86 – Abril 2007

Fantasmas do Backup

Copias de seguranca ou simplesmente backups nos acompanham há tempos, mas não é por isso, que tenham deixado de ser um grande aborrecimento mesmo nos dias de hoje.
Tornam-se um problema quando precisamos deles acessíveis, funcionando e prontos para recuperar informações destruídas por erros, acidentes e sabotagens, mas também representam um grande desafio no momento de definir o que fazer, como fazer, como que freqüência fazer e como administrar os riscos residuais da adoção de uma solução de backup.

Muitas perguntas surgem no momento de escolher uma solução e um processo de backup, especialmente para o usuário final:

- Que mídia será capaz de armazenar todos os meus dados e mantê-los acessíveis ao longo do tempo?
- Com que freqüência devo realizar as copias de segurança sem que as perdas de um incidente sejam grandes?
- Como manter minhas cópias de segurança atualizadas sem ter de realizar o backup full periodicamente?
- Quantas cópias de segurança eu devo manter e onde devem ser armazenadas?
- O que fazer para evitar que uma cópia de segurança corrompida sobrescreva uma cópia de segurança íntegra antes que processo seja irreversível?
- Em caso de recuperação, como identificar o que foi perdido pelo gap entre os dados atualizados e a última cópia de segurança?
- Existe solução de software capaz de realizar cópias de segurança integrando meus dados distribuídos entre computador, telefone, PDA e outros dispositivos móveis?
- Como manter a segurança dos dados armazenados pelas cópias de segurança sem que isso represente um problema para mim mesmo no momento de restaurá-las?

E esta é só uma pequena mostra dos aspectos que rondam as cópias de segurança. Refletem a realidade de muitos usuários que acabam convivendo com questões não respondidas na esperança de nunca precisar de uma cópia backup de verdade.

Talvez algumas destas perguntas permaneçam sem resposta aqui, onde é impossível detalhar cada caso e cenário considerando que existem dados e usuários com sensibilidades distintas, além de dispositivos e ambientes operacionais com características diferentes, mas já podemos endereçar o assunto de forma conceitual.

- O primeiro passo é avaliar a sensibilidade para a perda de seus dados. Isso pode ser feito medindo o impacto da perda de forma qualitativa ou quantitativa, esta última, permitindo maior precisão ao tangibilizar a extensão de um acidente. Com isso em mente e considerando seu volume de produção de conteúdo, já é possível fazer um *short list* dos seus requerimentos, ou seja, velocidade, capacidade de armazenamento, quantidade e periodicidade.

- Considere mídias e equipamentos de backup de alta qualidade fabricados por empresas que tenham histórico rico de pesquisa, desenvolvimento e larga absorção de suas soluções pelo mercado, para que você reduza os riscos de descontinuidade do produto e de suporte ao longo do tempo. Mas atenção, não há nada que garanta que seu backup poderá ser lido na próxima década, por isso, estar atento às mudanças e acompanhá-las é fundamental para garantir seu sono. Se for preciso mudar de solução, mude enquanto há tempo.

- Quanto à freqüência e ao método de backup, existem muitas soluções que oferecem o recurso de agendamento de cópias periódicas e ainda os métodos mais utilizados de cópia completa e cópia incremental, esta última capaz de comparar a última versão com seu disco atual para identificar as mudanças e capturá-las. De qualquer forma, o nível de parametrização e controle deverá ser compatível com os seus requerimentos, por isso, avalie e teste o máximo de soluções que puder para encontrar aquela perfeita para você, afinal, é para você que o software tem que trabalhar quando o céu cair sobre sua cabeça.

- Garantir a saúde das cópias é outro aspecto importante. Não basta fazer a cópia regularmente, é preciso também mantê-la em local adequado para evitar danos físicos à mídia, assim como para evitar que a mesma acidente/ameaça que venha a afetar seu disco principal também o faça com a cópia de segurança, como seria o caso de um incêndio, por exemplo.

- Saber o que se perdeu em uma recuperação ou ainda evitar que uma cópia danificada sobrescreva outra saudável não é tarefa fácil e mais uma vez, a resposta dependerá de sua sensibilidade e da robustez da solução adotada. Muitas delas realizam testes antes de iniciar uma restauração, mas não estou apenas falando disso. Considero também o erro do usuário, que ao apagar acidentalmente um arquivo do disco principal, quando se dá conta do engano e resolve restaurar o backup, percebe que o último backup já fora feito sem o arquivo apagado e não existem mais cópias para recuperá-lo. Neste caso, só mesmo um rodízio estruturado de cópias em que os discos são individualmente designados para cópias com periodicidades diferentes, sendo na maioria dos casos feitos anualmente, trimestralmente, mensalmente e diariamente, dependendo da sensibilidade.

- Integração de dados distribuídos e a proteção dos dados armazenados nas cópias de backup são um respeitável problema. Parece uma balança de difícil equilíbrio, pois ou se decide multiplicar as cópias para cobrir situações rigorosas de recuperação e assim se tem aumentado o trabalho de controle e também o risco de ter os dados vazados de uma das cópias, ou se reduz o número de cópias, o esforço de controle,

os risco de vazamento, mas se tem aumentado o risco de indisponibilidade de recuperação. Nesta encruzilhada, sua sensibilidade deve falar mais alto, além de considerar as reais possibilidades de se manter um complexo processo de backup. Em caso de necessidade você vai perceber que é melhor tem um processo simples bem executado do que um processo complexo que seja falho, por isso, aumente a robustez da sua solução à medida que puder suportá-la com qualidade.

- O último e não menos importante aspecto está relacionado à forma de proteção e acesso aos dados backupeados. Na minha humilde opinião, não existe forma mais segura do que aplicar criptografia forte ao processo de cópia de segurança, mas lembre-se que isso pode ainda trazer dor-de-cabeça para o usuário mais sensível ao tempo de recuperação. Isso por que o método tende a tornar o processo mais lento e ainda oferecer o risco real do usuário não poder restaurar e acessar seus próprios dados caso haja perda da chave de criptografia. Este é, portanto, mais um momento de escolha, apesar de estar convencido de que definindo bem a estrutura de backup, armazenamento das chaves criptográficas e mantendo uma boa documentação, o usuário poderá definitivamente "descansar".

  Bom backup a todos. Sucesso!

Marcos Sêmola *é Diretor de Operações de Security & Information Risk da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, certificado CISM, BS7799 Lead Auditor, Membro da ISACA, ISSA, CSI e fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV, Pós Graduado em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Premiado SecMaster® em 2003 e 2004, tornando-se membro da comissão em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*