dos backups estão incompletos". Isso é devido principalmente ao uso de tecnologias de backup desatualizadas pelas empresas
https://invenioit.com/continuity/disaster-recovery-statistics

37%
37% das PMEs perderam dados na nuvem
https://invenioit.com/continuity/disaster-recoverystatistics

#4 Adotar uma *abordagem híbrida* para os backups

A melhor prática nº 4 é adotar uma abordagem híbrida para os backups. Em vez de fazer o backup do Microsoft 365 separadamente das aplicações locais do Microsoft Office, é mais vantajoso usar uma única aplicação de backup que possa proteger simultaneamente os dois ambientes.

O backup está mudando de soluções locais para as soluções baseadas na nuvem e gerenciadas por um provedor de serviços, com uma trajetória relatada de 29% em 2020 para uma previsão de 46% até 2023.

Ao longo dos próximos dois anos, a maioria das empresas esperam reduzir gradualmente seus servidores físicos, além de manter e fortalecer sua infraestrutura virtualizada, adotando estratégias com prioridade para a nuvem. Isso significa que metade das cargas de trabalho de produção serão hospedadas na nuvem até 2023.

https://solutionsreview.com/backup-disasterrecovery/veeam-data-protection-report-2021-shows-58-of-backups-are-failing

#5 Manter os SLAs como *prioridade do seu planejamento de backup*

A melhor prática nº 5 é manter os contratos de nível de serviço (SLAs) como prioridade em seu planejamento de backup. Especificamente, você precisa considerar o Objetivo de Ponto de Recuperação (RPO) e o Objetivo de Tempo de Recuperação (RTO) para o seu ambiente do Microsoft Teams. O RPO determinará a frequência com que os backups serão criados, definindo portanto a quantidade de dados que poderiam ser perdidos entre os backups. O RTO é relacionado ao período de tempo que leva para restaurar um backup.

80%
80% de todas as empresas reconhecem que têm uma "lacuna de disponibilidade" entre a velocidade com que conseguem recuperar aplicações e a velocidade com que essas aplicações precisam ser recuperadas.

76%
Além disso, 76% dessas mesmas empresas dizem possuir uma "lacuna de proteção" entre a frequência do backup dos dados e a quantidade de dados que elas podem perder.

#6 Não ignorar a *granularidade da recuperação*

Uma das melhores práticas, que costuma ser ignorada no backup do Microsoft Teams, é se certificar de que a solução de backup que você está usando oferece recursos de recuperação granular. Embora a capacidade de restaurar uma equipe completa seja importante (ou até múltiplas equipes), é igualmente importante ser capaz de restaurar um arquivo ou um chat dentro de uma equipe.

44% dos administradores de SaaS e 47% dos administradores de backup listam uma restauração melhor, incluindo granularidade, como seu principal motivo para proteger dados do Office 365.
https://www.youtube.com/watch?v=RIHm8-0LUJs

70% das empresas da Fortune 500 compraram o Office 365 em 2020
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 Usar o backup para aumentar seus *recursos de descoberta eletrônica*

O Microsoft 365 incluiu há muito tempo recursos de descoberta eletrônica, que permitem que a organização localize dados específicos dentro do ecossistema do Microsoft 365 em resposta a uma intimação. Embora os recursos nativos de descoberta eletrônica tenham seus usos, muitas vezes é mais eficaz usar o software de backup no processo de descoberta.

Uma pesquisa da Disruption in eDiscovery descobriu que "pelo menos 58% do público usou a tecnologia de descoberta eletrônica para questões não relacionadas a processos ou disputas, pelo menos 'em várias ocasiões'". Isso ilustra que a descoberta eletrônica não está mais limitada aos litígios.

$12.9 Billion
O mercado da descoberta eletrônica tem uma previsão de crescimento de US$ 12,9 bilhões até 2025

*https://ediscoverytoday.com/2020/08/31/here-are-some-disruptivestats-in-discovery-ediscovery-trends

**https://www.prnewswire.com/newsreleases/global-12-9-billion-ediscovery-market-forecast-to-2025---focus-on-proactive-governance-withdata-analytics-and-the-emergence-of-new-content-sources-301231643.html

#8 Defender o Teams *contra o ransomware*

Outra melhor prática é se certificar de que você esteja protegendo seus dados do Microsoft Teams contra o ransomware. Ao contrário do que muitos acreditam, os dados armazenados no Microsoft 365 podem ser criptografados por ransomware. O fato de que muitas pessoas ainda estão trabalhando remotamente a partir de dispositivos pessoais aumenta muito o risco de uma infecção por ransomware. Um bom backup é a melhor defesa contra a perda de dados relacionada ao ransomware.

De acordo com o Ponemon Institute, somente **45% das empresas** acreditam que possuem um orçamento de segurança virtual adequado

De acordo com o IDC, **69% das empresas** sofreram ataques de malware bem-sucedidos em um prazo de 12 meses, e 39% dos ataques envolviam ransomware

*https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf)

**https://www.veeam.com/why-backup-office-365.html

#9 Garantir que o seu *Storage* ofereça *flexibilidade*

Ao selecionar uma aplicação de backup para o Microsoft Teams, é importante garantir que a solução dê a você a liberdade de escolher seu próprio storage, independentemente de onde o storage esteja localizado. Assim, as empresas podem escolher uma camada de storage que ofereça o desempenho e a resiliência que o negócio exige, pelo melhor custo possível. Ter flexibilidade de storage também dá às empresas a opção de gravar backups em storage imutável se desejarem, protegendo os backups contra ataques de ransomware.

A CAN Financial estabeleceu um recorde mundial em 2021, quando a empresa pagou um resgate de US$ 40 milhões.

Uma pesquisa de 2021, feita pela Sophos, descobriu que "7% das empresas dos entrevistados foram atacadas por ransomware no ano passado"

*https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5).

**https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-ofransomware-2021-wp.pdf?cmp=120469

#10 Foco na *facilidade de uso*

Algumas aplicações de backup têm a reputação de serem muito complexas de configurar e usar. O problema com isso é que a complexidade aumenta as chances de erro humano. Se uma empresa seleciona uma aplicação de backup intuitiva e fácil de usar, isso pode reduzir as chances de que ocorram falhas no backup ou na recuperação por causa de erros humanos.

De acordo com a FEMA, de 40% a 60% das pequenas empresas jamais reabrirão após um evento de perda de dados
https://hostingtribunal.com/blog/data-loss-statistics/#gref

58%
De acordo com um estudo de 2021, 58% dos backups falham durante as tentativas de restauração

*https://www.continuitycentral.com/index.php/news/technology/6092-survey-finds-that-58-percent-ofdata-backups-fail-when-restoration-is-attempted

ConversationalGeek® ©2022 Conversational Geek
Patrocinado por veeam