REFERENCE NORMS FOR DATA BACKUP AND INFORMATION SECURITY

Eliana Márcia Moraes - Universidade de Taubaté - São Paulo - Brasil
eliana@unitau.br
José Alberto Fernandes Ferreira - Universidade de Taubaté - São Paulo - Brasil - jaff@unitau.br
Marcio Lourival Xavier dos Santos - Universidade de Taubaté - São Paulo - Brasil - marcio@unitau.br

The present article shows that by keeping adherence to the NBR ISO/IEC 17799 ABNT guidelines one can write efficient data backup rules, to be inserted into a given Information Security Policy proposal. The importance of following the NBR ISO/IEC 17799 has come to light through a research including internet documents from secure sources, books and other references on the importance of data backup to Information Security, Security Policies and their relation with the NBR ISO/IEC 17799 regarding the best practices for protecting data. The main rules for data backup as stated in the NBR ISO/IEC 17799 have been studied, which has lead to demonstrating how they can be rendered into practices by the actual Information Technology administrator when devising secure data backup procedures. Also, the analysis of the answers of a selected group of Information Security professionals to a questionnaire elaborated to reveal if the respondent would keep adherence to the NBR ISO/IEC 17799 has shown that the vast majority does so, confirming the importance of the ISO document as a main guide to data backup procedures.
Keywords: Information Security. Security Policy. NBR ISO/IEC 17799. Data Backup.

NORMAS DE REFERÊNCIA PARA BACKUP DE DADOS E SEGURANÇA DA INFORMAÇÃO

No presente artigo busca-se demonstrar como a aderência à NBR ISO/IEC 17799 da Associação Brasileira de Normas Técnicas contribui para a elaboração eficaz de normas de Backup de dados, a serem inseridas em Políticas de Segurança da Informação. Para atingir o objetivo proposto foram pesquisados, além da NBR ISO/IEC 17799, documentos de fontes seguras encontrados na Internet, livros e outras referências sobre a importância da Segurança da Informação, Políticas de Segurança e Backup de Dados e sua relação com a norma NBR ISO/IEC 17799 da ABNT, para a melhor proteção dos dados. Foram abordadas as principais normas para backup de Dados, recomendadas pela NBR ISO/IEC 17799 da ABNT, e porque devem ser adotadas pelos Administradores de Tecnologia da Informação na criação de procedimentos para backup seguro dos dados. Também foi realizada uma pesquisa de campo através de questionário, respondido por profissionais da área de Segurança da Informação, para saber se utilizam a NBR ISO/IEC 17799, e finalmente é apresentada a conclusão da pesquisa que confirma a utilização da NBR ISO/IEC 17799 como importante guia para normas de backup de dados.
Palavras chaves: Segurança da Informação. Política de Segurança. NBR ISO/IEC 17799. Backup de Dados.

1. INTRODUÇÃO

Há algum tempo o *backup* simplesmente significava cópia de segurança. Entretanto, no ambiente de Tecnologia da Informação, o *backup* e a proteção dos dados são utilizados para prover continuidade de negócios, replicação de dados, recuperação de desastres e redução nos custos de infra-estrutura. Porém a melhor maneira para assegurar os dados, seja local ou remotamente, pode ser um desafio desanimador, se não forem estabelecidas normas estratégicas para este fim.

Para a proteção das informações e para atenderem a padrões de segurança e regulamentações governamentais, as organizações estabelecem um conjunto de Políticas de Segurança da Informação. Para auxiliar na elaboração de Políticas de Segurança da Informação existe a norma NBR ISO/IEC 17799 homologada pela Associação Brasileira de Normas Técnicas, que é um conjunto de normas e padrões, baseados em melhores práticas.

Mesmo estabelecendo políticas de segurança, as organizações não estão livres de erros humanos, ataques de vírus, catástrofes naturais, e outras ameaças. E caso ocorram perdas de informações é preciso recuperá-las, e isto se torna possível se o processo de *backup* e recuperação de dados for seguro.

Este artigo aborda as principais normas de *backup* de dados recomendadas pela NBR ISO/IEC 17799 a serem incluídas no conjunto de políticas de segurança de uma organização. A partir destas recomendações, os analistas de Tecnologia da Informação podem criar um conjunto de procedimentos sob medida, ou seja, de acordo com a dinâmica da organização, para o processo de *backup* de dados e assegurar que as cópias estão dentro de um padrão de segurança de referência. O papel essencial da estruturação da prática de *backup* segundo NBR ISO/IEC 17799 é enfatizado.

2. METODOLOGIA

Os materiais utilizados para este trabalho são normas e indicações para política de *backup* de dados, publicadas na área de Segurança da Informação por especialistas neste assunto, como o *National Institute of Standards and Technology* (NIST), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), e principalmente a NBR ISO/IEC 17799 de 2005 da Associação Brasileira de Normas Técnicas (ABNT).

Além das referências teóricas são utilizados os resultados de um questionário, respondido por profissionais da área de Tecnologia da Informação, sobre a utilização da NBR ISO/IEC 17799 para o planejamento de *backup* de dados. Os profissionais que responderam ao questionário trabalham a mais de um ano na área de Segurança da Informação e são responsáveis pelos dados nas organizações onde trabalham, e a maioria possui cursos na área de Segurança da Informação.

O método para se chegar ao objetivo proposto, que é a abordagem das normas de *backup* de dados proposta pela NBR ISO/IEC 17799, é o resumo e a análise do material coletado.

3. SEGURANÇA DA INFORMAÇÃO

No mundo globalizado, as informações são o ativo mais valioso para a maioria das organizações, e com o acréscimo do volume e a rapidez com que as informações precisam ser acessadas, as organizações estão cada vez mais dependentes das Tecnologias de Informação (TI), que precisam ter e oferecer segurança adequada.

A NBR ISO/IEC 17799 (ABNT, 2005), explicita que a Segurança da Informação (SI) é caracterizada pela preservação de:

a) confidencialidade: garantia de que a informação é acessível somente aos usuários autorizados;

b) integridade: garantia de que as informações não sejam alteradas indevidamente;

c) disponibilidade: garantia de que os usuários autorizados tenham acesso à informação sempre que preciso.

O objetivo principal da SI deve ser resguardar a informação importante para a organização e não apenas o software, hardware ou mídias que a mantém.

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005), a SI é obtida a partir da implementação de uma série de controles que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos para garantir que os objetivos de segurança da organização sejam atendidos.

A SI é fundamental, e para que ela seja estabelecida nas organizações é preciso a elaboração de um conjunto de políticas de SI por meio do conhecimento das particularidades de cada negócio.

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conforme Gonçalves (2002), as Políticas de SI são um conjunto de diretrizes, regras bem determinadas e práticas, que regulam como uma organização deve gerenciar, proteger e distribuir suas informações e recursos. A Política de SI e outros controles de segurança tem a finalidade de procurar garantir que a SI seja mantida, e que os dados armazenados nos computadores sejam confiáveis e disponíveis.

O objetivo da criação de Políticas de SI, segundo a NBR ISO/IEC 17799 (ABNT, 2005), é o de prover uma orientação e base para a SI. Convém estabelecer uma Política clara, com apoio e comprometimento com a SI para toda a organização.

Para facilitar a elaboração de Políticas de SI, foi estabelecida pela ABNT a NBR ISO/IEC 17799, com padrões de metodologia de implementação de segurança. A NBR ISO/IEC 17799 é equivalente à norma ISO 17799, proveniente da BS 7799, criada pelo BSI (*British Standards Institute*) em 1995, que é um conjunto de padrões britânicos, o primeiro documento a ser reconhecido internacionalmente como guia de práticas de SI.

Segundo a NBR ISO/IEC 17799 (ABNT, 2005), no mínimo, convém que as seguintes orientações sejam incluídas no conjunto de Políticas de SI de uma organização:

- Definição de SI, resumo das metas e escopo e a importância da segurança, como um mecanismo que capacita o compartilhamento da informação;
- Declaração do comprometimento da alta direção, apoiando as metas e princípios da SI;
- Estrutura para estabelecer os objetivos de controles, incluindo a estrutura de análise, avaliação e gerenciamento de risco;
- Explicação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
    - conformidade com a legislação e cláusulas contratuais;
    - requisitos de conscientização e treinamento de segurança;
    - gestão de continuidade de negócios;
    - conseqüências das violações na política de SI;
- Definição das responsabilidades gerais e específicas na gestão da SI, incluindo o registro dos incidentes de segurança;
- Referências à documentação que possam apoiar a política.

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005), o documento da Política de SI deve ser aprovado pela direção, publicado e comunicado, através de toda a organização para os usuários na forma que seja relevante, acessível e compreensível para o leitor interessado.

O principal objetivo da Política de SI é proteger as informações e os recursos computacionais que as comportam, e é essencial que o conjunto de políticas de SI, estabelecido pelas organizações, contenha normas para *backup* de dados.

5. RECOMENDAÇÕES PARA NORMAS PARA *BACKUP* DE DADOS

As normas para *backup* de dados devem ser incluídas no conjunto de Políticas de SI de modo que sejam preservados os requisitos de confidencialidade, integridade e disponibilidade dos dados.

Segundo Gonçalves (2002) a criação de uma Política de SI precisa de esforços entre o pessoal técnico e o pessoal responsável pelas decisões da organização. É importante fazer uma avaliação dos riscos envolvidos para decidir o que realmente precisa ser protegido e a quantidade de recursos que devem ser utilizado para a economia dos mesmos.

As principais recomendações para normas de *backup* de dados apontadas pela NBR ISO/IEC 17799 são encontradas no capítulo “10.5.1 Cópias de segurança das informações”, e são abordadas a seguir.

5.1 Política de *backup* de Dados

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005), as cópias de segurança das informações e dos sistemas devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança estabelecida.

Segundo Swanson et al. (2002), as políticas de *backup* devem especificar a freqüência dos *backup*s (por exemplo, diário ou semanal, incremental ou completo), baseada na criticidade dos dados e na freqüência em que informação nova é introduzida. Elas devem designar o local de dados armazenados, procedimentos de nomeação de arquivos, periodicidade de trocas das mídias, e os métodos para transportar os dados, além de outros requisitos para *backup* de dados.

É importante que seja estabelecida a política de *backup* de dados, que faz parte da Política de SI, e que haja o comprometimento dos usuários, através de conscientização, treinamentos e auditorias periódicas e com punições para os casos omissos ou do não cumprimento das normas.

5.2 Diretrizes para implementação

Conforme a NBR ISO/IEC 17799 (ABNT, 2005), recursos adequados para a geração de cópias de segurança devem ser disponibilizados para garantir que toda informação e sistemas essenciais possam ser recuperados após a perda de dados devida a desastres, erros, falhas de mídias ou outros fatores.

Para que a Política de *backup* se torne válida é necessária aprovação da alta direção da organização, e que sejam direcionados os recursos para o cumprimento da mesma.

Segundo Gonçalves (2002), para que a implantação de uma Política de Segurança se torne adequada e efetiva em qualquer organização, é de suma importância o envolvimento de profissionais de todos os níveis, inclusive da alta direção, e que esses suportem de forma completa o processo, caso contrário, haverá poucas chances de que ela obtenha o impacto desejado.

É importante considerar os seguintes itens para a geração das cópias de segurança:

5.2.1 Níveis de *backup*

Segundo a ISO/IEC 17799 (ABNT, 2005), é importante definir o nível necessário das cópias de segurança dos dados. É a classificação das informações que determinará quantos níveis de *backup* serão necessários. Para as informações críticas recomendam-se três níveis de *backup*, que podem ser, por exemplo, *backup* em disco local, outro em mídia removível, fitas, e *backup* remoto.

Os *backup*s precisam de um plano claro, que esteja de acordo com os objetivos específicos de cada negócio. Para isso é importante desenvolver e manter uma estratégia de *backup* contínua que proteja os dados relevantes, usando a plataforma de *backup* apropriada. Esta estratégia deve evoluir de acordo com o desenvolvimento da organização para que os dados fiquem seguros, recomenda Bigelow (2006).

5.2.2 Registro e documentação

Registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de recuperação dos dados devem ser mantidos, recomenda a ISO/IEC 17799 (ABNT, 2005).

Conforme Zhu et al.(2005), para reduzir o tempo de recuperação, há diversos pontos a considerar, e um deles é ter documentos de procedimentos de recuperação para situações diferentes. Para cada situação é importante ter um plano de recuperação dos dados, onde estejam as ações a serem tomadas e os contatos dos responsáveis para recuperar os sistemas.

5.2.3 Extensão e Freqüência

De acordo com a ISO/IEC 17799 (ABNT, 2005), a extensão (por exemplo, completa ou diferencial) e a freqüência da geração das cópias de segurança devem refletir os requisitos dos negócios da organização, além dos requisitos de SI e ser de acordo com a criticidade da informação.

O *backup* completo é a cópia e guarda de todos os dados do sistema. Já o *backup* diferencial é o *backup* apenas dos dados modificados depois do *backup* completo. Em todos os casos a freqüência do processo de *backup* tem que ser adequada aos negócios da organização, como por exemplo, todos os dados têm que ser copiados e mantidos em caso de recuperação mandatória.

Segundo Garfinkel (2004), 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 utilizados sempre, como arquivos de configuração e inicialização de sistemas. Os *backups* trimestrais e anuais podem ser realmente úteis em disputas de patente, em outros tipos de litígio e na manutenção de históricos em geral.

5.2.4 Localidade remota

A ISO/IEC 17799 (ABNT, 2005) recomenda que as cópias de segurança sejam armazenadas em um local remoto, a uma distância suficiente para evitar danos advindos de um desastre ocorrido no local principal onde os dados são armazenados.

De acordo com Swanson et al. (2002), é boa prática armazenar os dados remotamente em instalações de armazenamento de dados que sejam projetadas especialmente para arquivar mídias e proteger os dados de ameaças.

O episódio ocorrido em onze de setembro de 2001 no *World Trade Center* em Nova Iorque, onde foram destruídas as torres gêmeas, e com elas sistemas de computadores de organizações que mantinham dados principais em uma torre e o *backup* na outra, mostra o quanto é importante pensar na distância e na segurança física do *backup* remoto.

Segundo Farias Junior (2002), o *Deutsche Bank*, com dois escritórios funcionando no *World Trade Center*, tinha um site de *backup* remoto instalado em local afastado da sede, com cópias de todos os arquivos importantes atualizados. Assim, no dia seguinte ao atentado terrorista, o *Deutsche Bank* já operava os seus sistemas quase que normalmente.

5.2.5 Proteção física e ambiental

A ISO/IEC 17799 (ABNT, 2005) indica que deve ser dado um nível apropriado de proteção física e ambiental às cópias de segurança. Esta proteção, tanto no local de armazenamento local e remoto, deve estar de acordo com as normas aplicadas na instalação principal.

É importante avaliar as exigências do usuário bem como as instalações do ambiente, antes de se considerar que tipo de estratégia de *backup* de dados adotar, recomenda Zhu et al. (2005).

No local onde são guardados os *backup*s, alguns cuidados devem ser considerados. Segundo CERT (2003), o local deve ser restrito para evitar que pessoas não autorizadas tenham acesso aos *backup*s e protegido contra agentes naturais prejudiciais aos dados ou recursos computacionais, como poeira, calor, umidade, incêndio, etc.

5.2.6 Testes e Reciclagem

As mídias de cópias de segurança precisam ser testadas regularmente, adverte a ISO/IEC 17799 (ABNT, 2005), para garantir que elas estejam suficientemente confiáveis para a recuperação, quando necessária.

Segundo Cook (2006), a falha de mídias é a falha mais comum, tratando-se de *backup* e recuperação de dados. Portanto é importante tratar as mídias com cuidados, seguindo as instruções do fabricante. No caso de fitas é importante saber como deve ser feita a manipulação, o armazenamento, a reciclagem e a limpeza de *drives*. As fontes redundantes nos equipamentos computacionais são importantes para proteção de *backup*s de dados em disco.

As máquinas alvo para a reprodução das mídias e elas próprias devem ser recicladas, caso ocorram degraus de inovação tecnológica, para evitar a obsolescência em *backup*s de longa permanência.

5.2.7 Testes dos Processos

Os procedimentos de recuperação precisam ser verificados e testados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação, aconselha a ISO/IEC 17799 (ABNT, 2005).

Segundo Cook (2006), a melhor prevenção contra a maioria dos erros de *backup* é o treinamento, que deve envolver as melhores práticas, e ter certeza do entendimento dos usuários sobre o *backup* e recuperação, e sobre o que elas devem ou não fazer para salvar e recuperar os dados.

Os testes periódicos dos *backup*s permitirão corrigir falhas antes que as perdas de dados aconteçam e também tornar melhor o tempo de recuperação.

5.2.8 Criptografia e Confidencialidade

Em situações onde a confidencialidade é importante, a ISO/IEC 17799 (ABNT, 2005, p.48) recomenda a criptografia do *backup*.

O CERT (2006) define a criptografia como a ciência e arte de escrever mensagens em forma cifrada ou em código.

A criptografia do *backup* deve ser uma das muitas atividades de um conjunto de estratégias para a segurança dos dados. O principal objetivo da criptografia é oferecer sigilo, integridade e autenticação para os dados armazenados e/ou transmitidos via rede, não permitindo exposição indevida dos dados.

5.3 Continuidade dos Negócios

É importante que as cópias de segurança de sistemas específicos sejam testadas periodicamente para garantir que elas estão aderentes aos requisitos definidos nos planos de continuidade do negócio, aconselha a NBR ISO/IEC 17799 (ABNT, 2005).

Conforme Erlich (2004) o PCN visa a assegurar a continuidade das atividades críticas de uma organização durante um desastre, procurando restabelecer a normalidade de todas as operações no menor espaço de tempo possível.

De acordo com Zhu et al. (2005) um Plano de Continuidade de Negócio (PCN) é uma combinação de *backup*, recuperação, disponibilidade alta, bem como um Plano de Recuperação de Desastres.

5.3.1 Recuperação de Desastres

“Para sistemas críticos, convém que os mecanismos de geração de cópias de segurança abranjam todos os sistemas de informação, aplicações e dados necessários para a completa recuperação do sistema em um evento de desastre.” ISO/IEC 17799 (ABNT, 2005, p.49)

Conforme Massiglia (2001), a informação, além de ser confiável, rápida, gerenciável e escalável, deve ser à prova de desastres. Os dados eletrônicos e as aplicações têm que estar disponíveis, mesmo com incêndio, inundação, ou qualquer tipo de falha.

5.4 Período de Retenção

A ISO/IEC 17799 (ABNT, 2005) indica que o período de retenção seja determinado para informações essenciais ao negócio e também qualquer requisito para que cópias de arquivo sejam permanentemente retidas.

Conforme Geronaitis (2005), com o aumento do volume de dados as organizações enfrentam alguns desafios como: o orçamento disponível para gerenciar os dados não cresce ao mesmo ritmo que o aumento do volume de dados, e há exigências cada vez mais rigorosas de retenção de dados por regulamentações do governo, bem como considerações de recuperação para continuidade de negócios.

É preciso estabelecer normas para que os dados fiquem retidos pelo período necessário, para evitar manter dos dados além do tempo pedido, sendo possível assim economizar espaço e outros recursos, e melhorar o tempo de recuperação.

5.5 Automação e Autoregulação

De acordo com a NBR ISO/IEC 17799 (ABNT, 2005), os mecanismos de cópias de segurança podem ser automatizados para facilitar os processos de geração e recuperação das cópias de segurança. É importante que tais soluções automatizadas sejam suficientemente testadas antes da implementação e verificadas em intervalos periódicos.

Segundo Cook (2006), os erros humanos são, provavelmente, os erros que mais se multiplicam e causam falhas de *backup* de dados, portanto além de conscientização para serem usadas as melhores práticas, é boa idéia tornar os *backup*s automáticos, sem muita intervenção humana. De acordo com Dorion (2005), monitorar de maneira pró-ativa os processos de *backup* é o melhor modo de assegurar e manter o *backup* e a sua recuperação.

A figura 1 mostra uma síntese da abordagem feita sobre o capítulo “10.5.1 Cópias de segurança das informações” da NBR ISO/IEC 17799.

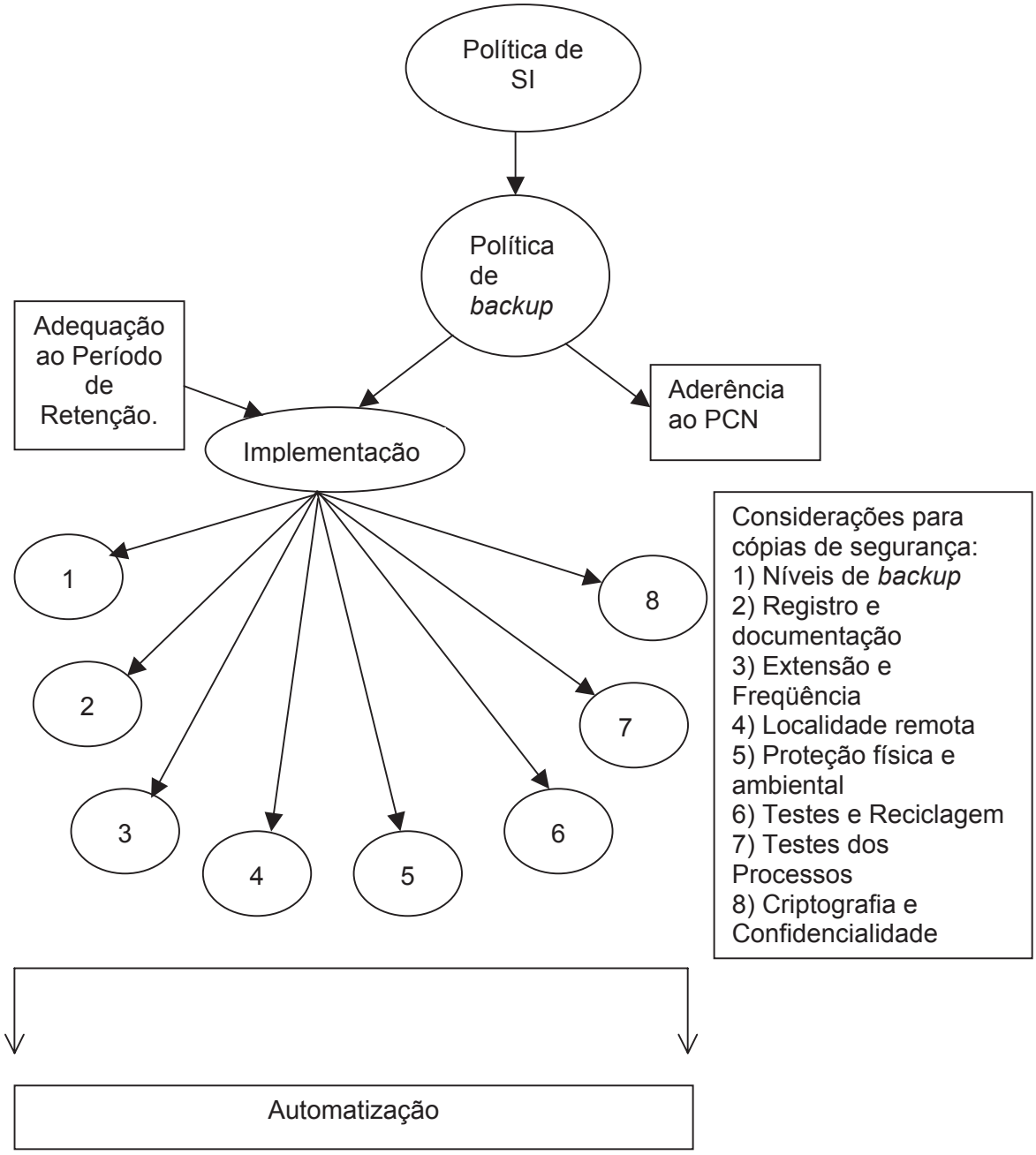

Figura 1: Política de SI e *backup* de dados

6. ANÁLISE DOS RESULTADOS DO QUESTIONÁRIO

Após analisar as normas da NBR ISO/IEC 17799 para políticas de SI e backup de dados, foi feita uma pesquisa de campo, através de questionário, sobre a utilização da NBR ISO/IEC 17799 pelos profissionais de SI.

O objetivo do questionário aplicado foi conseguir dos profissionais da área de SI, que já trabalham nesta área há mais de um ano, e que são responsáveis pela SI nas organizações onde trabalham, recomendações para procedimentos de *backup* de dados. Os resultados da pesquisa de campo, relacionados à aplicação da NBR ISO/IEC 17799, apresentados na figura 2, referem-se às respostas dadas à seguinte pergunta:

Quais as normas e/ou recomendações que contêm regras para *backup* de Dados, utilizados no seu ambiente de trabalho, para formulação de um Plano de *backup* de Dados?

( ) NBR ISO/IEC 17799

( ) Práticas de Segurança da Informação recomendadas pelo CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

( ) Recomendações e guias para Segurança do NIST (*National Institute of Standards and Technology*)

( ) Outros:

A opção “Outros”, deixada como alternativa, permitiu aos pesquisados a indicação de outras recomendações para o planejamento de *backup* de dados, ainda não apontadas na pesquisa. Conforme a figura 2, os respondentes acrescentaram que para *backup* de dados utilizam também normas estabelecidas pelas organizações onde trabalham, indicações da UNICAMP, outras fornecidas por meio de cursos de certificação para profissionais SI como, o *Certified Information Systems Security Professional* (CISSP), além das apontadas por livros na área de SI.

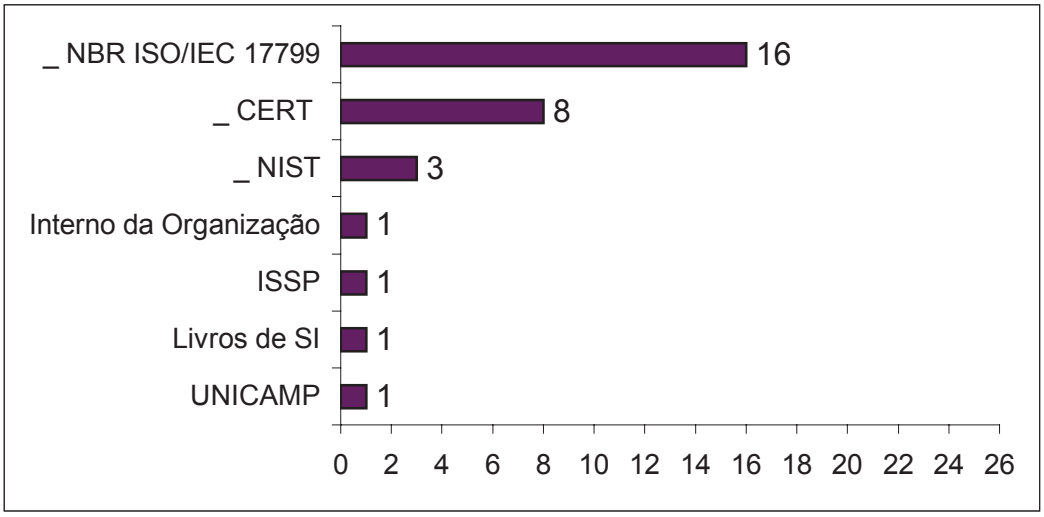

Figura 2: Normas e recomendações para plano de *backup* de dados.

De acordo com a figura 2, a maioria dos profissionais da área de SI, selecionados para esta pesquisa, utiliza recomendações, normas e outros tipos de indicações para planejarem o *backup* de dados, e 16 dos 26 respondentes utilizam a NBR ISO/IEC 17799, ou seja, apenas 61%. Este percentual é baixo, visto que a maioria dos respondentes trabalha há mais de 2 anos na área de SI e faz cursos de pós-graduação nesta área, portanto devem conhecer a NBR ISO/IEC 17799, mas não a incluem como recurso para o planejamento do processo de *backup* de dados.

7. DISCUSSÃO

De acordo com o estudo bibliográfico da NBR ISO/IEC 17799 e de outras referências sobre normas para *backup* de dados pôde-se compreender a importância de normas para os procedimentos de *backup* de dados de acordo com o conjunto de políticas de SI estabelecido pelas organizações. Porém o resultado do questionário não atingiu o índice esperado, que era que a grande maioria dos questionados, pelo menos 90%, utilizassem as NBR ISO/IEC 17799.

As principais recomendações, apontadas pelas NBR ISO/IEC 17799, sobre *backup* de dados, podem ser resumidas ao estabelecimento de um nível de proteção dos dados de acordo com o valor dos mesmos, ou seja, para os dados mais críticos deve-se investir mais, proteção física e lógica adequada tanto local quanto remota, testes dos procedimentos para verificar a sua eficácia, e documentação de todo o processo para facilitar a recuperação. Todo o processo deve considerar o período de retenção dos dados e a adequação ao PCN.

A abordagem das recomendações da NBR ISO/IEC 17799 permitiu verificar as exigências para os procedimentos de *backup* de dados, porém não são simples de serem implementadas. É preciso estabelecer responsabilidades e os responsáveis pelos *backup*s, fornecendo a estes recursos para que as devidas providências de segurança sejam tomadas, e auditorias para verificação dos procedimentos.

O ideal seria que todos utilizassem a NBR ISO/IEC 17799, além de apontarem outros documentos de referência para normas de *backup* de dados, porém muitos profissionais de SI ainda não aplicam a NBR ISO/IEC 17799. Isto sugere que a NBR ISO/IEC 17799 precisa ser mais bem estudada e conhecida pelos profissionais de SI. A conscientização de que a da NBR ISO/IEC 17799 pode ajudar na elaboração eficaz do conjunto de políticas de SI e *backup* de dados é a chave para melhorar este quadro, sendo que esta foi uma das contribuições do presente trabalho.

8. CONCLUSÃO E RECOMENDAÇÕES

A proteção dos dados visa à continuidade dos negócios em caso de perda das informações, assim como para atendimento a regulamentações governamentais e tantos outros casos que exijam a informação disponível. Por meio da abordagem da NBR ISO/IEC 17799 e outras referências foi possível facilitar o entendimento das recomendações para normas *backup* de dados e a inclusão das mesmas em políticas de SI.

A partir destas normas, os analistas de TI podem criar um conjunto de procedimentos-padrão para *backup* e recuperação de dados de acordo com as necessidades e critérios dos negócios de sua organização.

Além da aplicação das recomendações aqui discutidas é preciso pensar estrategicamente no fornecimento dos recursos para *backup* e recuperação dos dados, que deve ser de acordo com a disponibilidade exigida e com o valor das informações para os negócios da organização.

Na pesquisa de campo com profissionais de SI constatou-se que mais investigações devem ser elaboradas a fim de levar aos profissionais de SI melhores esclarecimentos sobre a contribuição da NBR ISO/IEC 17799 para normas de *backup* de dados. Este trabalho serve como início para outras pesquisas, pois há muito para ser explorado sobre normas para *backup* de dados. Cada recomendação para *backup* de dados da NBR ISO/IEC 17799 pode ser explicada em artigos separados, pois merecem muita atenção. Outra sugestão é de artigos específicos para a aplicação da NBR ISO/IEC 17799 para diferentes tipos de organizações.

REFERÊNCIAS

ABNT. **Tecnologia da informação – Código de prática para a gestão da Segurança da Informação (NBR ISO/IEC 17799).** Rio de Janeiro: 2005.

BIGELOW, S. J. ***Backup* Strategies**. 2006. Disponível em: http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1179087,00.html. Acesso em: 01 jun. 2006, 20:23:30.

CERT. **Práticas de Segurança para Administradores de Redes Internet**, 2003. Disponível em http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html. Acesso em 21 ago. 2005, 23:05:40.

CERT. **Cartilha de Segurança para Internet 3.1**, 2006. Disponível em http://cartilha.cert.br/conceitos/sec8.html#sec8. Acesso em 27 jan. 2007, 02:35:40.

COOK, R. ***Backup* failure: Five reasons *backup*s fail and tips for prevention**. 2006. Disponível em: http://searchstorage.techtarget.com/tip/0,289483,sid5_gci1204974,00.html. Acesso em 11 jan. 2007, 18:55:25.

DORION, P. **Best practices: Optimizing your *Backup*s**. 2006. Disponível em: http://searchstorage.techtarget.com/tip/1,289483,sid5_gci1154114,00.html?track=NL-53&ad=540066USCA. Acesso em 05 set. 2006, 16:35:35.

ERLICH, L. **Plano de Continuidade de Negócios: uma pesquisa exploratória na perspectiva estratégica no âmbito da Segurança da Informação.** 2004. 100f. Dissertação (Mestrado em Administração) - Curso de Pós-graduação em Administração de Empresas, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro. Disponível em: http://bdtd.ibict.br/bdtd/. Acesso em: 21 jun. 2005, 23:20:30.

FARIAS JUNIOR, A. **Nova norma garante Segurança da Informação**. 2002 Disponível em http://www.serasa.com.br/serasalegal/05-fev-02_m2.htm. Acesso em 26 ago. 2005, 17:00:00.

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, 00:35:40.

GERONAITIS, J. **ILM - Controlling the data mountain**. 2005. Disponível em: http://itnow.oxfordjournals.org/cgi/reprint/47/5/6. Acesso em 24 jan 2007, 22:30:40.

GONÇALVES, J.C. **O Gerenciamento da Informação e sua Segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico**. 2002. 339f. Dissertação (Mestrado em Administração de Empresas) – Faculdade

de Economia, Contabilidade e Administração, Universidade de Taubaté, Taubaté. Disponível em: http://www.unitau.br/prppg/cursos/ppga/mestrado/2002/goncalves_julio_cesar.pdf. Acesso em: 21 jun. 2005, 23:20:30.

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, 01:55:50.

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, 22:37:00.