RECOMENDAÇÕES PARA PRÁTICAS DE *BACKUP* DE DADOS

Eliana Márcia Moraes[1], José Alberto Fernandes Ferreira[2], Marcio Lourival Xavier dos Santos[3]

[1]Mestranda em Gestão e Desenvolvimento Regional - Universidade de Taubaté – Rua Visconde do Rio Branco, 210 Centro - 12020-040 - Taubaté - SP - Brasil - eliana@unitau.br

[2]Doutor - Professor no Mestrado em Gestão e Desenvolvimento Regional - MGDR - Universidade de Taubaté – Rua Visconde do Rio Branco, 210 Centro - 12020-040 - Taubaté - SP - Brasil - jaff@unitau.br

[3]PhD - Orientador no Mestrado em Gestão e Desenvolvimento Regional - MGDR - Universidade de Taubaté – Rua Visconde do Rio Branco, 210 Centro - 12020-040 - Taubaté - SP - Brasil – marcio@unitau.br

Resumo- O objetivo deste artigo é demonstrar a importância e as recomendações para estratégias de *backup* de dados. Para atingir a finalidade proposta, foram pesquisados documentos encontrados na Internet, e referências já publicadas sobre indicações e normas para *backup* de dados, elaboradas por entidades reconhecidas, por possuírem e estabelecerem melhores práticas na área de Segurança da Informação. Com o decorrer deste artigo, será mostrada a importância de se investir em Segurança da Informação e como os dados devem ser protegidos. Conclui-se com um resumo das estratégias, de maior incidência, recomendadas para práticas de *backup* de dados.

Palavras-chave: *Backup* de Dados, Estratégia, Segurança da Informação.
Área do Conhecimento: Ciências Sociais Aplicadas

Introdução

No mundo dos negócios, as informações armazenadas nos computadores têm um valor incalculável, e dependendo do porte da Organização, a falta dessas informações pode significar a falência. As exigências legais do Governo e Organismos Reguladores nacionais e internacionais também requerem a guarda de algumas informações por anos. Em caso de perda de dados, é essencial poder recuperá-los, para isto é preciso o *backup* (Cópia segura).

As bases de dados crescem consideravelmente, fazendo-se necessárias estruturas eficientes para o armazenamento e recuperação dos dados. Para a proteção das informações e para a prevenção de perdas são elaboradas e estabelecidas Políticas de Segurança e Planos de Continuidade de Negócios, e nestes estão as práticas de *backup* de dados. Para que sejam eficientes é necessário um planejamento estratégico, onde haja a análise das necessidades dos usuários e do ambiente, a classificação das informações, análise de riscos para o negócio e outras que se façam presentes, além de aplicar as boas práticas publicadas, para a decisão de onde, como, quando, e quanto investir para a proteção dos dados críticos.

Busca-se, neste estudo resumir as principais estratégias de *backup* de dados recomendadas por especialistas no assunto Segurança da Informação, como o *NIST (National Institute of Standards and Technology)*, a ABNT (Associação Brasileira de Normas Técnicas), que elaborou a NBR 17799 (Código de Prática para a Gestão da Segurança da Informação), e outros documentos nacionais e internacionais, visto que a Segurança da Informação é um objetivo mundial.

Materiais e Métodos

Os materiais utilizados para este trabalho são normas e indicações para práticas de *backup* de dados, publicadas na área de Segurança da Informação por especialistas neste assunto. O método para se chegar ao objetivo proposto, que são as principais recomendações para práticas de *backup* de dados, é análise e resumo do material coletado.

Conforme Massiglia (2001, tradução nossa), a informação, além de ser classificada, confiável, rápida e gerenciável deve ser à prova de desastres: Os dados eletrônicos e as aplicações têm que estar disponíveis, mesmo que haja incêndio, inundação, ou qualquer tipo de falha da natureza ou não.

Os *backups* precisam de um plano claro, que se encontre com os objetivos específicos de cada negócio. Os administradores de armazenamento devem desenvolver e manter uma estratégia de *backup* contínua que proteja os dados relevantes, usando a plataforma de *backup* apropriada, e esta estratégia deve evoluir, de acordo com a evolução da organização, para que os dados fiquem seguros, recomenda Bigelow (2006, tradução nossa).

De acordo com Bigelow (2006, tradução nossa), os administradores devem fazer a triagem dos dados, alocando recursos de *backup* principalmente para as aplicações mais importantes.

Segundo Swanson et al. (2002, tradução nossa), é uma boa prática armazenar o *backup* remotamente. As instalações comerciais de armazenamento de dados são projetadas especialmente para arquivar mídias e proteger os dados de ameaças.

A NBR ISO/IEC 17799 (ABNT, 2001), indica que um nível mínimo de cópias de segurança (*backup*), juntamente com o controle consistente e atualizado dessas cópias e com a documentação dos procedimentos de recuperação, seja mantido em local remoto, a uma distância suficiente para livrá-lo de qualquer dano que possa ocorrer na instalação principal. Convém que no mínimo três gerações ou ciclos de cópias de segurança das aplicações críticas sejam mantidos.

Existem muitos tipos de *backups*. Antes de considerar que tipo de estratégia de *backup*, a se adotar, é preciso avaliar as exigências do usuário, bem como as instalações do ambiente, recomenda Zhu et al. (2005, tradução nossa).

Segundo Garfinkel (2004, tradução nossa), os *backups* são como um seguro que protege em casos de desastres e erros. Por exemplo, um *backup* feito diariamente pode recuperar um arquivo acidentalmente perdido ou um *hd* (*hard disk*) formatado. Os *backups* semanais são vitais para recuperar arquivos importantes que não são usados sempre, como arquivos de configuração dos sistemas. Os *backups* trimestrais e anuais podem ser realmente úteis em disputas de patente e em outros tipos de litígio. Estes *backups* podem também recuperar memorandos e mensagens de e-mail que foram apagadas ou perdidas há muito tempo.

Segundo Swanson et al. (2002, tradução nossa), as políticas de *backup* devem especificar a freqüência dos *backups* (por exemplo, diário ou semanal, incremental ou completo), baseada na importância dos dados e na freqüência em que informação nova é introduzida. Elas devem designar a posição de dados armazenados, procedimentos de nomeação de arquivos, freqüência de rotação das mídias, e método para transportar os dados.

Resultados

Após a revisão da literatura sobre práticas de *backup*, é possível resumir as recomendações nos seguintes itens:

- Elaborar um plano de *backup* de dados, que deve ser revisado e testado periodicamente e onde apenas os dados relevantes sejam resguardados, diminuindo tempo, custo e espaço para o *backup* e recuperação dos dados.

- Armazenar os dados, mídias e documentação do *backup* em local remoto, com segurança física e lógica, que seja distante dos dados originais, evitando que um desastre possa afetar os locais ao mesmo tempo.

- Para os dados críticos são necessárias três gerações de *backup*.

- O *backup* deve ser agendado, podendo ser diário, semanal ou a todo o momento, dependendo do valor da informação.

Discussão

O resumo de algumas recomendações relevantes sobre *backup* de dados foi colocado neste artigo em modo simples e pode ser consultado de maneira rápida, ajudando no planejamento, execução e controle do plano de *backup* de dados.

As recomendações mostram que antes de se planejar o *backup* é preciso classificar a informação, e esta também deve ser resguardada, antes de se fazer o *backup*, ou seja, é necessário que os dados sejam compactados, cifrados e que estejam com permissões de acesso apenas aos autorizados. A documentação de todo processo é essencial (e desta também é preciso fazer *backup)* para a recuperação das informações. Nesta documentação também devem ser colocados os responsáveis pelos *backups* e os contatos dos mesmos.

Uma equipe deve ser formada para analisar os interesses para o *backup* das informações e fazer o planejamento, onde muitos detalhes e particularidades de cada negócio devem ser considerados, ou seja, cada negócio terá um plano único de *backup* de dados, mas as recomendações apresentadas servem como base para todos os planos.

Conclusão

O risco de se perder os dados mantidos nos computadores, devido às ameaças, aumenta a preocupação em se manter a disponibilidade, confidencialidade e integridade das informações. Para manter a segurança dos dados, além de outras medidas, é necessário que as estratégias para *backup* de dados façam parte do planejamento estratégico das Empresas, e que sejam testadas e analisadas continuamente para serem válidas, mesmo com mudanças no ambiente de negócios.

Através deste artigo, que evidencia as principais recomendações para *backup* de dados, é possível facilitar o planejamento, segundo melhores práticas, embora cada negócio terá estratégias únicas de *backup* de dados.

Este trabalho serve como início para outras pesquisas, há muito para ser explorado. Algumas sugestões são como classificar a informação, como definir o quanto investir, como calcular o retorno do investimento em *backup* de dados, entre outras.

Referências

ABNT. Tecnologia da informação – Código de prática para a gestão da Segurança da Informação (NBR ISO/IEC 17799). Rio de Janeiro: 2001.

BIGELOW, S. J. *Backup* Strategies. 2006. Disponível em: http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1179087,00.html. Acesso em: 01 jun. 2006.

GARFINKEL, S. Calling for *Backup*: Backing up your data might not seem important until you need to retrieve it. 2004. Disponível em: http://www.csoonline.com/read/030104/shop.html. Acesso em 23 ago. 2005.

MASSIGLIA, P. Veritas in E-Business. Veritas Software Corporation, 2001.

- SWANSON M.; WOHL A.; POPE L.; GRANCE T.; HASH J.; THOMAS R. Contingency Planning Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology, 2002. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf. Acesso em: 31 mar. 2006.

ZHU W-D.; ABRHAMS M.; NGAI D.M.M.; POND S.; SCHIAVI H.; SHAZLY H.A.; STONESIFER E.; STONESIFER V. Content Manager OnDemand *Backup*, Recovery, and High Availability, 2005. Disponível em: http://www.redbooks.ibm.com/redbooks/pdfs/sg246444.pdf. Acesso em: 18 mai. 2006.