UNIVERSIDADE DE TAUBATÉ
Eliana Márcia Moraes

PLANEJAMENTO DE *BACKUP* DE DADOS

Taubaté – SP

2007

UNIVERSIDADE DE TAUBATÉ
Eliana Márcia Moraes

PLANEJAMENTO DE *BACKUP* DE DADOS

Dissertação apresentada para obtenção do Título de Mestre pelo curso de Mestrado em Gestão e Desenvolvimento Regional do Departamento de Economia, Contabilidade e Administração, da Universidade de Taubaté,

Área de Concentração: Gestão de Recursos Sócio-produtivos

Orientador:
Prof. Dr. Marcio Lourival Xavier dos Santos

Taubaté – SP

2007

M827p Moraes, Eliana Márcia
Planejamento de *backup* de dados / Eliana Márcia Moraes - 2007.
124f. : il.

Dissertação (mestrado) - Universidade de Taubaté, Pró-reitoria de Pesquisa e Pós-graduação, 2007.
Orientação: Prof. Dr. Marcio Lourival Xavier dos Santos, Departamento de Informática.

1. Segurança da informação. 2. Estratégias de *backup* de dados. 3. Política de segurança. 4. Plano de continuidade de negócios. I. Título.

ELIANA MÁRCIA MORAES

PLANEJAMENTO DE *BACKUP* DE DADOS

Dissertação apresentada para obtenção do título de Mestre pelo curso de Mestrado em Gestão e Desenvolvimento Regional do Departamento de Economia, Contabilidade e Administração da Universidade de Taubaté.
Área de Concentração: Gestão de Recursos Sócio-produtivos

Data: 25 / 07 / 2007

Resultado: _____

BANCA EXAMINADORA

Professor Dr. Marcio Lourival Xavier dos Santos — Universidade de Taubaté

Assinatura: _____

Professor Dra. Isabel Cristina dos Santos — Universidade de Taubaté

Assinatura: _____

Professor Dr. Luiz Alberto Vieira Dias — Instituto Tecnológico de Aeronáutica

Assinatura: _____

Aos profissionais da Área de Segurança da Informação. E a todos os que acreditam e investem em pesquisas no Brasil.

AGRADECIMENTOS

A **Deus** pela **minha família** e por tudo o que me anima nesta caminhada.

À **Universidade de Taubaté – UNITAU**, principalmente à **Pró Reitoria de Pesquisa e Pós Graduação** pela oportunidade e pela **bolsa de estudos**, a mim concedida.

Especialmente ao meu **orientador, Professor Dr. Marcio Lourival Xavier dos Santos**, pela confiança em mim, dedicação, contribuição e incentivo para meu desenvolvimento no Mestrado.

Ao **Professor Dr. José Alberto Fernandes Ferreira** pelo apoio e ensinamentos.

À **Professora Dra. Isabel Cristina dos Santos** e ao **Professor Dr. Luiz Alberto Vieira Dias** pelas observações e correções construtivas.

Ao **Professor Dr. Edson Aparecida de Araújo Querido de Oliveira** pela excelente qualidade deste curso de mestrado.

À **Professora Dra. Maria Júlia Xavier Ribeiro** e à **Professora Dra. Hilda Maria Salomé Pereira** pela atenção e pelas recomendações.

Ao **professor Dr. José Glênio Medeiros de Barros** pelo apoio e compreensão.

Aos **Professores Dr. Marco Antonio Chamon, Dr. Marcio da Silveira Luz, Dr. José Luís Gomes da Silva, Dr. Francisco Cristóvão Lourenço de Melo** e **Dr. Antônio Pascoal Del'Arco Júnior** pelas indicações nas bancas de seminários.

Ao **Professor Álvaro Augusto Neto**, do ITA, Instituto Stefanini e IBTA, por indicar grande parte da amostra de respondentes desta dissertação.

A todos os **professores e funcionários da UNITAU** por tudo o que me foi proporcionado, sobretudo à **secretária Alda Aparecida dos Santos**.

Aos **colegas de trabalho e de estudo** pelas palavras de conforto, críticas e sugestões.

Aos **respondentes** do questionário pela disponibilidade e por compartilharem seus conhecimentos.

A **todos** que colaboraram direta ou indiretamente para a conclusão desta dissertação.

"Há os que se queixam do vento. Os que esperam que ele mude. E os que procuram ajustar as velas." -- William George Ward

RESUMO

Esta dissertação propõe etapas a serem seguidas para o planejamento eficaz de *backup* de dados, do ponto de vista de gestão de Segurança da Informação. Para atingir o objetivo proposto, foram pesquisadas as variáveis envolvidas para o planejamento de *backup* de dados, através de documentos de fontes seguras encontradas na Internet, em livros, em artigos e em outras referências, sobre as estratégias de *backup* de dados, reunindo as de maior relevância e incidência. No decorrer da pesquisa foi aplicado um questionário a alguns profissionais da área de Segurança da Informação para saber o que estes recomendam e se utilizam as respectivas estratégias de *backup* de dados. Para a análise dos dados coletados foram usados métodos qualitativos e quantitativos. Com avaliação das respostas ao questionário constatou-se que nem todas as estratégias indicadas pela literatura são aplicadas pelos profissionais de Segurança da Informação. As opiniões dos respondentes divergem em alguns pontos, o que pode ser explicado pela falta de guias e cursos específicos para o planejamento de *backup* de dados. No decorrer da dissertação, foi mostrada a importância da Segurança da Informação e finalmente, foram propostas as fases a serem respeitadas em um planejamento de *backup* de dados.

Palavras-Chave: Segurança da Informação. Estratégias de *Backup* de Dados. Política de Segurança. Plano de Continuidade de Negócios.

ABSTRACT

This work presents some results from a research carried out with the main objective of proposing Data Backup Strategies. The results have been collected based upon both the known practices found in the literature, publicized articles and comments in the "world wide web" and on the actual practices which have been in use by a technical staff in Information Security. To this objective, documents describing the "best" and the "most used practices" in Data Backup Management were collected in the Internet and also from technical references published on the subject. In order to access the most common practices, a written survey was devised and sent to a selected professional staff working in Information Security, which had been asked to answer a questionnaire regarding their recommended Data Backup planning strategies. From the answers given to the questionnaire; it can be detected that not all the prescribed practices are being used by the respondents. In fact, it is noticeable that their opinions diverge. This dissertation demonstrates the importance of keeping the integrity of the Information and the best practices to ensure its protection, availability and recovery. Finally, a Data Backup Strategy is presented.

Keywords: Information Security. Data Backup Strategies. Security Policy. Business Continuity Plan.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Nas diversas atividades da sociedade, sejam pertencentes aos setores de produção, de serviços, ou de governo, as informações armazenadas nos computadores têm um valor incalculável. Dependendo do objetivo organizacional, a falta dessas informações pode significar dificuldades administrativas e até a paralisação de atividades essenciais. Em caso de perda de dados, é quase sempre imprescindível poder recuperá-los e isto se torna possível se existir uma fonte segura de *backup*.

Backup é um termo em inglês que quase sempre é traduzido como cópia de segurança, porém o *backup* nem sempre é seguro. São necessárias estratégias para manter a integridade, confiabilidade e disponibilidade do *backup*.

Um dos exemplos de que o *backup* de dados nem sempre pode ser recuperável foi a perda de informações, relatadas depois do atentado às torres gêmeas nos Estados Unidos da América, em onze de setembro de dois mil e um, quando algumas organizações, mesmo tendo *backup*, não conseguiram recuperar seus dados devido à localização dos mesmos. Essas organizações tinham seus dados principais em uma torre e o *backup* dos dados na torre gêmea ao lado, e o desastre atingiu as duas torres. Esse foi um problema de mau planejamento e gerenciamento do *backup*.

O atentado de onze de setembro aumentou as preocupações com a segurança do *backup*, entre elas: a localidade do *backup* remoto a certa distância dos dados originais, para que um desastre no local onde estão os dados principais não atinja o *backup* remoto, a segurança do transporte e do

armazenamento dos dados, e de outros fatores que precisam ser considerados.

Além de manter o *backup* para ser recuperado em casos de perda de dados, as organizações obedecem a regulamentos governamentais, que obrigam a guarda de informações. Por exemplo, independente do porte ou negócios, as organizações que possuem funcionários contratados precisam manter os dados empregatícios por longo tempo determinado por lei. E a necessidade de manter a massa de dados por tanto tempo transforma o *backup* em operação crítica.

Este trabalho surgiu a partir de preocupações em guardar de maneira segura os dados de uma Universidade. Depois de informatizar alguns serviços e processos e com a utilização de bancos de dados para sistemas administrativos, internet, ensino à distância e outros, a Instituição passou a ser mais dependente dos dados eletrônicos, e com o volume desses dados aumentando há a dificuldade de guardá-los de modo seguro.

Para garantir o presente e assegurar o futuro dos dados dessa Universidade, procurou-se resolver o problema da guarda dos dados eletrônicos, porém ao tratar desse assunto verificou-se o nível de complexidade do tema *backup*, desde a parte de planejamento até a prática em si. Como esta foi a primeira pesquisa na Universidade sobre *backup* optou-se por analisar sobre o planejamento do *backup*, ou seja, quais as estratégias para *backup* de dados.

Foi realizado um estudo onde foram levantadas as principais variáveis para o planejamento de *backup* de dados. Para isso foi feita uma revisão na literatura sobre Segurança da Informação com enfoque em *backup* de dados.

Devido ao fato de encontrar pouca literatura nacional sobre *backup*, até onde foi possível examinar no conjunto de documentos citados na bibliografia, procurou-se saber o que estava sendo utilizado como estratégias de *backup* de dados no Brasil. Para isto foi selecionado um grupo de profissionais, responsáveis pela Segurança da Informação nas organizações onde trabalham, para responderem a um questionário.

Com o desenvolvimento desta pesquisa verificou-se que as estratégias de *backup* de dados estudadas podem beneficiar outras organizações, e por isso, optou-se por não se fazer um estudo de caso, porém cada organização possui necessidades distintas e apresentará abordagens diversas para tratar as questões relacionadas a *backup* de dados. Entretanto, um conjunto genérico de estratégias, com requisitos básicos, pode ser definido para guiar o planejamento de *backup* de dados para diferentes naturezas de negócios.

Este trabalho se desenvolve sob o ponto de vista de gestão de Segurança da Informação, pois apresenta um conjunto de estratégias a ser destinado principalmente, aos supervisores responsáveis pela área de Segurança da Informação, com o objetivo de se planejar o *backup*, além de mostrar aos administradores, responsáveis pelo orçamento das organizações, as necessidades de se investir em *backup* de dados.

O *backup* de dados precisa de estratégias para ser seguro e recuperável. Assim, busca-se neste estudo, propor etapas para o planejamento de *backup* de dados, de acordo com a literatura pesquisada e respostas a um questionário aplicado a profissionais da área de Segurança da Informação, para a preservação da segurança e continuidade dos negócios.

1.1 O PROBLEMA DE PESQUISA

O Problema da presente pesquisa é:

Identificar, através da literatura e profissionais da área de Segurança da Informação, as principais variáveis e estratégias para o planejamento de *backup* de dados, do ponto de vista de gestão de Segurança da Informação.

1.1.1 Objetivo Geral

- O objetivo geral é propor etapas para o planejamento eficaz de *backup* de dados.

1.1.2 Objetivos Específicos

- Pesquisar estratégias de *backup* de dados através da literatura e das respostas dadas a um questionário por profissionais responsáveis pela área de Segurança da Informação.
- Reunir as estratégias de relevância e de maior incidência para *backup* de dados.
- Demonstrar a importância da participação da área administrativa no planejamento de *backup* de dados.
- Propor estratégias de *backup* de dados do ponto de vista de gestão de Segurança da Informação.

1.2 DELIMITAÇÃO DO ESTUDO

Serão abordadas as estratégias de maior relevância e incidência para *backup* de dados.

O levantamento das estratégias será feito através de pesquisa na literatura constituída de artigos especializados em Segurança da Informação, *backup* e recuperação de dados, e através de questionário.

O questionário sobre estratégias de *backup* de dados foi aplicado a profissionais responsáveis pela Segurança da Informação que trabalham há um ano ou mais em organizações que possuem dados críticos e que precisam ser mantidos por um período mínimo de dois anos. As respostas foram fornecidas por profissionais de organizações do Estado de São Paulo: Capital, Vale do Paraíba e Campinas.

Em relação aos portes, tamanhos ou qualquer informação sobre as empresas às quais pertencem funcionalmente os respondentes, ficou acordado com todos que seria mantida a confidencialidade, evitando-se, portanto, uma identificação, mesmo que indireta.

As etapas propostas para o planejamento seguro de *backup* de dados visam à gestão de Segurança da Informação.

1.3 RELEVÂNCIA DO ESTUDO

A Segurança da Informação é necessária para a gestão administrativa, independente do tipo de negócios, seja da informação, comércio, educação, produção e negócios em geral. Dependendo da criticidade da informação surgem as justificativas de quanto investir em *backup* de dados.

Os investimentos de uma organização com Segurança da Informação, normalmente representam um seguro contra perdas. Antes que casos isolados ocorram, como, por exemplo, a invasão de um sistema por um vírus ou até um incêndio em um centro de processamento de dados, o investimento em segurança pode eliminar ou diminuir os prejuízos devido à perda de informações.

Para que não haja conflitos quanto aos requisitos de orçamento para *backup* de dados, é preciso o entendimento de que não é só o pessoal da área de Tecnologia de Informação que deve ser responsável pela Segurança da Informação, mas a organização como um todo.

Para investir em *backup* de dados, entretanto, é necessário saber quais estratégias utilizar, de acordo com a criticidade da informação. Com base nesta afirmação, este trabalho propõe estratégias de *backup* de dados, mostrando que, tanto a área administrativa, quanto à área de Tecnologia da Informação devem participar deste planejamento.

A importância deste estudo também consiste no potencial de discussão e geração de trabalhos acadêmicos relacionados a *backup* de dados, do ponto de vista de gestão da Segurança da Informação. Até onde foi possível investigar, os trabalhos acadêmicos voltados para *backup* de dados são específicos sobre algoritmos ou programas de *software* para *backup* de dados.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho distribui-se em cinco capítulos onde o primeiro é esta introdução.

No Capítulo 2, Revisão da Literatura, são apresentados os conceitos básicos e considerações teóricas sobre a importância da Segurança da Informação, Política de Segurança da Informação e Plano de Continuidade de Negócios, como base para o assunto principal da presente pesquisa: Estratégias de *backup* de dados.

No Capítulo 3, reservado à Metodologia, é definido o tipo de pesquisa, são mostrados os critérios de composição da amostra, as formas de coleta de dados e os procedimentos da análise e do tratamento dos dados.

No Capítulo 4, que aborda Resultados e Discussão e Proposta, e no Capítulo 5, Conclusão, são apresentadas e comentadas as análises dos dados coletados, e o que é esperado deste estudo: as estratégias de *backup* de dados.

Ao final, encontram-se as Referências Bibliográficas e Anexos.

2 REVISÃO DA LITERATURA

A revisão da literatura está dividida em quatro seções. A primeira define e mostra a importância da Segurança da Informação, a segunda e a terceira partes, respectivamente, explicam sobre Política de Segurança da Informação e Plano de Continuidade de Negócios. As três primeiras partes introduzem e fornecem informações para a compreensão do contexto, formulando as origens das preocupações com *backup* de dados. Finalmente na quarta seção são apresentadas as estratégias de *backup* de dados, principal assunto desta pesquisa.

2.1 SEGURANÇA DA INFORMAÇÃO

"A Segurança da Informação pode ser usada como um diferencial na estratégia, especialmente em uma economia globalizada em que mais negócios são conduzidos eletronicamente." (EGAN, 2005, p.11).

Para auxiliar na implementação de Segurança da Informação, foi publicada pela Associação Brasileira de Normas Técnicas (ABNT) a NBR ISO/IEC 17799, com padrões de metodologia de segurança. A NBR ISO/IEC 17799 é equivalente à norma ISO 17799, que teve como origem a BS 7799, criada pelo *British Standards Institute* (BSI), que é um conjunto de padrões britânicos, criado em 1995 e foi o primeiro documento a ser reconhecido internacionalmente como guia de práticas de Segurança da Informação.

A norma NBR ISO/IEC 17799 (ABNT, 2005), especifica que a Segurança da Informação 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.
d) Outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

A informação é um ativo importante, normalmente o bem mais valioso para a maioria das organizações, e por isso deve ser protegido. De acordo com Erlich (2004), a Segurança da Informação deve servir de seguro contra as ameaças.

O episódio ocorrido em onze de setembro de 2001 no *World Trade Center*, em Nova Iorque é um dos exemplos que mostra o quanto é importante para as organizações preservarem a Segurança da Informação.

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, depois do atentado terrorista, no dia seguinte, já operava os seus sistemas quase normalmente.

Segundo 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.

Ao contratar um site de *backup* remoto, ou aperfeiçoar as formas de acesso às fontes de informação utilizando controles automatizados como, sistemas de reconhecimento de retina, voz, digitais, pessoal qualificado, etc. ampliam-se os custos com a Segurança da Informação. No entanto, diante de situação de alto risco, como catástrofes naturais ou provocadas é que se pode avaliar a importância de um investimento maior. Existem duas formas de desastres que, por suas conseqüências, podem ilustrar essa consideração: quando em um desastre os dados são perdidos sem o devido *backup*, ou quando apesar das perdas os dados são recuperados.

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

A Segurança da Informação é fundamental, e para que ela seja estabelecida nas organizações, é preciso a elaboração de uma política de segurança e de um Plano de Continuidade de Negócios. Para isto é preciso antes classificar a informação e determinar os riscos de perdas através do conhecimento das particularidades de cada negócio.

2.1.1 Classificação da Informação

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

Para a norma NBR ISO/IEC 17799 (ABNT, 2005), o objetivo da classificação da informação é indicar as necessidades e prioridades da informação e garantir que seja dado o nível adequado de proteção à informação.

Prado (2002) alerta que não adianta investir na proteção de um servidor de rede que não armazena nenhuma informação crítica aos negócios, e que os esforços devem ser concentrados no que realmente é significativo para a organização.

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

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), a informação possui vários níveis de sensibilidade e criticidade. Alguns dados podem necessitar um nível adicional de proteção ou tratamento especial. É importante que um sistema de classificação da informação seja utilizado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

Para a classificação da informação, a norma NBR ISO/IEC 17799 (ABNT, 2005) recomenda considerar o valor para os negócios, requisitos legais, sensibilidade e criticidade para a organização. E ao implementar a classificação convém levar em consideração as necessidades de compartilhamento ou restrição de informações e os respectivos impactos nos negócios, incluindo convenções para classificação inicial e reclassificação ao longo do tempo, de acordo com algumas políticas de controle e de acesso predeterminadas.

Os processos de reclassificação ao longo do tempo são designados por processos de *backup* hierárquico que retratam a condição de que a informação freqüentemente deixa de ser sensível ou crítica após certo período de tempo.

A norma NBR ISO/IEC 17799 (ABNT, 2005) adverte que esquemas de classificação de informação excessivamente complexos podem ser inviáveis economicamente ou impraticáveis.

Este assunto será complementado quando definidas as estratégias de *backup* de dados e o conceito de Gerenciamento do Ciclo de Vida da Informação for explicado.

A informação deve ser classificada de acordo com a sua importância e criticidade através de análise de riscos, para se determinar a necessidade e um possível prejuízo com a falta da informação para os negócios da organização.

2.1.2 Análise de Riscos, Vulnerabilidades, Ameaças e Falhas.

A norma NBR ISO/IEC 17799 (ABNT, 2005) define que a avaliação de riscos é uma consideração sistemática do impacto aos negócios resultantes de uma falha de segurança. Deve-se levar em conta as conseqüências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos e da probabilidade de tal falha ser explorada por ameaças e vulnerabilidades mais freqüentes.

De acordo com Egan (2005), vulnerabilidades são brechas ou fraquezas dos sistemas, que exploradas, podem comprometer os mesmos.

Estar vulnerável é encontrar-se exposto a possíveis ataques de uma ameaça. Por exemplo, estar com o antivírus desatualizado é uma vulnerabilidade.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2003) conceitua ameaça à segurança como a quebra de uma ou mais das três propriedades fundamentais confidencialidade, integridade e disponibilidade da informação.

Segundo Erlich (2004), as ameaças da área de Segurança da Informação podem se originar de alguns tipos de situações, tais como:

a) Catástrofes: incêndio, alagamento, vazamento, explosão, desabamento, relâmpago.
b) Problemas ambientais: variações térmicas, umidade, poeira, radiação, ruído, vapores, gases, fumaça, magnetismo, trepidação, falta de energia elétrica.
c) Comportamento anti-social: paralisação, greve, piquete, invasão, alcoolismo, drogas, sabotagem, omissão, inveja, rixa entre funcionários, ação criminosa, furtos, fraudes, terrorismo, seqüestro, espionagem industrial.
d) Problemas Eletrônicos: pane de equipamentos ou de redes, falhas nos sistemas operacionais, paradas de sistema.
e) Procedimentos inadequados: supressão de serviços, erros de usuários, erros de *backup*, utilização inadequada de sistemas ou arquivos, dados incompletos ou inconsistentes, violação de confidencialidade, treinamento insuficiente, ausência e demissão de funcionários, sobrecarga de trabalho.

Ambientes vulneráveis diante de ameaças podem sofrer perdas quando as ameaças se concretizam, ou então têm a oportunidade de reavaliar seu plano de segurança em conseqüência da insegurança iminente.

Conforme Zhu et al (2005), as faltas ou paradas de sistemas podem ser classificadas em duas categorias: planejadas e as não planejadas.

a) As paradas planejadas podem ocorrer na execução do *backup*, atualizações, manutenção, e outros eventos programados, que podem deixar o usuário *off-line*, ou sem acesso ao sistema.
b) As paradas não planejadas ocorrem devido aos eventos imprevisíveis, tais como queda de energia, falha de *hardware* ou *software*, erros humanos, rupturas da segurança, ou desastres naturais.

Em conseqüência das paradas planejadas ou não planejadas, pode ocorrer uma falta de disponibilidade ou *downtime* do sistema. Para que isso não ocorra, deve-se concentrar esforços para minimizar as faltas de disponibilidade como, por exemplo, projetar sistemas fáceis de usar, que sejam bem documentados e que reduzam fatores de riscos, afirma Zhu et al (2005).

O *backup* é uma das estratégias principais para a proteção dos dados, mas, segundo Cook (2006a), de acordo com algumas estimativas, mais que metade dos sistemas de *backup* e recuperação falha, e as razões das falhas são as mesmas.

Cook (2006a) escreveu uma lista de problemas comuns de falhas, entre eles são destacados alguns, decrescendo em ordem de freqüência:

a) Falhas de mídias são as falhas mais comuns, tratando-se de *backup* e recuperação de dados. Portanto, é importante tratar as mídias com cuidados, seguindo as instruções do fabricante, por exemplo, no caso de fitas, é importante saber como deve ser feita a manipulação, o armazenamento, a reciclagem e a limpeza de drives. Em caso de

backup de dados em disco, um dos cuidados a serem tomados é a instalação de fontes redundantes nos equipamentos.

b) Erros humanos são, provavelmente, os erros que mais se multiplicam e causam falhas de *backup* de dados. Por exemplo, se as mídias estão guardadas de maneira imprópria, resultando em falhas, é um erro humano e não falha de mídias.

   A melhor prevenção contra erros humanos em *backup* é o treinamento, que deve envolver as melhores práticas e a certeza do entendimento das pessoas sobre o que elas devem ou não fazer em relação ao *backup*. È importante tornar os sistemas de *backup* automáticos, sem muita intervenção humana.

c) Falhas de software, geralmente geradas devido a muitas opções contidas nos sistemas para *backup*, que podem conter erros de configuração, levando ao *backup* incompleto ou totalmente falho. As configurações não são estáticas, devido às mudanças em relação à quantidade e a lista de arquivos principais, às atualizações de versões, e às outras modificações.

d) Falhas de hardware, geralmente geradas devido a drives e bibliotecas de fitas, espelhamento de discos e outros tipos de hardware de *backup*, que podem também falhar. As causas podem ser relacionadas a *backup* ou não, por exemplo: versões de fitas não compatíveis com os drives, erros de alinhamento e de leitura de drives.

e) Falhas de rede, apesar do *backup* em rede diminuir o número de dispositivos de *backup* e melhorar a eficiência, uma falha na conexão pode impedir a conclusão do *backup* de maneira segura.

2.1.3 Impactos e Prevenções

Os Impactos podem ser tanto financeiros como morais. Cada risco traz impacto diferente para cada negócio.

De acordo com Zhu et al (2005), embora sejam desejáveis sistemas disponíveis, é necessário calcular o custo da disponibilidade e o custo da indisponibilidade. É crucial compreender o impacto aos negócios devido a perdas não planejadas.

As conseqüências da falta de disponibilidade variam de acordo com os diferentes tipos de negócios. Para serviços financeiros, pode haver uma perda de valores monetários e comprometimento nas transações de negócios para cada minuto de indisponibilidade que, para outro negócio, poderia significar meramente uma inconveniência aos usuários. Entre as possibilidades de perdas irrecuperáveis, pode-se citar a imagem da organização e a confiança do cliente.

Para se calcular o impacto que um determinado risco pode causar ao negócio, pode-se usar o *Business Impact Analysys*. De acordo com Prado (2002), esta técnica consiste na estimativa de prejuízos financeiros decorrentes da paralisação de um serviço. Com o *Business Impact Analysys*, torna-se possível responder questões do tipo: “quanto uma empresa deixaria de arrecadar caso um sistema estivesse indisponível durante duas horas?”.

Como prevenção, uma das melhores estratégias é ter o *backup* sempre disponível de acordo com a política de Segurança da Informação e com o Plano de Continuidade de Negócios.

2.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conforme Gonçalves (2002), a política de Segurança da Informação é um conjunto de diretrizes, regras e práticas que impõem como uma organização gerencia, protege e distribui suas informações e recursos.

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

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), no mínimo, convém que as seguintes orientações sejam incluídas na política de Segurança da Informação:

a) Definição de Segurança da Informação, resumo das metas, seu escopo e a sua importância, como um mecanismo que capacita o compartilhamento da informação;
b) Declaração do comprometimento da alta administração, apoiando as metas e princípios da Segurança da Informação;
c) Estrutura para estabelecer os objetivos de controles, incluindo a estrutura de análise, avaliação e gerenciamento de riscos;
d) 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 da continuidade dos negócios;

- Conseqüências das violações na política de Segurança da Informação;

e) Definição das responsabilidades gerais e específicas na gestão da Segurança da Informação, incluindo o registro dos incidentes de segurança;
f) Referências às documentações que possam apoiar a política.

Segundo a norma NBR ISO/IEC 17799 (ABNT, 2005), o documento da política de Segurança da Informação deve ser aprovado pela alta administração, publicado e comunicado, através de toda a organização para os usuários na forma que seja relevante, acessível e compreensível para o leitor em foco.

Conforme Gonçalves (2002), a criação de uma política de Segurança da Informação precisa de esforços entre o pessoal técnico e o pessoal responsável pelas decisões da organização. Para que a política seja bem sucedida após a implantação, é importante o comprometimento dos usuários, sistemáticas de auditorias internas periódicas e punições para os casos omissos ou de não cumprimento das diretrizes. Convém que rotinas de treinamento sejam adotadas, buscando a conscientização e participação dos usuários visando à utilização dos recursos computacionais para o desempenho funcional.

A adoção de uma norma, como a NBR ISO/IEC 17799, é a base para um conjunto de políticas de Segurança da Informação bem conduzido, e o desenvolvimento, estabelecimento e todas as ações sobre as políticas devem ser adequados para cada organização e os negócios aos quais se aplicam.

2.2.1 Política de Segurança da Informação e *backup* de dados

Segundo Swanson et al (2002), as políticas de *backup* devem especificar a freqüência do *backup*, 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, freqüência de trocas das mídias, e método para transportar os dados.

Segundo Gonçalves (2002), é importante fazer uma avaliação dos riscos envolvidos para decidir o que realmente precisa ser protegido e a quantidade de recursos que devem ser utilizados para a economia dos mesmos. A política de Segurança da Informação e outros controles têm a finalidade de procurar garantir que a segurança seja mantida e que os dados armazenados nos computadores sejam confiáveis e disponíveis.

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2005), é importante que as cópias de segurança, ou seja, o *backup*, das informações e das aplicações de *software* seja efetuado e testado regularmente conforme a política de geração de cópias definida.

As normas e recomendações de segurança para *backup* de dados pertencentes ao conjunto de política de Segurança da Informação devem ser baseadas em estratégias que visem preservar as informações importantes para os negócios da organização.

2.3 PLANO DE CONTINUIDADE DE NEGÓCIOS

Segundo Erlich (2004), o Plano de Continuidade de Negócios visa manter o funcionamento das atividades críticas das organizações durante

desastres, procurando restabelecer a normalidade de todas as operações no menor espaço de tempo possível.

Conforme Sêmola (2003), o Plano de Continuidade de Negócios deve ser desenvolvido com o claro objetivo de reparar incidentes de segurança que não puderam ser evitados.

A norma NBR ISO/IEC 17799 (ABNT, 2005) recomenda que os Planos de Continuidade de Negócios sejam desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados o mais rápido possível. E que estes planos sejam mantidos e testados de forma a se tornarem parte integrante de todos os outros processos gerenciais.

Existem várias denominações ou componentes do Plano de Continuidade de Negócios, entre eles se encontram: Plano de Contingência, Plano de Administração de Crises e Plano de Recuperação de Desastres.

Conforme Zhu et al (2005), a conformidade com leis e regulamentos é uma das razões principais para fazer um plano de Recuperação de Desastres. Nas últimas décadas, as exigências legais para a proteção dos dados e a recuperação envolvem a maioria de setores de negócios.

De acordo com Daft (2005), para desenvolver os planos de contingência, que definem respostas da empresa às emergências, contratempos ou condições inesperadas, os gerentes devem identificar os fatores incontroláveis. O Plano de Administração de Crises deve especificar as medidas a serem tomadas, e por quem, se ocorrer uma crise, ele deve incluir além de outros planos, procedimentos para *backup* e recuperação dos sistemas de computadores e proteção da propriedade da informação.

Os Planos de Recuperação de Desastres, conforme Zhu et al (2005), descrevem como a organização tratará dos desastres potenciais, e consiste em precauções, de modo que, os efeitos de um desastre sejam minimizados, e a organização mantenha ou recomece rapidamente as atividades essenciais aos negócios.

Conforme avalia 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.

De acordo com Swanson et al (2002), embora os grandes desastres, com efeitos de longo prazo, possam ser raros, eles devem ser explicados no plano de contingência. Assim, o plano deve incluir uma estratégia para recuperar e executar operações de sistema em uma instalação alternativa por um período prolongado.

Conforme Zhu et al (2005), o planejamento para a recuperação de desastre varia de uma organização a outra, dependendo de variáveis, tais como, o tipo de negócio, os processos envolvidos, e o nível da segurança necessário. Ao fazer um Plano de Continuidade de Negócios, necessita-se considerar o custo de executar uma solução, o projeto da solução, e outras considerações e fatores críticos de sucesso.

Gherman (2005), afirma que é indispensável determinar objetivos para a Tecnologia da Informação, não só para atender aos requisitos próprios dos negócios, mas também aos da segurança das informações processadas, armazenadas e transmitidas, e perseguir esses objetivos.

2.3.1 Plano de Continuidade de Negócios e *backup* de dados

"Um Plano de Continuidade de Negócios é uma combinação de *backup*, recuperação, disponibilidade alta, bem como um Plano de Recuperação de Desastres" (ZHU et al 2005, p.22).

Há benefícios adicionais com a implementação de soluções de recuperação de desastres, pois é necessário repensar o processo operacional, o dispositivo de armazenamento e onde os dados estão armazenados, aponta Zhu et al (2005). Empregar processos mais dinâmicos, incluindo dispositivos de armazenamento mais confiáveis, também melhorará a eficiência e reduzir-se-ão as falhas de armazenamento.

É possível simplificar a gerência de armazenamento usando uma estratégia global, aplicação holística, propondo exigências comuns de *backup* e recuperação. Todas as aplicações e sistemas devem entrar em conformidade com as mesmas exigências e regras de recuperação de desastre baseados em diferentes tipos de dados, propõe Zhu et al (2005).

As melhores práticas de *backup* que permitirão a recuperação eficiente dos dados para a continuidade dos negócios devem ser baseadas em estratégias de acordo com as particularidades de cada organização.

2.4 ESTRATÉGIAS DE *BACKUP* DE DADOS

Para a política de Segurança da Informação e para o Plano de Continuidade de Negócios são necessárias estratégias de *backup*, que serão apresentadas nesta seção. Inicialmente, coloca-se a seguinte questão:

Quanto complexa ou detalhada a estratégia de *backup* deve ser?

Bigelow (2006) diz que não há uma resposta única a esta pergunta. O plano certo depende do que cada organização necessita. Um ambiente pequeno pode somente necessitar de *backup* de dados em fita convencional, uma vez por semana. Outras organizações podem requerer armazenamento baseado em disco para suportar dados críticos. As grandes empresas podem exigir uma plataforma contínua da proteção dos dados.

O *backup* precisa de um plano claro, que esteja de acordo com os objetivos específicos de cada negócio. Para isso é necessário 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).

Para a estratégia de *backup* de dados, deve-se compreender porque o motivo do *backup*, o que é necessário para o plano de *backup*, saber onde o *backup* deve estar, como recupera-lo e então combinar as ferramentas para servir estas necessidades.

Antes de continuar a explicação sobre estratégias de *backup* de dados, é necessário definir e esclarecer alguns termos da área de Segurança da Informação e de *backup* de dados.

2.4.1 Termos utilizados para o planejamento de *backup* de dados

Para melhor compreensão dos termos utilizados na literatura técnica sobre *backup* de dados, foram relacionados abaixo o jargão comum da área e seu significado especial ou específico. São eles:

Janela de *backup* - É o período de tempo em que o *backup* é executado.

Recovery Point Objective (RPO) – é a quantidade de dados perdida, em unidade de tempo, aceitável para ser refeita após um desastre. Por exemplo, uma organização que poderia perder dados durante cinco minutos, tem um *Recovery Point Objective* de cinco minutos, explica Zhu et al (2005).

Recovery Time Objective (RTO) – é quanto tempo a organização pode esperar pela recuperação de seus sistemas depois de um desastre. Por exemplo, uma organização que poderia permitir ficar sem os sistemas por oito horas tem um *Recovery Time Objective* de oito horas, exemplifica Zhu et al (2005).

Disponibilidade - Zhu et al (2005) define disponibilidade como o período em que usuários e processos estão funcionando normalmente. A disponibilidade requer que o sistema forneça redundância para eliminar pontos críticos de falha ou *Single Point Of Failure* (SPOF).

Alta disponibilidade - O conceito da alta disponibilidade, conforme Zhu et al (2005), é ter os sistemas e seus dados disponíveis vinte e quatro horas por dia, sete dias por semana, e trezentos e sessenta e cinco dias por ano.

Sabe-se que obter uma disponibilidade próxima a cem por cento não é uma realidade para todas as organizações devido ao custo. O objetivo é projetar e construir sistemas altamente disponíveis minimizando as faltas ou perdas, planejadas ou não, que podem ser causadas por pontos críticos de falha. Para se ter a alta disponibilidade é necessária a redundância de recursos para tornar o *backup* de dados de fácil e rápida recuperação.

Disponibilidade continua - A alta disponibilidade é um componente da disponibilidade contínua. A alta disponibilidade focaliza em reduzir a falta de disponibilidade em paradas de sistemas não planejadas. As operações

contínuas focalizam ajustar as aplicações para “nunca parar”. A soma da alta disponibilidade e de operações contínuas leva à disponibilidade contínua, ver Zhu et al (2005).

2.4.2 Tipos de *Backup* de dados

Há dois tipos de *backup* de dados: *backup on-line* e *backup off-line*. Ambos podem ser também dos tipos: completo ou incremental. Conforme Zhu et al (2005):

a) O *backup* off-line é feito quando o sistema não está em operação. Os usuários não podem conectar a uma aplicação ou à base de dados e nesse período não haverá nenhuma atividade no sistema, exceto o processo de *backup*.
b) O *backup* on-line permite a execução do *backup*, mesmo com o sistema em operação. Neste período os usuários podem utilizar a aplicação e/ou a base de dados e executar ações normais, tais como a atualização e a recuperação dos dados com o sistema funcionando normalmente.
c) O *backup* completo é o *backup* de todas as bases de dados e também de todos os arquivos envolvidos na aplicação.
d) O *backup* incremental é o *backup* dos dados que foram modificados. Esse *backup* somente conterá os dados modificados desde o último *backup* completo ou desde o último *backup* incremental.

O *backup* também pode ser local ou remoto. O *backup* local é feito no mesmo lugar em que se encontram os dados originais, e o *backup* remoto é a cópia segura dos dados em local distante dos dados principais.

Segundo Garfinkel (2004), o *backup* é 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 *Hard Disk* (HD) formatado. O *backup* semanal é vital para recuperar arquivos importantes que não são utilizados sempre, como arquivos de configuração e inicialização de sistemas. O *backup* trimestral e anual pode ser realmente útil em disputas de patente, em outros tipos de litígio e na manutenção de históricos em geral, tais como componentes anuais de históricos escolares.

Os sistemas de *backup* tradicionais copiam simplesmente dados para mídia de armazenamento sem a preocupação sobre que dados são copiados ou sobre a importância dos dados para a organização. As estratégias envolvem um pouco mais do que apenas trabalhos de *backup* programados e manter a substituição de mídias. O *backup* exige planejamento melhor e bem detalhado.

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

Antes de se fazer o *backup,* é necessário fazer a classificação da informação, com atributos, como permissões de acesso, data, tempo de retenção, local de armazenamento, etc. Assim recursos de armazenamento podem ser utilizados de maneira efetiva, ou seja, os recursos mais caros de *backup* e armazenamento são destinados às informações mais valiosas. Para o gerenciamento de informações e armazenamento existem também as estratégias de Gerenciamento do Ciclo de Vida das Informações, sendo este último conceito definido no parágrafo seguinte.

2.4.3 Gerenciamento do ciclo de vida das informações

As estratégias de Gerenciamento do Ciclo de Vida das Informações ou *Information Lifecycle Management* (ILM) são projetadas para melhorar a gerência de criação, o arquivamento e/ou a remoção da informação.

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.

Segundo Geronaitis (2005), os analistas, que desenvolvem estratégias de Gerenciamento do Ciclo de Vida das Informações, devem considerar dois fatores:

a) O Gerenciamento do Ciclo de Vida das Informações redefine a gerência de armazenamento de dados. A gerência de armazenamento antes do conceito de Gerenciamento do Ciclo de Vida das Informações focalizou em utilizar a infra-estrutura de armazenamento tão eficientemente quanto possível. Historicamente, por exemplo, os dados foram movidos entre meios de armazenamento ou suprimidos de acordo com a data dos arquivos, porque se pensava que os dados mais antigos tinham menos valor.

   Com Gerenciamento do Ciclo de Vida das Informações, os dados são movidos em intervalos predeterminados, de acordo com seu atual valor para o negócio. Assim evita-se dedicar recursos mais caros de armazenamento a dados que têm pouco valor real para os negócios. As

organizações devem avaliar o valor de negócio dos dados e a relevância das exigências regulatórias. Os processos e as políticas definidas devem ser estabelecidos para assegurar que os dados sejam direcionados dinamicamente à posição mais apropriada de armazenamento.

b) O Gerenciamento do Ciclo de Vida das Informações transcende a gerência de armazenamento, de dados e de informação. O gerenciamento de armazenamento sozinho não é suficiente para suportar objetivos de Gerenciamento do Ciclo de Vida das Informações da organização. Por exemplo, quando usuários de desktops atualizam o sistema operacional, as propriedades associadas aos seus arquivos normalmente são alteradas. Tais modificações podem comprometer a conformidade com regulamentos, que exigem a data exata de arquivos. Assim, através de Gerenciamento do Ciclo de Vida das Informações, as precauções apropriadas serão tomadas para assegurar a integridade de tais atributos dos dados, com o uso de ferramentas automatizadas.

Como parte de toda a estratégia de Gerenciamento do Ciclo de Vida das Informações, é importante para as organizações assegurar a identidade e os controles de acesso dos recursos computacionais, de modo que perguntas como: “A quem foi dado o acesso a esta informação?” e “Quem modificou estes dados e quando?” possam ser respondidas.

Porque o Gerenciamento do Ciclo de Vida das Informações acopla uma escala tão larga de funções de gerência de Tecnologia da Informação, ela apresenta claramente algumas dificuldades tecnológicas. Uma boa estratégia é

implementar o Gerenciamento do Ciclo de Vida das Informações em estágios incrementais, a fim obter primeiramente os benefícios mais importantes para a organização como, por exemplo, a conformidade com regulamentos, reduções no custo de armazenamento, ou reduzir a exposição de informações a riscos, aconselha Geronaitis (2005).

2.4.4 Recomendações para *Backup* e Recuperação de Dados

A otimização do *backup*, visando melhorias na recuperação dos dados, não trata só de aperfeiçoar o desempenho de armazenamento e ajustes na configuração de *software*, mas Dorion (2006) considera também outros aspectos, entre eles:

a) Analisar os negócios da organização para fazer o *backup* apenas dos dados necessários.
b) Categorizar os dados baseando-se na prioridade de recuperação.
c) Utilizar *backup* completo e incremental e entender como o *backup* está sendo feito para não fazer *backup* de arquivos repetidos.
d) Assegurar-se de que a largura de banda da rede e o subsistema do disco sejam capazes de suportar uma quantidade grande de dados, tais como a recuperação do *backup* completo.
e) Agendar o *backup* e as tarefas administrativas para não atrapalhar a disponibilidade do sistema.
f) Monitorar de maneira pró-ativa os processos de *backup* é o melhor modo de assegurar e manter o *backup* e a recuperação.

Segundo Bigelow (2006), a maior fraqueza em relação ao *backup* é que a estratégia freqüentemente é confundida com as ferramentas. Os analistas

são rápidos para notar as ferramentas centrais para o *backup* como *software* e *hardware*, mas a disponibilidade não garante uma prática de *backup* confiável. Por exemplo, uma biblioteca virtual de fitas não garante que os dados cruciais estão sendo armazenados adequadamente, nem que são recuperáveis.

Além de dar maior importância à escolha de *hardware* e *software*, muitos analistas se preocupam muito com o desempenho e rapidez do *backup*, não dando atenção a grande consideração que requer a recuperação do *backup*.

De acordo com Cook (2006b), não é necessário o *backup* de todo o sistema, isto pode aumentar a janela de *backup* e diminuir o desempenho. O *backup* bem sucedido necessita de estratégias, como cuidado no planejamento e decisão de quais tipos dos dados fazer o *backup* e com qual freqüência, eliminando duplicatas e outros tipos de dados desnecessários, possibilitando a restauração de dados de maneira mais rápida.

Também é preciso atender a algumas exceções para usuários ou departamentos que têm necessidade de certos tipos de dados, que aparentemente seriam desnecessários para outros setores da organização.

Para diminuir a quantidade de *backup*, Cook (2006b) lembra que as aplicações normalmente precisam ser armazenadas com menos freqüência que os dados. Colocar aplicações em volumes separados de arquivos de dados e de arquivos de registros pode-se reduzir o tempo de *backup* e recuperação dos dados.

De acordo com Bigelow (2006), as estratégias de *backup* podem:

a) Ajudar a ajustar um *Recovery Time Objective* apropriado, permitindo que uma empresa identifique e dê prioridade a aplicações de missão crítica e

determine como as aplicações precisam ser recuperadas em caso de emergência.

b) Ajudar a deixar o *Recovery Point Objective* apropriado determinando uma freqüência e programação de *backup* para cada tipo de dados.
c) Selecionar tecnologias de *backup* mais apropriadas e determinar o nível de investimento necessário para essas tecnologias.
d) Atribuir um período de retenção apropriado para cada tipo de dado de acordo com exigências regulatórias e de continuidade de negócios.

De acordo com Bigelow (2006), mesmo o plano de *backup* de dados sendo bem detalhado, é ineficiente sem considerações de *Recovery Point Objective* e de *Recovery Time Objective*.

Conforme Zhu et al (2005), para reduzir o tempo de recuperação, *Recovery Time Objective*, há diversos pontos a considerar, entre eles:

a) Arquivos de configuração de sistema e *backup*.
b) Estimativa de tempo necessário para executar os procedimentos de recuperação, incluindo o tempo de identificar o problema e a solução e o tempo de restaurar os dados dos meios de armazenamento.
c) Prioridade aos procedimentos de recuperação. Por exemplo, se o *cache* e o outro método de armazenamento forem utilizados, os usuários podem acessar os dados no *cache*, enquanto o restante dos dados é restaurado.
d) Documentos de procedimentos de recuperação para situações diferentes.
e) Desenvolvimento de uma estratégia equilibrada entre o custo do *backup* e a velocidade da recuperação.

Segundo Bigelow (2006), não há estratégia de *backup* única. Cada organização deve formular uma estratégia de acordo com suas necessidades de *backup*, conformidade ou recuperação de desastre. O problema é complicado principalmente pela variedade de tipos de dados que devem ser tratados diferentemente, envolvendo geralmente uma mistura dos produtos para suportar a diversidade de tipos de *backup*.

De acordo com o CERT (2003), logo que gerado, o *backup* deve ser testado, e revisado periodicamente. Deste modo será possível descobrir problemas em dispositivos e locais de armazenamento, podendo assim evitar dificuldades na recuperação.

Conforme Collet (2005), muitas companhias não têm um responsável que seja o mesmo por todo o processo de transporte e guarda dos dados, e nem meios claros de autenticação de pessoal e garantia de transporte, de um local para outro. Assim o *backup* pode expor os dados sensíveis quando transportado para o local de armazenamento devido à falta de segurança física e lógica.

O processo de *backup* é muito mais complexo do que simplesmente examinar e entregar as mídias para serem armazenadas. A análise dos riscos começa no trajeto das mídias do ponto de origem ao local de armazenamento e atribui responsabilidades para cada etapa, utilizando recursos seguros. Há várias maneiras de se transportar com segurança. De acordo com Collet (2005), para uma viagem tranqüila e mitigação dos riscos é importante considerar, pelo menos, estas quatro estratégias:

a) Transportar as mídias com os dados sensíveis através de escoltas seguras: Para resguardar os dados sensíveis é necessária uma

estratégia de alto nível de segurança para classificar os dados em categorias, por exemplo: altamente sensíveis para informações como estados de saúde de pacientes; confidenciais para informações como planos de negócios e dados dos clientes; e gerais para informações como correspondências.

b) Utilizar serviço de transporte e entrega especializado e criptografar os dados do *backup*: A criptografia pode ser aplicada de várias maneiras. Uma das soluções é criptografar os dados sensíveis automaticamente, quando são criados. A maioria dos sistemas de banco de dados vem com esquemas internos de criptografia, mas se não vierem é possível utilizar programas externos para fazer a criptografia.

c) Esquecer o serviço de transporte e utilizar uma conexão segura de Internet. Para a maioria de organizações que trabalham com grandes volumes de informações, a quantidade de dados em fitas é demais para uma conexão de Internet, e o custo para criar redes dedicadas é ainda muito elevado, porém limitando tais transmissões à informação altamente sensível pode-se reduzir os custos.

d) Saber exatamente quem faz a manipulação dos dados sensíveis quando chegam às instalações de armazenamento. A companhia deve fiscalizar o pessoal que guarda os dados, e pedir garantia de segurança para a empresa que faz o transporte e armazenamento. Deve-se estabelecer um conjunto de políticas de segurança que sejam respeitadas por todos que manipulam os dados e ter garantia de que as empresas terceirizadas têm o controle do pessoal que manipula os dados.

No local onde é guardado o *backup*, alguns cuidados devem ser considerados, segundo o CERT (2003):

a) O local deve ser restrito, para evitar que pessoas não autorizadas tenham acesso ao *backup*;
b) O local deve ser protegido contra agentes naturais prejudiciais aos dados ou recursos computacionais, como poeira, calor, umidade, incêndio; etc.

As recomendações a serem adotadas dependem das estratégias da organização. Para que sejam adotadas as melhores decisões é importante que o planejamento de *backup* de dados seja elaborado de acordo com os negócios e necessidades das organizações.

3 METODOLOGIA

Neste capítulo, é apresentado o tipo de pesquisa, a sua conceituação, os critérios para a seleção dos respondentes pesquisados e os procedimentos seguidos para a coleta e o tratamento de dados.

3.1 TIPO DE PESQUISA

Esta pesquisa é exploratória e descritiva, telematizada, documental e bibliográfica, além de ser de campo.

De acordo com Vergara (2000), a pesquisa do tipo exploratória é realizada em área na qual há pouco conhecimento acumulado e sistematizado. Por sua natureza de sondagem, não comporta hipóteses que, todavia, poderão surgir durante ou ao final da pesquisa.

Segundo Lakatos e Marconi (1999), a pesquisa do tipo descritiva aborda quatro aspectos: descrição, registro, análise e interpretação de fenômenos atuais, objetivando o seu funcionamento no presente.

Exploratória e descritiva quanto aos fins, devido ao fato de estar explorando um assunto com pouca literatura na área Acadêmica e Empresarial, e porque busca descrever as características do assunto tratado.

Em relação aos meios a pesquisa é, em sua maior parte, telematizada, uma vez que a maioria das referências é obtida na Internet. É bibliográfica, pois se avalia o que foi publicado de relevante sobre o tema da pesquisa, e documental porque analisa documentos, principalmente normas, referentes à Segurança da Informação. Também é de campo, pois foi realizado um levantamento, através de questionários, sobre estratégias de *backup* de dados.

3.2 UNIVERSO E AMOSTRA

O universo é composto por responsáveis pela Segurança da Informação de organizações do Estado São Paulo: Capital, Vale do Paraíba e Campinas, que estavam dispostos a colaborar com este trabalho. Através de explicações dadas por telefone, *e-mail* ou pessoalmente foi mostrada a importância da pesquisa e que os respondentes seriam também beneficiados ao receberem o resultado da consolidação das respostas ao questionário.

Observa-se que o presente trabalho conta com a amostra acessível, onde a escolha dos profissionais foi feita de forma individualizada, levando a que se obtenha uma visão mais qualitativa do que quantitativa da realidade. No futuro poder-se-á adotar uma amostra estatística e tentar obter mais informações quantitativas. Foram realizadas a localização e abordagem de profissionais responsáveis pela área de Segurança da Informação, que trabalham há um ano ou mais nesta área e que tratam estrategicamente de informações críticas.

Sobre as organizações onde trabalham os questionados, não foi revelado nenhum aspecto sobre ramo ou porte, por se tratar de um assunto da área de Segurança da Informação.

Foram entregues quarenta e cinco questionários, destes retornaram 31, mas apenas 26 estavam válidos para serem utilizados nesta pesquisa, pois alguns não responderam totalmente à parte A do questionário, que se refere à identificação do questionado.

Se, entretanto o termo amostra conduz à expectativa de avaliação estatística, adverte-se que não é esse o caso aqui descrito. Talvez se possa,

para maior clareza, denominar de Consulta a Especialistas Acessíveis a técnica de questionamento empregada.

Mesmo sabendo da Importância da pesquisa e concordando em responder o questionário alguns dos profissionais não entregaram as respostas a tempo de serem utilizadas nesta pesquisa. Para aumentar o número de respondentes, o questionário foi aplicado em dois cursos de especialização em Segurança da Informação em São Paulo e em São José dos Campos, resultando em uma amostra com a maioria dos respondentes com cursos nesta área.

3.3 COLETA DE DADOS

A pesquisa bibliográfica é composta de materiais relevantes, já publicados sobre Segurança da Informação, focalizando estratégias de *backup* de dados, encontrados, na sua maioria, em *sites* na *Internet*. Dentre os principais *sites* pesquisados destacam-se:

- *National Institute of Standards and Technology* (NIST),
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT),
- *International Business Machines* (IBM),
- Empresas de *Software* para *backup* e Segurança da Informação: *Symantec* e *Veritas.*
- Site internacional com publicações de profissionais de Tecnologia da Informação reconhecidos: *Techtarget*.
- Site brasileiro com cursos e produtos na área de Segurança da Informação: Módulo *Security Magazine*.

- Sistema da Biblioteca Digital Brasileira de Teses de Dissertações (BDTD) do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), ou diretamente nos sites de Bibliotecas como da UNITAU.

Quanto à pesquisa documental, são estudadas as normas pertinentes, como a NBR ISO/IEC 17799 da Associação Brasileira de Normas Técnicas (ABNT).

Na pesquisa de campo, solicitam-se respostas ao questionário elaborado, que foi aprovado pelo Comitê de Ética da UNITAU e se encontra anexo a este trabalho. Neste questionário foram colocadas perguntas resultadas dos textos e discussões sobre o tema e também outras que emergiram nas entrevistas iniciais com os possíveis respondentes. Dessa forma o questionário é um documento que agrega questões originadas da revisão de literatura e outras julgadas importantes advindas de alguns dos questionados.

O questionário aplicado é composto de vinte e cinco questões, sendo cinco sobre a definição do perfil dos respondentes e vinte que procuram reproduzir as escolhas estratégicas dos profissionais de Segurança da Informação sobre o planejamento de *backup* de dados, dividindo estas vinte perguntas em oito áreas sobre Segurança da Informação e *backup* de dados:

A - Plano de *backup* de dados, questões de 1 a 4;

B - Políticas, Recomendações e Certificações, questões de 5 a 9;

C - Tratamento e Classificação dos Dados, questões de 10 e 11;

D - Facilidades de *backup*, Disponibilidade e Recuperação, questões 12 e 13;

E - Tecnologias para *backup* de dados questões 14 e 15;

F - *Backup* em Site Remoto questões 16 e 17;

G - Documentação, questão 18

H - Testes e Avaliações do plano de *backup* de dados, questões 19 e 20.

Para cada questão são apresentadas alternativas fechadas e a opção: outros, onde o respondente pode completar as opções, na contribuição de apresentar estratégias organizadas em um único documento.

A princípio foram enviados os questionários para profissionais nas organizações onde trabalham, através de *e-mail*. Devido ao retorno ter sido pequeno, optou-se por abordar os profissionais em cursos de pós-graduação, especialização em Segurança da Informação.

3.4 TRATAMENTO DOS DADOS

Os dados colhidos nesta pesquisa são mostrados quantitativamente através de gráficos e qualitativamente através de textos com análise das respostas conforme a incidência e através das respostas abertas pertinentes aos temas da pesquisa. Para a geração dos gráficos foi usado o *software* Excel da Microsoft.

4 RESULTADOS E DISCUSSÃO

O resultado principal obtido ao longo da presente pesquisa é o desenvolvimento da proposta aqui apresentada, estruturada em etapas para o planejamento de *backup* de dados. A proposta é baseada em normas, padrões e recomendações da literatura e profissionais da área de Segurança da Informação, visando à integridade, confiabilidade e disponibilidade da informação e está de acordo com políticas de Segurança da Informação e com Plano de Continuidade de Negócios.

Para chegar ao resultado principal da forma como apresentado, teoricamente coerente com a literatura revista e estudada, foi feita a consolidação das respostas, destacando e discutindo os pontos mais importantes do questionário.

Antes, são mostrados dados de algumas pesquisas sobre *backup* de dados, para melhor compreensão do problema desta dissertação. Observa-se que a conjunção aqui encontrada ocorre também em outros ambientes, como a seguir.

4.1 PESQUISAS SOBRE *BACKUP* DE DADOS

Uma pesquisa conduzida pela empresa de soluções de segurança Verio em 2006 nos Estados Unidos, segundo a IT WEB (2006) revelou o seguinte:

- Apesar de muitos usuários de pequenos negócios e *home office* afirmarem que a proteção de dados e serviços de *backup* seriam prioridade em suas listas de investimento dos próximos 18 meses, atualmente 45% dos respondentes não têm nenhum plano de

recuperação de dados para as informações armazenadas em seus computadores.

- 70% dos pequenos negócios informaram que não considerariam um único incidente de perda de dados expressivo e caro, e 53% dos respondentes contaram que já tinham perdido informações armazenadas em um computador, e 64% deles disseram que os prejuízos foram originados por eventos comuns, como quebra de disco.

Um estudo da *Dynamic Markets Limited*, feito na Europa, encomendado pela empresa de segurança *Symantec*, revela que gerentes de Tecnologia da Informação são displicentes em relação ao processo de *backup*, principalmente de mensagens de *e-mail*. Seguem algumas notas da pesquisa, apontadas por Kirk (2006):

- Quase metade dos gerentes de Tecnologia da Informação de 1,7 mil companhias européias não recebe diretrizes para salvar mensagens eletrônicas, mesmo com a crescente conscientização da necessidade do cuidado para gerenciá-las.
- Enquanto a maior parte dos departamentos de Tecnologia da Informação faz uma cópia de *backup* toda noite, apenas 4% das companhias fazem as cópias durante o dia, arriscando perder os dados, e não poder recuperá-los prontamente.
- 42% revelaram que faz *backup* de informações guardadas em dispositivos móveis e notebooks.
- 71% dos gestores de Tecnologia da Informação não arquivam e-mails de empregados que deixam suas organizações, mensagens que poderiam ser precisas em casos judiciais.

- 45% dos responsáveis pela Tecnologia da Informação deixam a responsabilidade pelo *backup* de e-mail para os funcionários.
- Os empregados freqüentemente não têm informações corretas sobre como são gerenciadas suas mensagens eletrônicas.
- Uma grande parte dos empregados, 78%, respondeu que eles, e não o departamento de Tecnologia da Informação, controlam os e-mails que podiam ou não ser salvos.

As pesquisas revelam que mesmo conscientes da necessidade do *backup* e recuperação dos dados, os gerentes de Tecnologia da Informação e outros usuários de sistemas de computadores não gerenciam os dados de maneira correta, muitas vezes não tendo planos e nem políticas para *backup* de dados.

O *backup* é um processo importante, tanto para pequenos e grandes negócios e organizações, e simplesmente é tido como cópia de segurança. Entretanto, no ambiente de Tecnologia da Informação a proteção dos dados, através do *backup*, pode ser utilizada para prover continuidade de negócios, replicação de dados, recuperação de desastres e redução nos custos de infra-estrutura.

A maneira para assegurar os dados, seja local ou remotamente, pode ser um desafio desanimador, se não forem conhecidas e estabelecidas normas e estratégias para este fim. Portanto, a análise do questionário buscará por estratégias recomendadas por profissionais da área de Segurança da Informação, para complementar as já indicadas pela literatura.

4.2 CONSOLIDAÇÃO DAS RESPOSTAS AO QUESTIONÁRIO

O principal objetivo do *backup* é prover a recuperação segura e rápida dos dados quando necessário e de acordo com o custo benefício. Para ajudar a alcançar este objetivo, ou seja, conseguir estratégias para este fim, além do estudo e revisão da literatura técnica e normativa, as respostas ao questionário e ou recomendações dos profissionais de Tecnologia da Informação selecionados foram analisadas.

A maioria dos respondentes disse que o questionário estava bem completo, não tendo muito a acrescentar. Também consideraram que a seqüência das perguntas permitiu um bom entendimento dos objetivos da pesquisa.

A seguir a consolidação das respostas é realizada por partes de acordo com o questionário, também são fornecidos gráficos para ilustrar a pesquisa.

Nas primeiras cinco perguntas do questionário foi identificado o perfil dos respondentes. Para participar da pesquisa todos têm um ou mais anos de trabalho na área de Segurança da Informação e precisam tratar os dados críticos das organizações, onde trabalham.

A maioria dos respondentes, vinte e um (21), já trabalha na área de Segurança da Informação há mais de dois anos conforme a Figura 1.

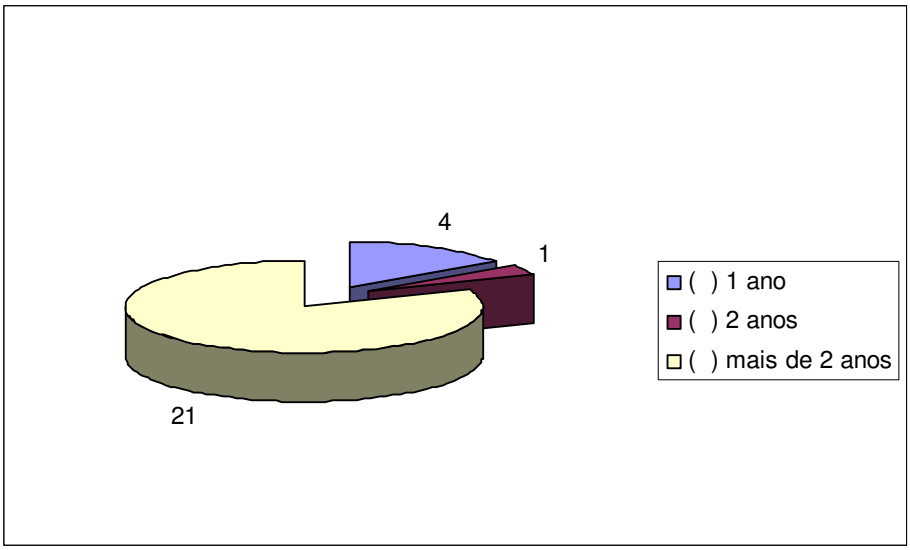

Figura 1 - Tempo de trabalho na área de Segurança da Informação

A quantidade de respondentes com curso na área de Segurança da Informação é de vinte e um (21), e é ilustrada na Figura 2.

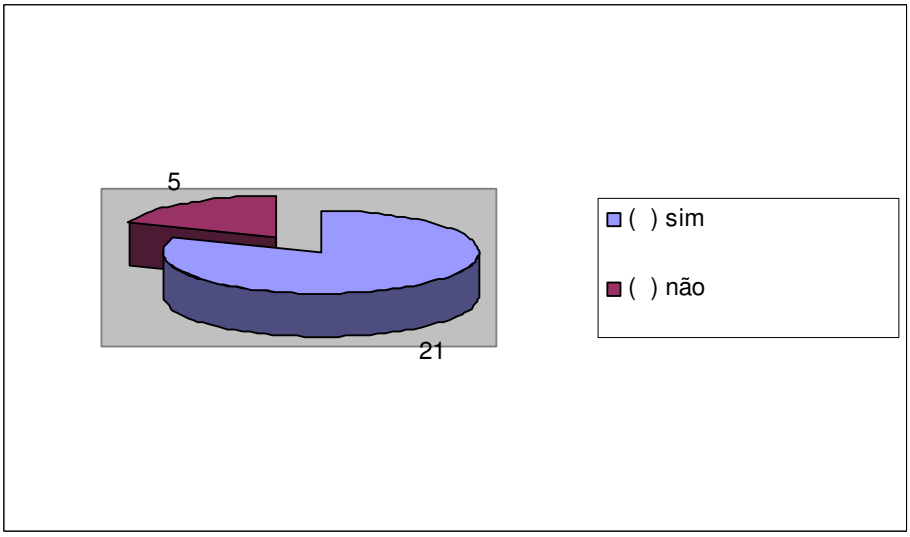

Figura 2 - Cursos na área de Segurança da Informação

Esta pesquisa contou, na sua maioria, com respondentes com cursos na área de Segurança da Informação, e que já trabalham há mais de dois anos nesta área, ou seja, profissionais que podem recomendar estratégias para a maior segurança dos dados.

Após a identificação do usuário, são verificadas as partes do questionário que tratam de estratégias de *backup* de dados.

Os gráficos apontados para a ilustração da pesquisa são baseados nas perguntas e respectivas alternativas do questionário. As recomendações apresentadas nos gráficos sem parênteses "( )" são as indicadas pelos respondentes.

A – Plano de *Backup* de dados

A primeira pergunta teve o propósito de saber os motivos pelos quais se deve planejar o *backup* de dados.

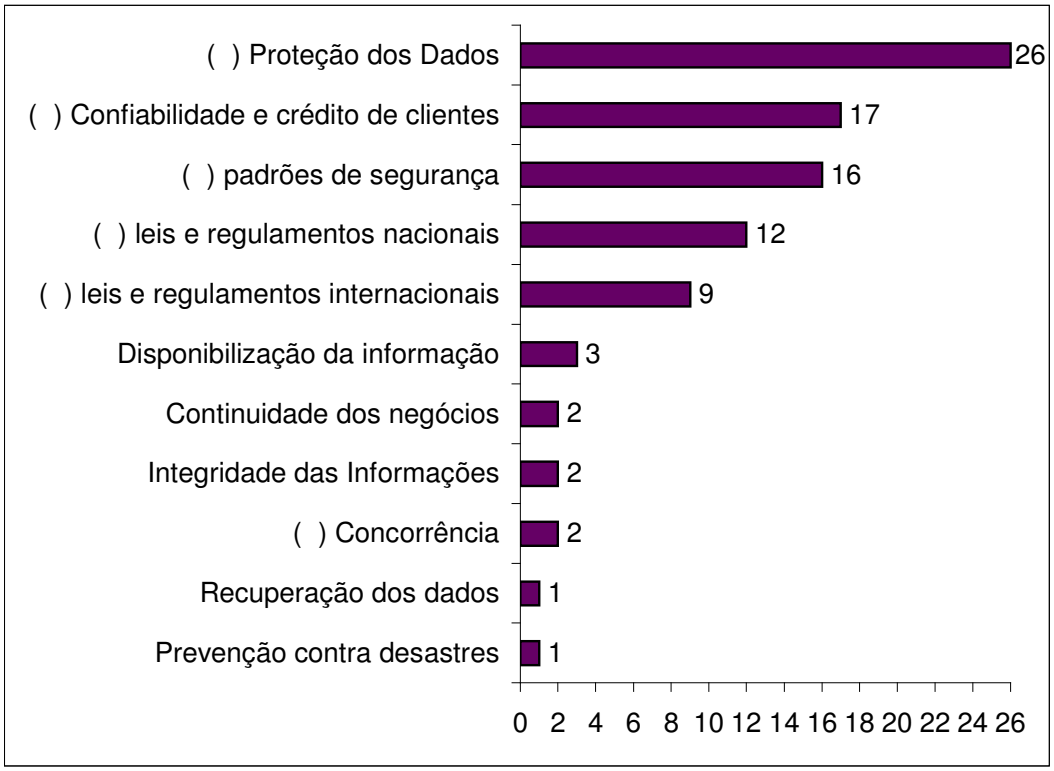

Figura 3 - Principais razões para se ter um plano de *backup*

Segundo a Figura 3, todos os vinte e seis (26) questionados apontam que o principal motivo para o *backup* é a proteção dos dados.

A confiabilidade dos clientes, indicada pela maioria dos respondentes, dezessete (17), mostra conscientização de que paradas nos sistemas podem

ocasionar a perda do cliente. Este fator depende do tipo de negócios e sistemas da organização. Para algumas organizações as paradas nos sistemas podem ser invisíveis para os clientes,

A conformidade com padrões de segurança, apontada por dezesseis (16) dos respondentes, além de auxiliar na proteção dos dados, ocasiona a confiabilidade dos clientes.

A conformidade com leis e regulamentos nacionais e internacionais foi menos indicada, do que a conformidade com padrões de segurança. Este fato mostra que a preocupação dos respondentes é mais voltada para padrões de Segurança da Informação, e que o atendimento a leis e regulamentos pode ser mais ligado ao pessoal da área administrativa.

O item “concorrência” foi indicado apenas por dois (2) dos respondentes, porém se existe a preocupação com o cliente, a concorrência também pode ser colocada como um motivo importante para o planejamento de *backup*.

Além dos motivos para planejamento de *backup* apontados pelo questionário, outros foram acrescentados por alguns dos respondentes como: Planejar o *backup* para ter a informação sempre disponível e integral evitando paralisações nos sistemas. Também para prevenir contra desastres e para recuperar a informação, caso necessário, dando continuidade aos negócios.

Conclui-se com a Figura 3, que os profissionais de Tecnologia da Informação estão conscientes das necessidades de se ter um plano de *backup* para a proteção dos dados e para a continuidade dos negócios, não só para caso de desastres, mas para atender a padrões de segurança e manter a confiabilidade e crédito dos clientes.

Após encontrar os motivos para o planejamento de *backup* de dados, procurou-se identificar o que é necessário e mais relevante para o plano e quais profissionais: Alta Administração, Supervisão de Tecnologia da Informação, Corpo técnico de Tecnologia da Informação, Corpo técnico Administrativo e/ou outros que devem ser responsáveis por estas etapas de planejamento.

Através da Figura 4, serão discutidas as questões 3 e 4 da parte 2 do questionário, que tratam sobre as partes de um plano de *backup* de dados. A questão 4, que, além disso, trata das equipes responsáveis pelo plano, também será ilustrada através de tabelas, conforme as respostas ao questionário.

A Figura 4 mostra as partes de um plano de *backup* de dados estipuladas no questionário e as acrescentadas pelos respondentes, referentes à pergunta 3 da parte 2 do questionário, e o total de pontos para cada parte. Cada respondente pôde dar o valor de 0 a 3 para cada opção. Ou seja, se todos os respondentes dessem o valor 3 para uma opção esta teria o total de 78 pontos (26x3).

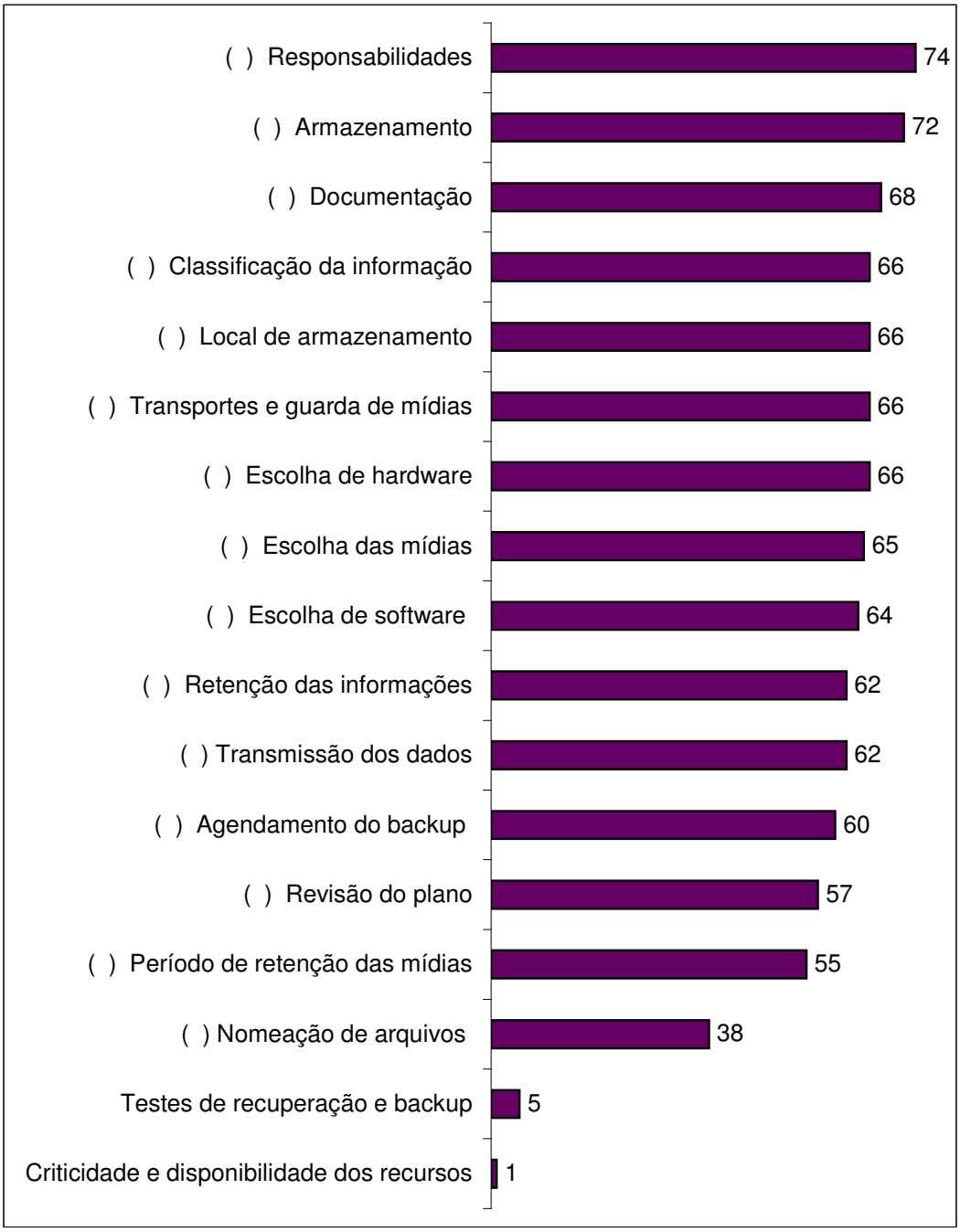

Figura 4 - Partes de um plano de *backup* de dados

É possível verificar todas as partes de um plano de *backup* de dados indicadas pelo questionário, e as equipes apontadas para as respectivas partes

na Tabela 1. Conforme o questionário, são apontados os seguintes índices e equipes:

1- Alta administração
2- Supervisão de Tecnologia da Informação
3- Corpo técnico de Tecnologia da Informação
4- Corpo técnico Administrativo

Foi colocada, na questão 4, a opção Outros, onde se pode colocar mais equipes. Alguns dos questionados indicaram que as seguintes equipes também devem participar:

- Equipe dedicada ao *backup*
- Comitê interno de Segurança da Informação
- Jurídico e
- Usuários em geral

As equipes apontadas pelos respondentes são representadas nas tabelas por “O” de Outros.

Na Tabela 1 os números indicados depois da primeira linha representam a quantidade de respondentes que indicaram a mesma equipe para cada parte de plano de *backup* de dados. A somatória dos números é igual a 26, que é o número de respondentes. Para melhor entendimento da Tabela 1, ela foi dividida em outras tabelas, onde fica mais evidente a indicação dos respondentes.

Tabela 1 - Equipes para o plano de *backup*

Partes do Plano/Equipes	**1**	**2**	**3**	**4**	**O**	**1,2**	**2,3**	**3,4**	**1,2,3**	**2,3,4**	**1,2,3,4,**	**2,3,4,O**	**1,2,4**	**2,3,O**	**1,4**	**1,2,4,O**	**2,4**	**1,4,O**	**1,3**	**1,3,4**	**Total**
Responsabilidades	4	11	1			5	1		2				1	1							26
Armazenamento		10	5	1			7	2	1												26
Documentação		6	8	2		1	7	1	1												26
Classificação da informação	4	7	1	1		1	3	1			1		3	1	1	1	1				26
Local de armazenamento	1	9	2			5	3		2	2					2						26
Transportes e guarda de mídias	1	6	3		1	1	7	1		2	1			1	2						26
Escolha de *hardware*		6	3	1		2	11		1	1										1	26
Escolha das mídias		5	4	1	1	2	11	1		1											26
Escolha de *software*		7	3			2	11			1					1					1	26
Retenção das informações	4	6		2		2	3			1			2	1	1		2	2			26
Transmissão dos dados	1	8	5				9		1	1					1						26
Agendamento do *backup*		4	12	1			7	1		1											26
Revisão do plano	3	8	1	2		3	2		1	1	2		2			1					26
Período de retenção das mídias	4	6	1	1		4	3	1	1			1		1	1		1	1			26
Nomeação de arquivos		5	11	2			3	2		1			1						1		26

Observa-se que o índice “O” de outros varia de tabela a tabela, dependendo da natureza de ocupação. Os textos que descrevem as tabelas identificam a ocorrência e o significado deste índice.

De acordo com a classificação dada pelos respondentes, conforme a Figura 4, a parte mais importante para a realização de um plano de *backup* de dados é a definição de responsabilidades. Isto mostra que não basta ter o plano sem indicar claramente os responsáveis por ele. Os responsáveis, além de planejar o *backup*, devem verificar se o plano está sendo executado, mantido e revisado.

A Tabela 2 demonstra as equipes que devem definir as responsabilidades para as partes de um plano de *backup* de dados, conforme a questão 4 da parte 2 do questionário.

Tabela 2 - Equipes para a definição de responsabilidades

Partes do Plano/Equipes	**2**	**1,2**	**1**	**1,2,3**	**3**	**2,3**	**1,2,4**	**2,3,O**	**Total**
( ) Responsabilidades	11	5	4	2	1	1	1	1	26

Segundo grande parte dos questionados onze (11), a Supervisão de Tecnologia da Informação da organização deve ser responsável pela definição de responsabilidades. Cinco (5) dos respondentes concordam que a Alta Administração junto com a Supervisão de Tecnologia da Informação devem fazer esta parte, outros quatro (4) preferem que apenas a Alta administração da organização se encarregue de planejar a definição de responsabilidades. Na última coluna da Tabela 2, o “O” de outros se refere ao Comitê interno de Segurança da Informação.

As opiniões diferem, mas a maior parte concorda que o pessoal da área de Tecnologia da Informação que deve definir as responsabilidades com a ajuda da Alta Administração.

A segunda parte mais importante, segundo a Figura 4, de acordo com os respondentes, é sobre os procedimentos de armazenamento dos dados. Esses procedimentos são alguns dos quais determinarão a eficácia na recuperação dos dados. É nesta parte que se pode verificar se os dados serão armazenados local e/ou remotamente, os tipos de recursos necessários para o armazenamento, etc.

Tabela 3 - Equipes para os procedimentos de armazenamento

Partes do Plano/Equipes	**2**	**2,3**	**3**	**3,4**	**4**	**1,2,3**	**Total**
( ) Armazenamento	10	7	5	2	1	1	26

Segundo a Tabela 3, os procedimentos de armazenamento, segundo dez (10) dos participantes da pesquisa, devem ser planejados pela Supervisão de Tecnologia da Informação. Sete (7) dos questionados preferem que a Supervisão de Tecnologia da Informação trabalhe com o Corpo Técnico de Tecnologia da Informação para este planejamento. Outros cinco (5) indicam que o corpo técnico de Tecnologia da Informação pode fazer esta parte sozinho.

As opiniões diferem, mas a maioria concorda que são os profissionais de Tecnologia da Informação os responsáveis por esta parte, de acordo com a Tabela 3.

O terceiro item mais indicado para o planejamento de *backup* de dados foi sobre os procedimentos de documentação, conforme a Figura 4. Esses

procedimentos podem indicar como a documentação deve ser criada, guardada, utilizada e revisada.

Tabela 4 - Equipes para os procedimentos de documentação

Partes do Plano/Equipes	**3**	**2,3**	**2**	**4**	**1,2**	**3,4**	**1,2,3**	**Total**
( ) Documentação	8	7	6	2	1	1	1	26

Os procedimentos de documentação devem ser planejados pela Supervisão ou pelo corpo técnico de Tecnologia da Informação, ou pelos dois em conjunto, segundo grande parte dos participantes da pesquisa. Poucos respondentes pensam que o pessoal da área administrativa deve definir os procedimentos de documentação, segundo a Tabela 4.

Os procedimentos de classificação da informação também foram apontados como importantes para o plano de *backup* de dados. Esta parte será tratada mais à frente nas questões 10 e 11 da parte 2 do questionário, pois é a classificação dos dados que determinará a escolha do *backup* e prioridade na recuperação.

Tabela 5 - Equipes para a classificação de informações

Partes do Plano/Equipes	**2**	**1**	**2,3**	**1,2,4**	**3**	**4**	**1,2**	**3,4**	**1,2,3,4,**	**2,3,O**	**1,4**	**1,2,4,O**	**2,4**	**Total**
( ) Classificação da informação	7	4	3	3	1	1	1	1	1	1	1	1	1	26

Pela Tabela 5 é possível verificar que a classificação das informações deve ser feita por várias equipes da organização, principalmente pela supervisão de Tecnologia da Informação indicada por sete (7) dos questionados e pela Alta Administração, segundo quatro (4) dos respondentes. Na Tabela 5, décima coluna, o “O” de outros se refere ao comitê interno de

Segurança da Informação, e na décima segunda coluna, o “O” se refere aos usuários em geral.

Definições importantes tais como a definição de local de armazenamento, e transporte das mídias, foram destacadas como tão importantes quanto à classificação dos dados, conforme a Figura 4.

Tabela 6 - Equipes para a definição de locais de armazenamento

Partes do Plano/Equipes	**2**	**1,2**	**2,3**	**3**	**1,2,3**	**2,3,4**	**1,4**	**1**	**Total**
( ) Local de armazenamento	9	5	3	2	2	2	2	1	26

Segundo grande parte, nove (9) dos respondentes, os procedimentos para a definição do local de armazenamento devem ficar por conta dos supervisores de Tecnologia da Informação, segundo alguns, cinco (5), deve haver a ajuda da Alta Administração. Outros três (3) preferem que o corpo técnico e a supervisão de Tecnologia da Informação façam essas definições. Outros concordam que o pessoal da área técnica administrativa deve participar destas definições, de acordo com a Tabela 6.

Tabela 7 - Equipes para os procedimentos de transporte e guarda de mídias

Partes do Plano/Equipes	**2,3**	**2**	**3**	**2,3,4**	**1,4**	**1**	**O**	**1,2**	**3,4**	**1,2,3,4,**	**2,3,O**	**Total**
( ) Transportes e guarda de mídias	7	6	3	2	2	1	1	1	1	1	1	26

Segundo sete (7) dos respondentes a definição dos procedimentos para transportes e guardas de mídias devem ficar por conta dos profissionais de Tecnologia da Informação, tanto supervisão quanto técnica. Outros seis (6) preferem que só a supervisão defina esses procedimentos, já outros três (3) preferem só a atuação do pessoal técnico de Tecnologia da Informação nesta parte. Segundo a Tabela 7 alguns poucos respondentes concordam que a área

administrativa deve participar da definição dos procedimentos de transporte e guarda de mídias.

Na Tabela 7, na sétima coluna o “O” de outros se refere à equipe de *backup*, e na última coluna se refere ao comitê interno de Segurança da Informação.

Conforme a Figura 4, os procedimentos de escolha de *hardware* foram mais considerados que os de escolha de mídia, e *software*. Os três são complementares, e dependem entre si para o eficaz *backup* e recuperação dos dados.

Tabela 8 - Equipes para os procedimentos de escolha de *hardware*

Partes do Plano/Equipes	**2,3**	**2**	**3**	**1,2**	**4**	**1,2,3**	**2,3,4**	**1,3,4**	**Total**
( ) Escolha de *hardware*	11	6	3	2	1	1	1	1	26

De acordo com a Tabela 8, segundo onze (11) dos respondentes, os procedimentos de escolhas de *hardware* devem ser definidos pela supervisão de Tecnologia da Informação, juntamente com seu corpo técnico. Seis (6) concordam que a Supervisão de Tecnologia da Informação pode dar conta desta etapa sem os técnicos e outros três (3) preferem que apenas os técnicos sejam responsáveis pelos procedimentos de escolha de *hardware*.

Esta parte vai depender dos profissionais de Tecnologia da Informação, se os supervisores tiverem conhecimentos técnicos suficientes, não precisarão de auxílio. Ainda, segundo poucos respondentes, o pessoal da área administrativa pode colaborar com a definição dos procedimentos de escolha de *hardware*, de acordo com a Tabela 8.

Tabela 9 - Equipes para os procedimentos de escolha de *software*

Partes do Plano/Equipes	**2,3**	**2**	**3**	**1,2**	**2,3,4**	**1,4**	**1,3,4**	**Total**
( ) Escolha de *software*	11	7	3	2	1	1	1	26

Os procedimentos de escolha de *software* devem ser definidos pela supervisão e corpo técnico de Tecnologia da Informação segundo a maioria dos respondentes. Alguns ainda dizem que é importante a participação das equipes da área administrativa da organização, segundo a Tabela 9.

Tabela 10 - Equipes para os procedimentos de escolha de mídias

Partes do Plano/Equipes	**2,3**	**2**	**3**	**1,2**	**4**	**O**	**3,4**	**2,3,4**	**Total**
( ) Escolha das mídias	11	5	4	2	1	1	1	1	26

Assim como os procedimentos de escolha de *software* e *hardware*, os de escolha de mídias, conforme a Tabela 10, também devem ser de responsabilidade dos profissionais da área de Tecnologia da Informação. Alguns respondentes também dizem ser importante a ajuda de outras equipes. Na Tabela 10, na sexta coluna, o "O" de outros se refere à equipe de *backup*.

Os procedimentos para se determinar o período de retenção das informações vão depender da classificação das mesmas, e o período de retenção vai influenciar na escolha de *hardware*, *software* e mídias para *backup*. Este item deve estar incluso no plano de *backup*, segundo a Figura 4.

Tabela 11 - Equipes para a determinação do período de retenção das informações

Partes do Plano/Equipes	**2**	**1**	**2,3**	**4**	**1,2**	**1,2,4**	**2,4**	**1,4,O**	**2,3,4**	**2,3,O**	**1,4**	**Total**
( ) Retenção das informações	6	4	3	2	2	2	2	2	1	1	1	26

Os procedimentos de definição do período de retenção das informações devem ter a participação de várias equipes da organização, principalmente da supervisão de Tecnologia da Informação e da alta administração, segundo a Tabela 11. Na Tabela 11, na oitava coluna, o “O” de outros se refere à equipe jurídica e aos usuários em geral, na décima coluna se refere ao comitê interno de Segurança da Informação.

Os procedimentos de como agendar o *backup* e de transmissão dos dados para *backup* remoto também são fatores preocupantes para serem incluído no planejamento de *backup* de dados, segundo a Figura 4.

Tabela 12 - Equipes para o agendamento do *backup*

Partes do Plano/Equipes	**3**	**2,3**	**2**	**4**	**3,4**	**2,3,4**	**Total**
( ) Agendamento do *backup*	12	7	4	1	1	1	26

Os procedimentos de agendamento do *backup* devem ficar por conta dos técnicos de Tecnologia da Informação segundo grande parte dos respondentes da pesquisa. Sete (7) concordam que a Supervisão deve participar da definição desses procedimentos junto com os técnicos de Tecnologia da Informação. Já quatro (4) dos respondentes preferem que só a Supervisão de Tecnologia da Informação defina estes procedimentos. Outros poucos respondentes consideram importante a participação dos técnicos da área administrativa para a definição desses procedimentos, segundo a Tabela 12.

Tabela 13 - Equipes para os procedimentos de transmissão dos dados

Partes do Plano/Equipes	**2,3**	**2**	**3**	**1**	**1,2,3**	**2,3,4**	**1,4**	**Total**
( ) Transmissão dos dados	9	8	5	1	1	1	1	26

Os procedimentos de transmissão dos dados devem ser definidos pela supervisão juntamente com os técnicos de Tecnologia da Informação, segundo a Tabela 13, onde é mostrado que nove (9) concordam que seja a supervisão mais os técnicos de Tecnologia da Informação. Oito (8) preferem que só a supervisão defina os procedimentos e outros cinco (5) dizem que os técnicos de Tecnologia da Informação podem definir estes procedimentos sozinhos. Alguns dos pesquisados também acham importante que o pessoal da área administrativa esteja presente na definição dos procedimentos de transmissão dos dados.

Os procedimentos para definir o período de retenção das mídias e de revisão do plano tiveram menos pontuação que os já abordados acima, porém não são menos importantes, e merecem tanta atenção quanto os outros itens.

Tabela 14 - Equipes para os procedimentos de retenção das mídias

Partes do Plano/Equipes	**2**	**1**	**1,2**	**2,3**	**3**	**4**	**3,4**	**1,2,3**	**2,3,4,O**	**2,3,O**	**1,4**	**2,4**	**1,4,O**	**Total**
( ) Retenção das mídias	6	4	4	3	1	1	1	1	1	1	1	1	1	26

De acordo com a Tabela 14, a equipe que deve definir o período de retenção das mídias é a supervisão de Tecnologia da Informação, apontada por seis (6) dos respondentes, a alta administração apontada por quatro (4) dos respondentes, e outros quatro (4) preferem que a supervisão de Tecnologia da Informação trabalhe junto com a alta administração para definir esses procedimentos.

Outros três (3) apontam ser necessário apenas o pessoal da área de Tecnologia da Informação. Segundo a Tabela 14, alguns acham importante a participação de outras equipes. Na Tabela 14, na nona coluna, o “O” de outros

se refere aos usuários em geral, na décima coluna se refere ao comitê interno de Segurança da Informação, e na última coluna à equipe jurídica.

Tabela 15 - Equipes para a definição da periodicidade da revisão do plano

Partes do Plano/Equipes	**2**	**1**	**1,2**	**4**	**2,3**	**1,2,3,4,**	**1,2,4**	**3**	**1,2,3**	**2,3,4**	**1,2,4,O**	**Total**
( ) Revisão do plano	8	3	3	2	2	2	2	1	1	1	1	26

A periodicidade da revisão do plano deve ser definida, segundo oito (8) dos respondentes pela supervisão de Tecnologia da Informação, outros três (3) respondentes preferem que apenas a alta administração da organização decida o período de revisão do plano. Já outros três (3) respondentes acham importante que a supervisão de Tecnologia da Informação trabalhe junto com a alta administração para definirem o período de revisão do plano. Ainda, segundo a Tabela 15, é importante que os profissionais técnicos e de outras áreas também participem da decisão. Na Tabela 15, na última coluna, o "O" de outros se refere à equipe jurídica.

A nomeação de arquivos foi o item menos apontado como importante para o plano de *backup* de dados pelos respondentes, segundo a Figura 4, porém na recuperação de arquivos este item pode se tornar essencial para o melhor desempenho do processo, segundo a literatura já estudada. É preciso maior conscientização sobre este fato.

Tabela 16 - Equipes para a nomeação de arquivos

Partes do Plano/Equipes	**3**	**2**	**2,3**	**4**	**3,4**	**2,3,4**	**1,2,4**	**1,3**	**Total**
( ) Nomeação de arquivos	11	5	3	2	2	1	1	1	26

Os procedimentos para a nomeação de arquivos, segundo onze (11) dos respondentes, devem ser de responsabilidade do corpo técnico de Tecnologia

da Informação. Cinco (5) dos respondentes concordam que esta parte deve ficar com a supervisão de Tecnologia da Informação. E outros três (3) acham importante que tanto a Supervisão quanto o corpo técnico de Tecnologia da Informação participem dessas definições. Conforme a Tabela 16 alguns dos respondentes também consideram importante a participação do pessoal da área administrativa na definição dos procedimentos de nomeação de arquivos.

Outros itens a serem incluídos no planejamento de *backup* de dados, lembrados pelos respondentes foram os procedimentos para testes de recuperação do *backup,* e criticidade, ou seja, o maior grau de dependência do funcionamento e disponibilidade dos recursos.

Os testes de recuperação de dados são essenciais para que esta seja cada vez mais rápida e eficaz, assim será possível identificar os erros antes que eles ocorram e melhorar a rapidez e facilidade da recuperação.

Quanto à criticidade e disponibilidade de recursos: existem muitos requisitos para um bom planejamento e execução do processo de *backup* de dados, porém este vai ser efetivo de acordo com os recursos disponíveis, ou seja, o investimento que a organização fornecerá para este planejamento.

Houve muita divergência nas respostas, mas de acordo com a maioria das respostas, a conclusão é de que a Supervisão e o Corpo técnico de Tecnologia da Informação devem ser os responsáveis pelo plano de *backup* de dados e a Alta administração da Organização também deve participar do planejamento, e a inclusão de outras equipes dependerá das particularidades de cada negócio.

B – Políticas, Recomendações e Certificações

Na fase anterior foi apontada a importância dos procedimentos para a eficácia do *backup* e para que esses se concretizem é importante estabelecer políticas de Segurança da Informação. Também, no Plano de Continuidade de Negócios é essencial inserir procedimentos de recuperação do *backup*.

Buscou-se nesta etapa identificar o que deve ser considerado sobre *backup* de dados em política de Segurança da Informação e Plano de Continuidade de Negócios.

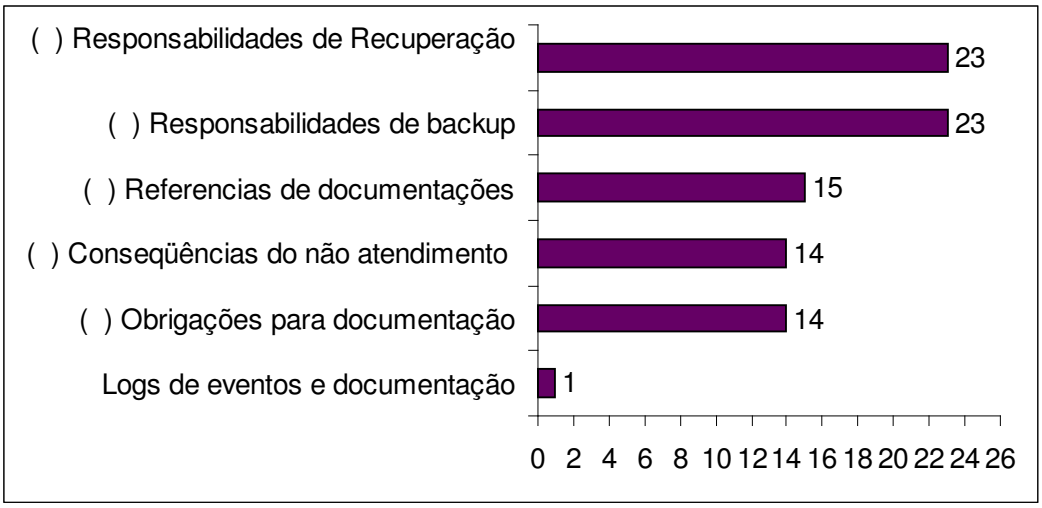

Figura 5 - Considerações para Política de Segurança da Informação

A política de Segurança da Informação deve contar com normas de *backup* de dados, que devem emergir do planejamento de *backup*, estas normas podem ser de responsabilidades gerais de *backup* e recuperação de dados, segundo a grande maioria dos respondentes, vinte e três (23), de acordo com a Figura 5.

É indispensável que seja estabelecido o comprometimento de se documentar o processo de *backup* e a recuperação dos dados para que haja referências na política de Segurança da Informação sobre documentações para auxiliar no processo de *backup*. Segundo a Figura 5, são importantes normas

para a documentação dos dados. Um dos respondentes lembrou que na documentação também devem estar os *logs* (registros) de eventos do processo de *backup*.

As conseqüências do não atendimento as normas para *backup* de dados devem estar explicitas na política de Segurança da Informação, este fator foi apontado por grande parte, quatorze (14) dos respondentes, de acordo com a Figura 5.

No Plano de Continuidade de Negócios o mais importante é que não haja interrupção para os negócios, e caso haja perda dos dados, é essencial saber como recuperá-los. A Figura 6 demonstra o que é necessário considerar sobre *backup* e recuperação de dados em Plano de Continuidade de Negócios, segundo os respondentes.

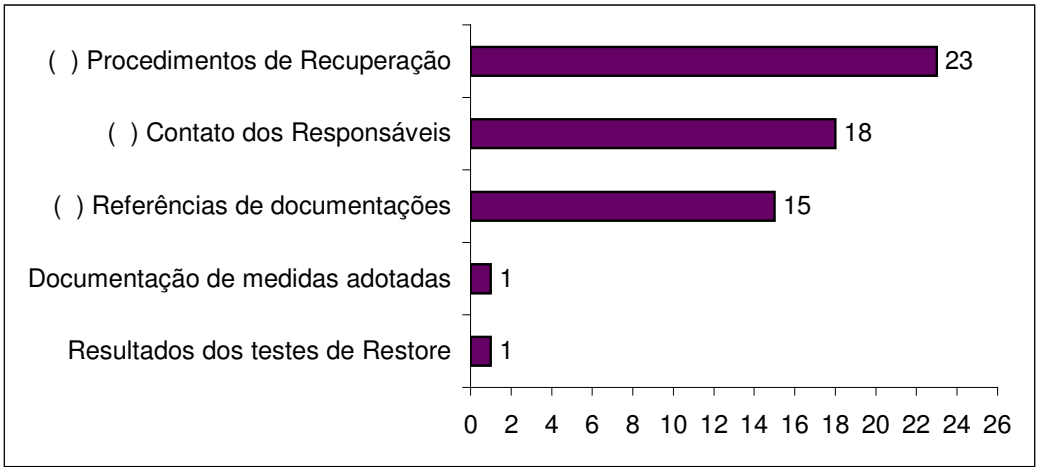

Figura 6 - Considerações para o Plano de Continuidade de Negócios

Segundo a Figura 6, vinte e três (23) dos respondentes concordam que o fator principal para o Plano de Continuidade de Negócios é a definição dos procedimentos para a recuperação dos dados. Porém os procedimentos nem sempre são simples, portanto, é preciso o treinamento constante do pessoal

responsável pela recuperação dos dados, e o contato desse pessoal deve estar contido no Plano de Continuidade de Negócios.

A documentação do *backup*, e os registros de testes de recuperações auxiliarão em recuperações mais rápidas e eficazes por evitar repetir erros, mesmo assim apenas 15 respondentes apontarem este item. Este resultado revela que é preciso maior conscientização sobre a necessidade de documentações.

Outros fatores importantes foram lembrados, como a documentação das medidas adotadas e dos resultados dos testes de recuperação. Estes itens fazem parte dos procedimentos de recuperação, indicados pela grande maioria dos respondentes como principal fator a ser incluído em Plano de Continuidade de Negócios.

Além do estabelecimento de políticas de Segurança da Informação e Plano de Continuidade de Negócios, para o planejamento do *backup* são necessários recursos, como manuais, porém a maioria dos pesquisados (23) respondeu não utilizar nenhum manual específico, segundo a Figura 7.

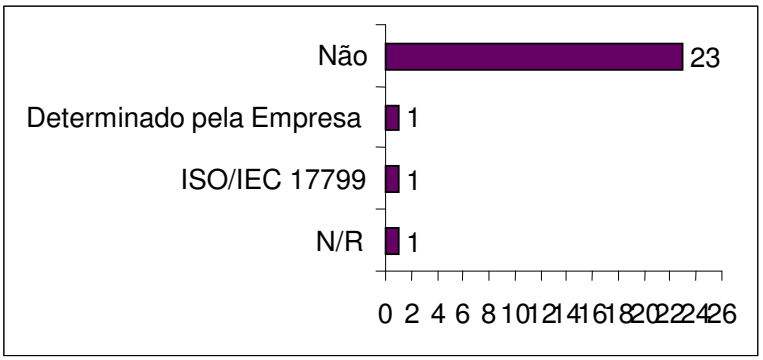

Figura 7- Manual específico para elaboração de plano *backup* de dados

Um dos questionados não respondeu a esta pergunta, pode-se presumir que também não conhece um manual específico para o planejamento de *backup* de dados.

Outro respondente utiliza um manual determinado pela organização onde trabalha.

Identificou-se que pelas respostas serem diferentes e divergentes, não é seguido um padrão para o planejamento de *backup*, mas a norma NBR ISO/IEC 17799, segundo um dos respondentes, pode ser utilizada como um manual no planejamento.

A norma NBR ISO/IEC 17799 possui recomendações para o planejamento e políticas de *backup* e recuperação de dados, porem não é um manual específico para este fim.

Com a falta de manuais específicos para planejamento de *backup* de dados procurou-se saber quais as principais recomendações utilizadas para o planejamento de *backup* de dados.

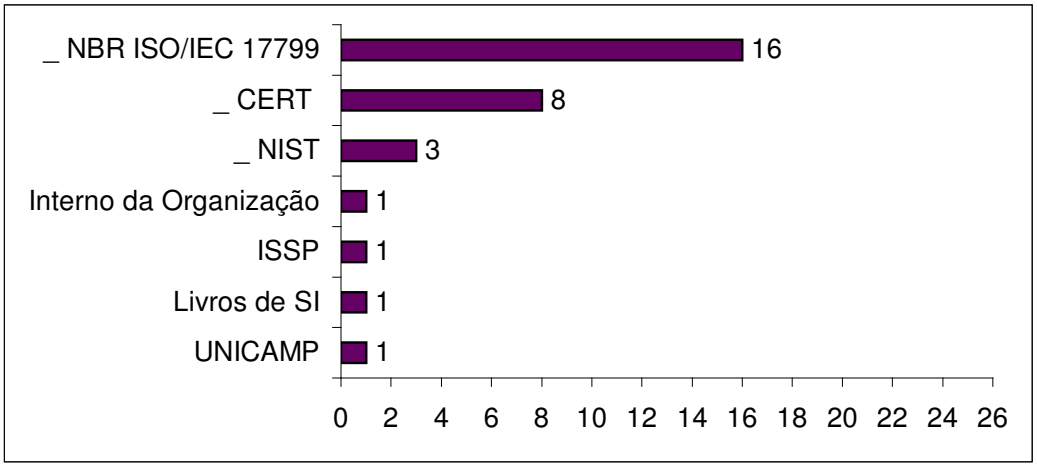

Figura 8 - Normas e/ou recomendações para *backup* de dados

De acordo com a Figura 8, a maioria dos profissionais da área de Segurança da Informação selecionados para esta pesquisa utiliza recomendações, normas e outros tipos de indicações para planejarem o

backup de dados, e dezesseis (16) dos vinte e seis (26) respondentes utilizam a norma NBR ISO/IEC 17799, ou seja, apenas 61%.

Esse percentual é baixo, visto que a maioria dos respondentes trabalha há mais de dois (2) anos na área de Segurança da Informação e tem cursos nesta área, portanto, devem conhecer a norma NBR ISO/IEC 17799, mas não a incluem como recurso para o planejamento do processo de *backup* de dados.

O CERT indicado por oito (8) dos pesquisadores possui recomendações práticas de segurança para administradores de redes, cartilha de segurança para Internet, e outras recomendações e artigos para Segurança da Informação na Internet, e nestes documentos encontram-se algumas indicações para *backup* de dados.

No NIST indicado por três (3) dos respondentes é possível encontrar muita documentação técnica e de governança de Tecnologia da Informação, onde há recomendações para *backup* de dados. Porque a indicação foi feita por apenas três (3) dos respondentes constata-se que é necessário que este *site* seja mais divulgado para que seja mais utilizado.

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. Os respondentes acrescentaram que para o planejamento de *backup* de dados utilizam também normas estabelecidas pela organização onde trabalham, indicações da UNICAMP, outras fornecidas por meio de cursos de certificação para profissionais de Segurança da Informação como, o *Certified Information Systems Security Professional* (CISSP), além das apontadas por livros na área de Segurança da Informação.

Também se procurou saber se existem certificações para o planejamento de *backup* de dados. Os resultados estão mostrados na Figura 9.

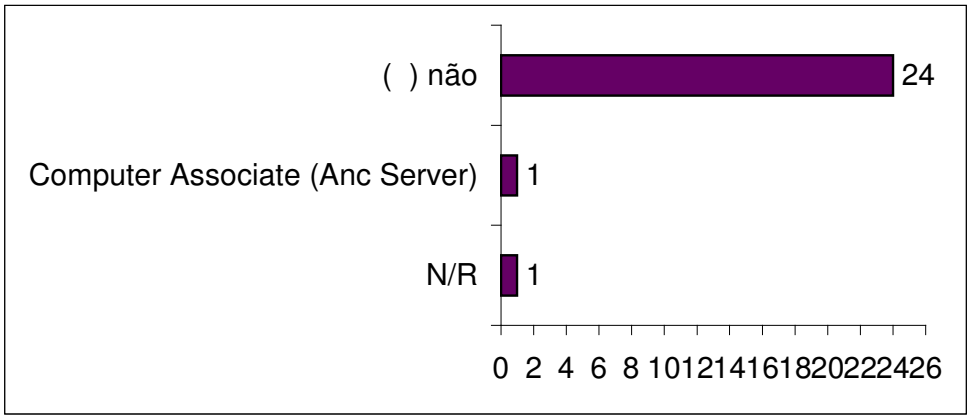

Figura 9 - Certificação em gestão ou planejamento de *backup*

Apenas um pesquisado, segundo a Figura 9, respondeu positivamente esta pergunta, porém depois de investigar sobre a certificação indicada, constatou-se que é especifica de um *software*. De acordo com o conhecimento dos respondentes há falta de certificação para planejamento de *backup* de dados.

Este fator é preocupante, visto que o processo de *backup* envolve muitas variáveis diferentes, tornando-o complexo. É necessário haver treinamentos e certificações específicos para auxiliar no planejamento de *backup* de dados.

C – Tratamento e Classificação dos Dados

Após procurar identificar as etapas e participantes de um plano de *backup* de dados, e quais recursos como manuais, normas e certificações existem para auxiliar o planejamento de *backup* de dados, buscou-se identificar quais tratamentos os dados precisam receber antes de serem "*backup*eados" e

como estes devem ser feitos. Esta parte visa identificar as estratégias para tornar os processos de *backup* e recuperação de dados mais eficazes e rápidos.

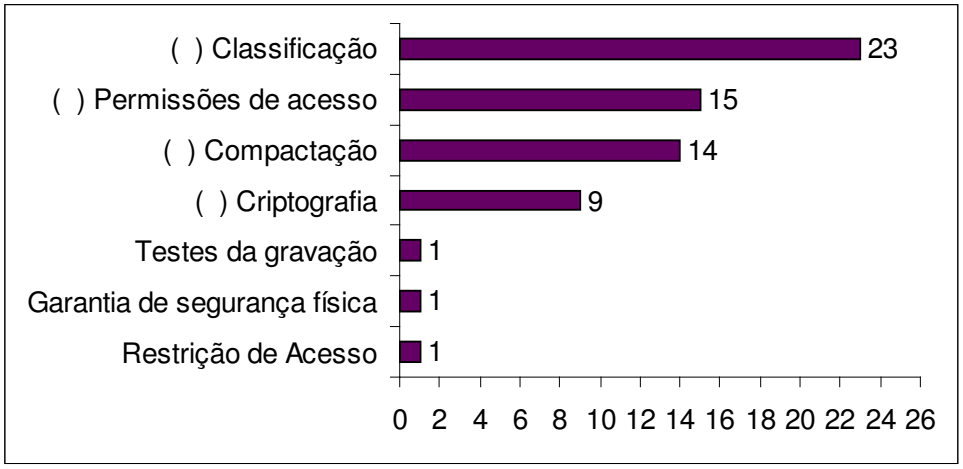

Figura 10 - Tratamentos dos dados antes de serem armazenados

De acordo com a Figura 10, para a grande maioria o principal tratamento que os dados precisam receber antes do *backup* é a classificação e após esta, as permissões de acesso e compactação.

Apesar de a criptografia ser importante, foi um dos itens menos considerados pelos respondentes segundo a Figura 10. Para o entendimento desta escolha, alguns respondentes foram contatados posteriormente, através de uma entrevista informal, para explicarem o motivo de não considerarem a criptografia.

A resposta foi que a criptografia será necessária apenas depois da classificação, quando os dados forem qualificados como confidenciais. Alguns disseram que o atributo de permissões de acesso é suficiente para evitar acesso não autorizado aos dados. Outro respondeu que certas bases de dados são complexas e difíceis de serem acessadas em outro sistema diferente do qual onde foi produzida, e que a criptografia e a compactação dos dados pode

atrapalhar ou impedir a recuperação dos dados na própria base onde os dados foram criados. É preciso que haja mais estudo sobre criptografia para que esta seja mais utilizada e de forma adequada.

A compactação dos dados antes do *backup* também pode ser complexa para algumas bases de dados, no entanto a maioria recomenda a compactação dos dados, para economizar recursos de armazenamento.

A alternativa “outros” foi preenchida por alguns dos respondentes e as estratégias acrescentadas foram: Testes de Gravação, Garantia de segurança física e Restrição de acesso.

Uma estratégia bem lembrada foi a de testar a gravação do *backup*, ou seja, verificar se os dados estão gravados corretamente para então armazena-los.

A garantia de segurança física implica na escolha de mídias e locais de armazenamento. Este item será mais profundamente abordado na fase procedimentos de escolhas de tecnologias.

O item Restrições de acesso indicado por um dos respondentes está ligado ao item Permissões de acesso, por exemplo, se há permissão de acesso ao arquivo para apenas dois usuários, os outros usuários estarão com o acesso restrito.

A classificação é um dos itens mais importantes para o planejamento de *backup* de dados, segundo a maioria dos respondentes. Alguns dos itens necessários para classificar a informação são demonstrados na Figura 11.

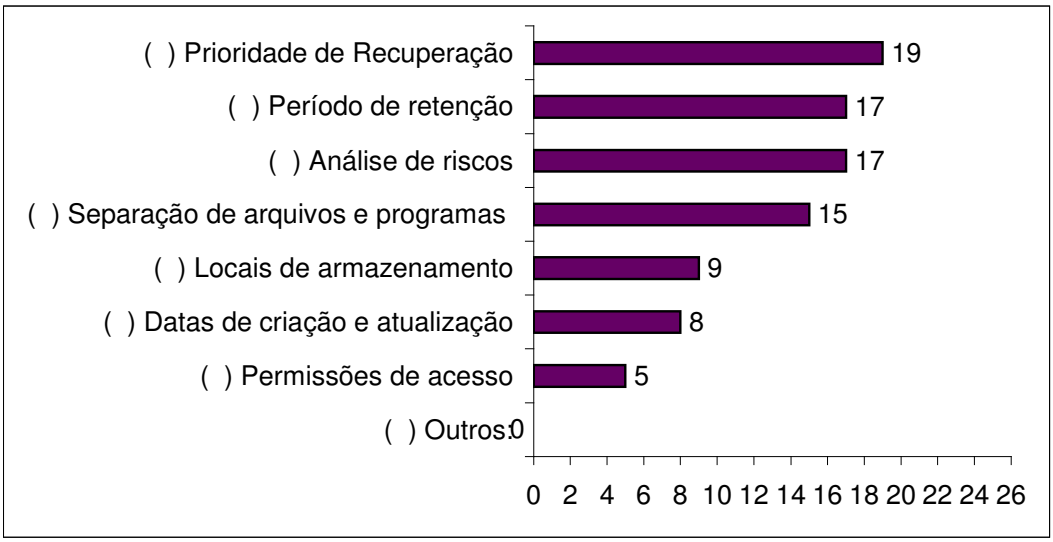

Figura 11 - Necessário para classificar os dados a serem “backapeados”

A maioria dos questionados concorda que para a classificação da informação é preciso determinar a prioridade de recuperação, seguida pela análise de riscos e estabelecimento do período de retenção, de acordo com a Figura 11.

Esperava-se que a análise de riscos fosse apontada por todos os respondentes, pois através dela é possível determinar as prioridades da informação na recuperação e o período de retenção.

A separação de arquivos, indicada por quinze (15) dos respondentes como importante para a classificação dos arquivos, além de facilitar o *backup*, agiliza a recuperação.

Segundo alguns dos respondentes, de acordo com a Figura 11, na classificação da informação também devem ser considerados o local de armazenamento dos dados e as datas de criação e atualização. As datas dos arquivos podem ser muitos importantes em casos judiciais.

Já o item Permissões de acesso, segundo a Figura 11, foi indicado por apenas cinco (5) dos respondentes como item a ser considerado na

classificação dos dados, porém este evita que os dados não sejam acessados por desautorizados.

D – Facilidades de *Backup*, Disponibilidade e Recuperação

Após identificar o que é necessário para os dados antes do *backup*, nesta parte buscou-se saber o que é preciso utilizar como estratégias para tornar o processo de *backup* mais eficiente, diminuindo a janela de *backup* e melhorando o *Recovery Time Objective* e *Recovery Point Objective*.

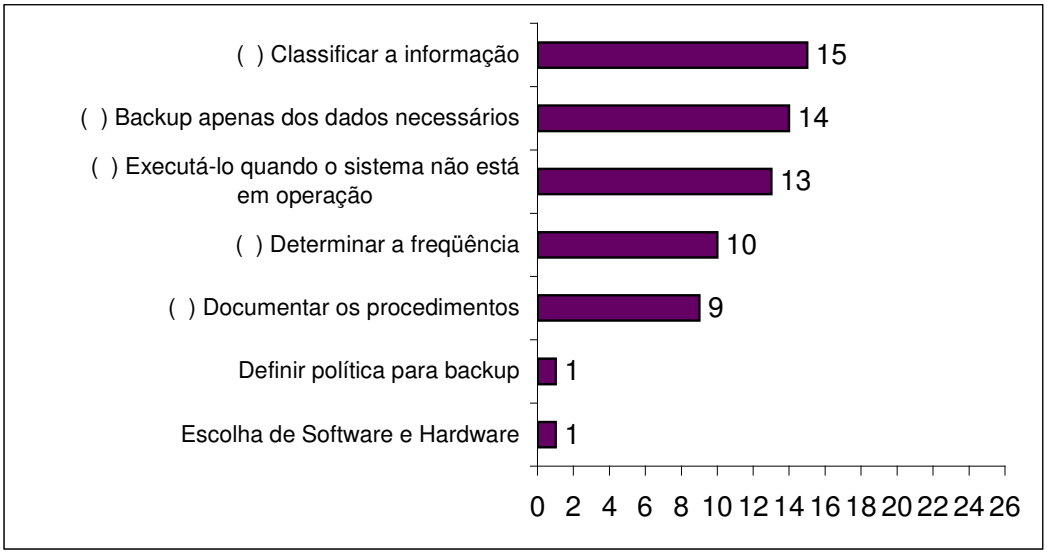

Figura 12 - Estratégias para minimizar o tempo do *backup*

De acordo com a Figura 12, segundo a maioria dos respondentes, é preciso classificar a informação e fazer *backup* apenas dos dados importantes e necessários aos negócios da organização.

Executar o *backup* quando o sistema não está em operação também diminui o tempo da janela de *backup,* segundo metade dos respondentes. Esta opção é válida apenas para alguns sistemas, pois alguns devem funcionar interruptivamente. É interessante ter servidores só para *backup* de dados.

Determinar a freqüência do *backup* e documentar todos os procedimentos para a realização do *backup* são estratégias que devem ser seguidas para diminuir a janela de *backup*, segundo alguns dos respondentes. Além de documentar é necessário que a documentação tenha acesso fácil para a recuperação.

Segundo a Figura 12, alguns dos respondentes indicaram mais estratégias para melhorar o tempo de *backup* como definir política para o *backup* de dados e possuir estratégias para a escolha de *software* e *hardware*.

Depois de conseguir estratégias para se fazer o *backup*, procurou-se saber o que é preciso para ter o *backup* disponível e rápida recuperação.

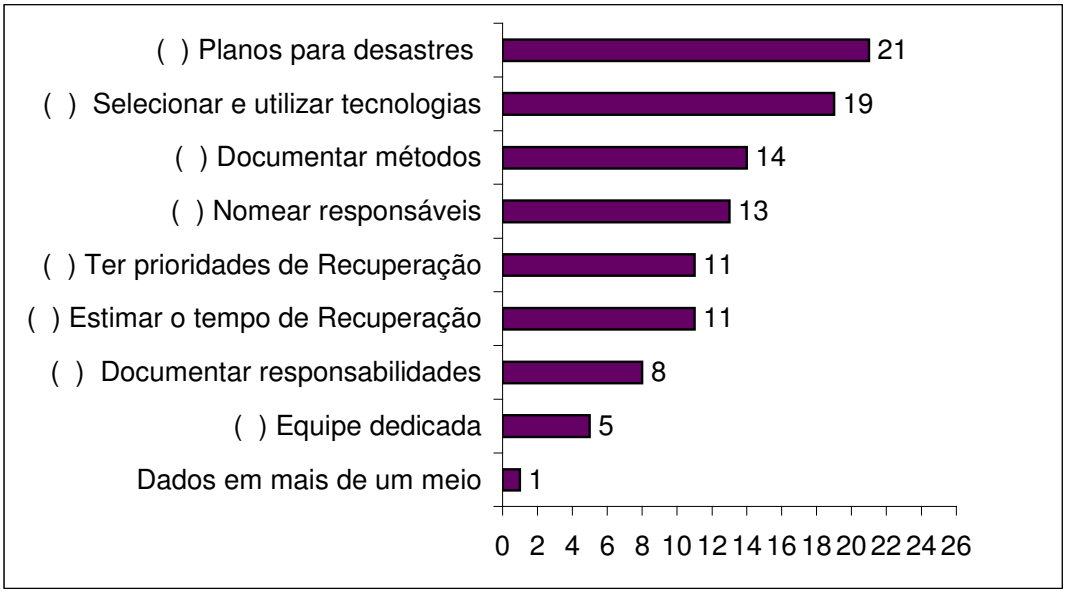

Figura 13 - Estratégias para o *backup* disponível, e rápida recuperação.

Segundo a Figura 13, ter planos para caso de desastres foi um dos itens mais apontados no questionário como estratégias para a recuperação dos dados. Outras estratégias importantes são a seleção e a utilização de tecnologias eficazes para o *backup* e recuperação dos dados. A maioria

também aponta que a documentação dos métodos de *backup* e recuperação de dados, e a nomeação de responsáveis são necessárias para a rápida recuperação dos dados.

De acordo com grande parte dos respondentes, segundo a Figura 13, os itens sobre determinar prioridades, estimar o tempo de recuperação e documentar responsabilidades devem ser considerados para facilitar a recuperação dos dados.

De acordo com a Figura 13, ter uma equipe dedicada apenas para o *backup* e recuperação de dados não é tão importante. A equipe pode realizar outras tarefas além do *backup*. Foi bem lembrado por um dos respondentes que para a disponibilidade é importante ter o *backup* em mais de um meio, ou seja, em disco, fitas, em servidores remotos, etc.

E – Tecnologias para *Backup* de dados

Para a eficácia do processo de *backup* de dados é necessária a aquisição de recursos tecnológicos. Buscou-se nesta parte obter informações sobre o que considerar para conseguir as tecnologias de *hardware*, *software* e mídias para *backup*.

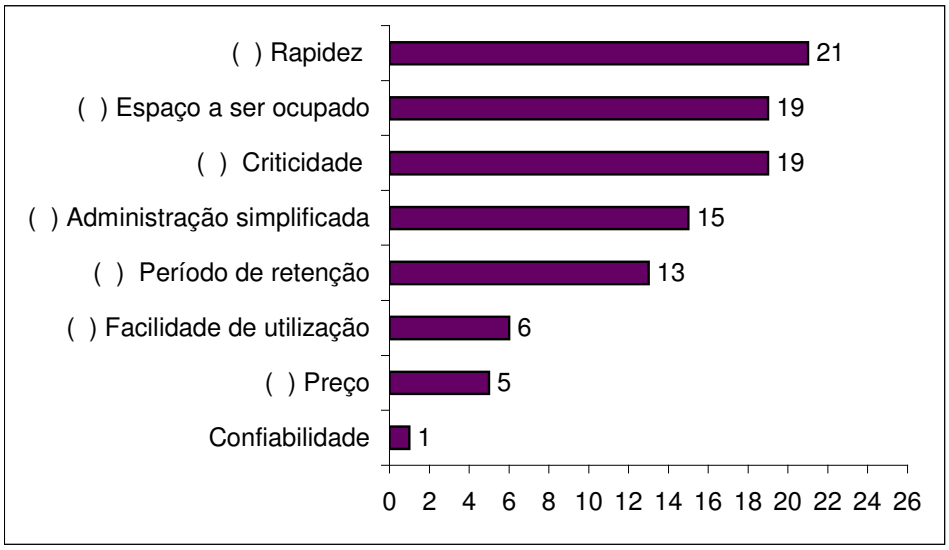

Figura 14 - Necessário para escolher tecnologias de *hardware* e *software*

De acordo com a Figura 14, para se escolher tecnologias de *hardware* e *software* para *backup* de dados, os responsáveis pela Tecnologia da Informação recomendam considerar, em primeiro lugar, a rapidez com que essas ferramentas recuperam os dados. A seguir deve ser ponderada a criticidade e o espaço a ser ocupado pelos dados.

A administração simplificada das tecnologias também deve ser avaliada ao se escolher *software* e *hardware* para *backup* de dados, segundo a maioria dos respondentes. Segundo a metade dos respondentes, o período de retenção dos dados deve influenciar na escolha de tecnologias de *hardware* e *software*.

A facilidade de utilização não foi muito considerada pelos respondentes, pois apenas seis (6) indicaram este item. A utilização das tecnologias normalmente fica por conta dos técnicos de Tecnologia da Informação e estes não foram consultados. A maioria dos analistas concordou que a administração simplificada influenciará na escolha de *software* e *hardware*, ou seja, os analistas parecem mais preocupados com a administração e não a

utilização técnica das tecnologias, porém esta deve influenciar na escolha, pois quanto mais fácil a utilização das tecnologias, mais rapidez poderá se ter por parte dos técnicos.

Em consulta posterior alguns respondentes disseram que o item "facilidade de utilização" já esta implícito em "Administração simplificada".

Segundo a Figura 14, o preço da tecnologia não influencia muito na escolha da mesma segundo a maioria dos profissionais consultados. Este fato indica certa mudança nas concepções do pessoal de Tecnologia da Informação, que está mais preocupada com segurança e sabe que esta custa cara, e merece investimentos. Porém esta parte será avaliada pelo pessoal da área administrativa, que é a que libera os recursos para a compra.

Um dos respondentes, de acordo com a Figura 14, lembrou que a confiabilidade nas Tecnologias também deve influenciar na escolha.

Em relação às mídias de *backup*, antes de adquiri-las, é importante saber a capacidade de armazenamento dos dados e o período de durabilidade, segundo a grande maioria dos respondentes de acordo com a Figura 15.

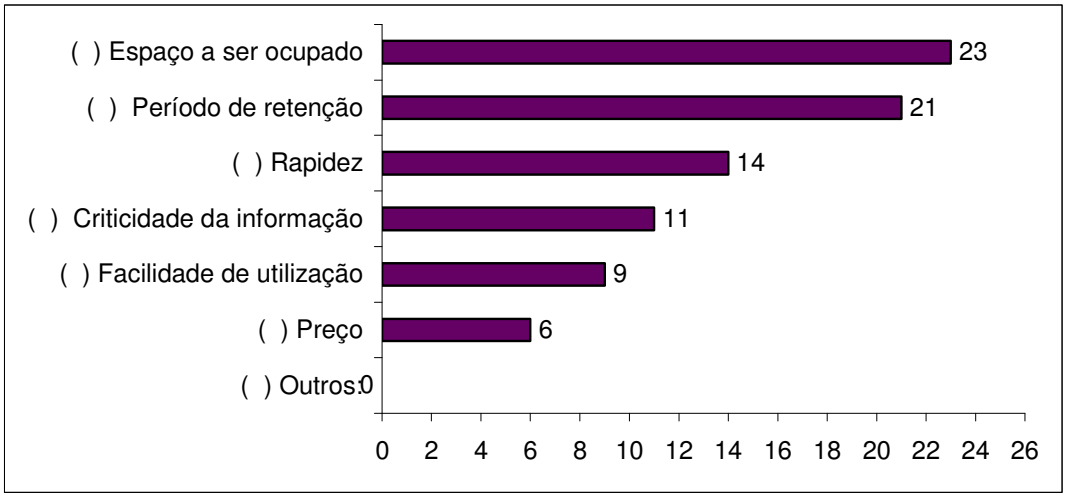

Figura 15 - Necessário para escolher mídias para *backup* de dados

O item rapidez não foi assinalado por todos os que assinalaram este fator ser importante para a aquisição de *hardware* e *software*. Se a mídia não for rápida, o *hardware* e *software* não bastarão para a facilidade da recuperação. É preciso mais atenção para este fato.

O item Facilidade de utilização foi indicado por nove (9) dos respondentes, isto revela que alguns dos questionados não atentaram ainda para este fator que é técnico, mas facilita e agiliza a recuperação.

Como na questão anterior de escolha de *hardware* e *software*, o item Preço também foi pouco indicado como determinante na escolha de mídias. De acordo com a Figura 15, segundo alguns respondentes, em consulta informal, alegaram que a Segurança da Informação precisa de investimentos, e que quem negocia os preços é o pessoal da área administrativa.

F – *Backup* em Site Remoto

Já com os dados "*backup*eados" com as tecnologias apropriadas, é preciso mais de uma geração de *backup* e que esta seja mantida a uma distância, que não permita que um desastre no *backup* local atinja também o *backup* remoto. Buscou-se nesta parte saber quando é necessário e como contratar o *site* de *backup* remoto.

De acordo com a Figura 16, os participantes da pesquisa consideraram mais importante ter o *backup* remoto para atendimento a padrões de segurança. Quando os dados exigem consultas contínuas, e/ou quando precisam de um longo período de retenção, também é importante que haja *backup* remoto segundo grande parte dos respondentes.

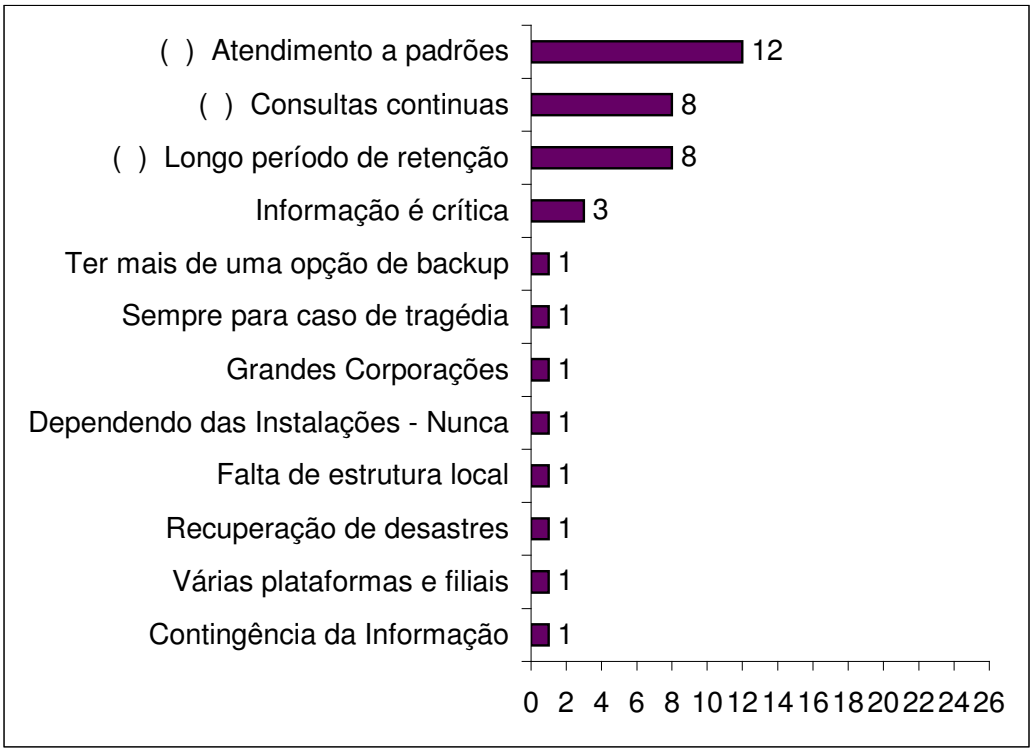

Figura 16 - *Backup* remoto

Segundo a Figura 16, foram indicados pelos respondentes, outros fatores que requerem o *backup* remoto. É preciso considerar o *backup* remoto para a Informação crítica, e para:

- Ter mais de uma opção de *backup*
- Várias plataformas e filiais
- Recuperação de desastres
- Recuperação em caso de tragédia
- Falta de estrutura local
- Grandes Corporações
- Contingência da Informação
- E dependendo das Instalações - Nunca

Dentre estes o mais apontado foi: considerar o *backup* quando a informação é crítica. Cada respondente vive uma realidade diferente em seu ambiente de trabalho e vai optar pelo *backup* remoto dependendo da criticidade da informação. O *backup* remoto vai ser de acordo com os dados classificados, quanto mais crítica a informação mais níveis de *backup* serão necessários.

Ainda houve respondente que acredita não ser preciso o *backup* remoto, por estarem os dados bem protegidos localmente. Desastres como o atentado às torres gêmeas, ou terremotos realmente são difíceis de acontecerem, mas pequenos incêndios ou erros humanos são comuns. É necessária conscientização de que na área de Segurança da Informação nunca existe proteção total.

Reconhecida a necessidade do *backup* remoto, é preciso saber onde será esse *backup*, na contratação de um site de *backup* remoto, a Figura 17 mostra algumas opiniões sobre o que considerar.

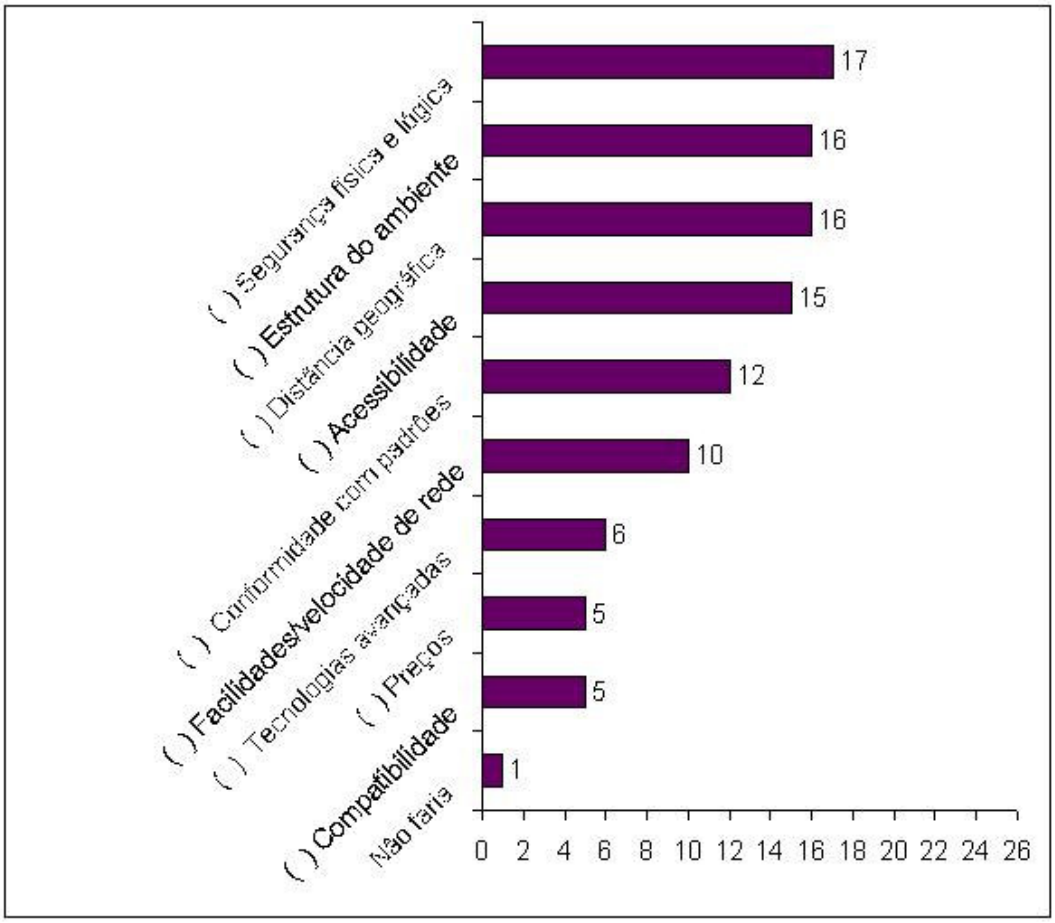

Figura 17 - Considerações para contrato de *backup* remoto

Para a contratação de *backup* remoto deve-se considerar primeiramente a estrutura física e lógica onde ficarão os dados, a estrutura do ambiente, a distância geográfica, a acessibilidade e rapidez na recuperação dos dados, segundo a Figura 17.

A conformidade com padrões de segurança no site contratado também precisa ser considerada para o *backup* remoto, segundo grande parte dos respondentes. Facilidades e velocidades de rede, assim como tecnologias avançadas, facilitam na recuperação dos dados, portanto, estes itens devem ser levados em conta para a contratação de um site de *backup* remoto.

A compatibilidade de *software* não foi tão considerada quanto os outros itens, de acordo com a Figura 17. Segundo alguns dos respondentes, em consulta posterior, este item está implícito nos outros, pois não é possível contratar o site de *backup* remoto se este não comporta os tipos de dados a serem *backup*eados.

O preço, apesar de ser importante, é tido como preocupação da área administrativa segundo alguns respondentes em entrevista informal.

G – Documentação

Para a eficaz recuperação dos dados é importante a documentação de como, quando e do que foi feito o *backup* e principalmente de como deve ser feita a recuperação.

Buscou-se nesta fase saber o que é preciso para criar e manter a documentação do *backup* de dados.

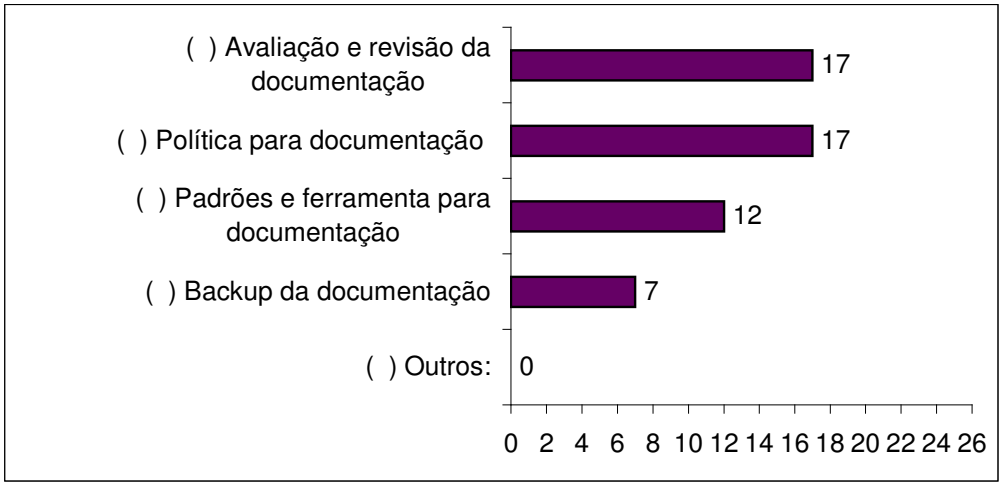

Figura 18 - Estratégias para documentação de *backup* e recuperação

Segundo a Figura 18, a maioria dos analistas de Segurança da Informação revela que é preciso uma política com normas para a documentação, e que é preciso a avaliação e revisão da documentação.

Menos que a metade indicou a necessidade de ferramentas para documentação, porém elas podem facilitar no estabelecimento de padrões para a criação e manutenção da documentação. Esta também pode ser considerada parte técnica.

De acordo com a Figura 18, o *backup* da documentação é pouco utilizado, porém esta documentação é feita de informações importantes, portanto também precisa de cópias. Falta conscientização para este fato.

H – Testes e Avaliações do Plano de *backup* de dados

Na primeira parte procurou-se saber como deve ser o plano e quais grupos devem participar da elaboração do mesmo, além de ter uma visão geral das mais importantes partes de um plano de *backup*, como classificação e documentação para o *backup* e recuperação de dados. Nesta última parte buscou-se quem revisa este plano e de quanto em quanto tempo.

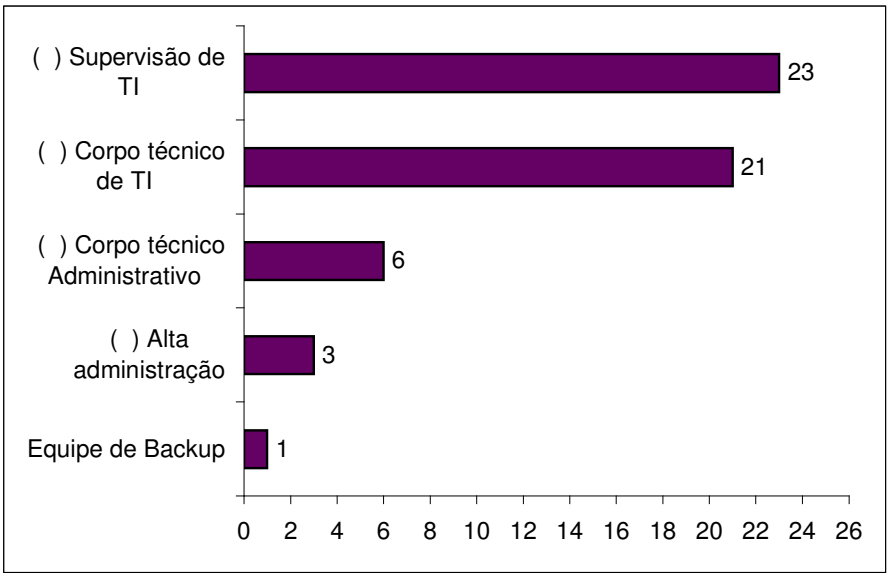

Figura 19 - Grupos que devem testar e avaliar o plano de *backup*

Segundo a Figura 19, a maioria dos respondentes concorda que os profissionais da área de Tecnologia da Informação, tanto a supervisão quanto à parte técnica, devem ser os responsáveis pela revisão do plano de *backup* de dados.

Após o plano feito, é preciso testes para avaliar, que normalmente são técnicos. Já que a informação foi classificada, separada e recebeu os tratamentos necessários antes do *backup*, os testes são para saber se os dados estão devidamente armazenados e de fácil e rápida recuperação apenas pelos autorizados, portanto, constata-se não há necessidade de participação do pessoal da área administrativa.

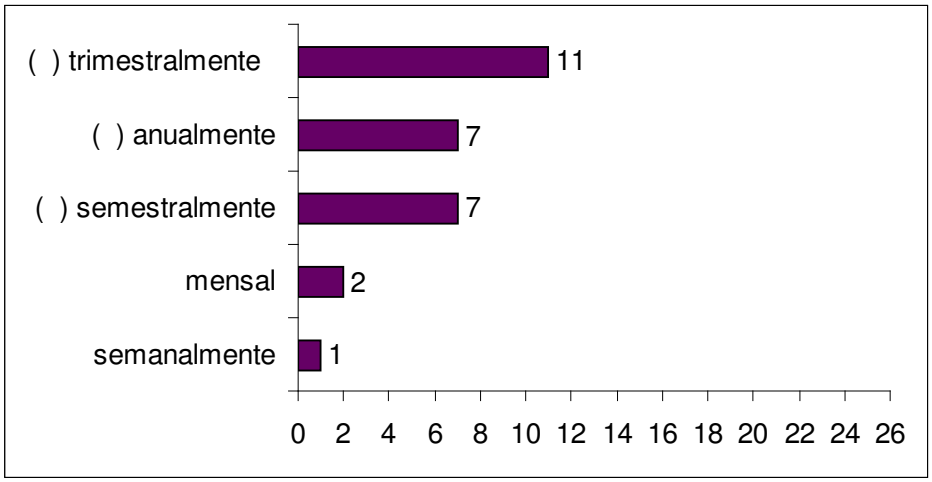

Figura 20 - Periodicidade para testar e avaliar os planos de *backup*

De acordo com a Figura 20, não houve nenhuma alternativa desta questão marcada por 50% dos respondentes Isto leva a conclusão de que a periodicidade dos testes dependerá dos dados, na medida em que estes aumentam de volume, ou criticidade.

4.3 PROPOSTA: ETAPAS PARA O PLANEJAMENTO DE BACKUP DE DADOS

Fundamentação

Esta proposta foi formulada através dos conhecimentos adquiridos pela revisão da literatura, da consolidação das respostas ao questionário e de entrevistas informais com alguns dos profissionais de Tecnologia da Informação participantes desta pesquisa.

A proposta é que haja um planejamento para o *backup* de dados com etapas bem definidas e com o envolvimento de todas as equipes da organização, desde técnicos à alta administração.

O *backup* de dados exige recursos tais como financeiros, de pessoal, de tempo, de equipamentos, de *software*, dentre outros. É preciso a

conscientização da área administrativa que libera os recursos sobre a importância do *backup* de dados.

Primeira Etapa: A conscientização da necessidade do *backup* de dados, que pode partir tanto da área de Tecnologia da Informação quanto da área administrativa da organização.

É necessário justificar o planejamento do *backup* de dados para então conseguir apoio da organização. As principais justificativas são:

- Proteção dos dados para a continuidade dos negócios, prevenção contra desastres e recuperação segura dos dados, para que esses estejam integrais e disponíveis.
- Atendimento a padrões de segurança e a leis e regulamentos nacionais e internacionais.
- Maior confiabilidade e crédito por parte dos clientes.

Sabendo da importância do planejamento do *backup* de dados, o próximo passo é formar equipes para serem responsáveis pelo planejamento.

Segunda Etapa: A definição do(s) responsável (is) pelo planejamento de *backup* de dados.

Sugere-se que os responsáveis sejam:

- Supervisão de Tecnologia da Informação
- Alta Administração, que deve liberar os recursos.

  Observação: Essas equipes deverão contar com o apoio das suas áreas técnicas.

Terceira Etapa: A Disponibilização de recursos para que essas equipes possam planejar o *backup*.

- Treinamentos na área de Segurança da Informação.
- Adoção de normas de Segurança da Informação, como a norma NBR ISO/IEC 17799
- Adoção de Recomendações:
    - CERT
    - NIST
    - Livros de Segurança da Informação
    - Materiais de cursos, como do Certified Information Systems Security Professional
    - Materiais internos da organização, elaborados a partir da bagagem de experiência de profissionais de Segurança da Informação
    - Análise e orientações de especialistas e as opiniões de consultores.

Quarta Etapa: A Determinação das ações a serem planejadas.

O plano de *backup* de dados deve contar, no mínimo, com os seguintes procedimentos:

- Classificação da informação

  Análise de riscos das informações, considerando, no mínimo:
    - Criticidade da informação para os negócios
    - Prioridade de recuperação
    - Período de retenção

- Datas de criação, atualização e exclusão
- Permissões e restrições de acesso
- Re-classificação das informações, lembrando que essas podem deixar de serem críticas para a organização.

Todos os procedimentos seguintes devem considerar a classificação das informações:

- Armazenamento

  Utilizar estratégias de Gerenciamento do Ciclo de Vida das Informações. Considerando no mínimo:

  - Fazer o *backup* apenas dos dados necessários
  - Separação de arquivos, de programas e aplicações
  - Armazenar dados com nomes padronizados
  - Manter os dados armazenados apenas pelo período necessário.

- Documentação do *backup* e recuperação dos dados:

  Considerar no mínimo:

  - Documentação de todos os processo de *backup* e Recuperação de dados
  - Utilização de Padrões e ferramenta de software adequada para documentação
  - Avaliação e revisão da documentação de *backup* e recuperação
  - *Backup* da documentação

- Escolha de hardware, software e mídias.

  Considerar no mínimo:

  - Velocidade para o *backup* e recuperação dos dados.
  - Espaço a ser ocupado pelos dados
  - Administração e utilização simplificada
  - Período de retenção dos dados
  - Confiabilidade

- Definição do local dos dados a serem armazenados

  Considerar no mínimo:

  - Garantia de seguranças física e lógica
  - Estrutura do ambiente, como controle de temperatura, umidade, prevenção contra incêndio, controles de energia elétrica, etc.

- Considerar o *backup* remoto, principalmente quando:

  - A Informação é crítica para os negócios
  - A informação precisa de contingência
  - Os dados precisam de um longo período de retenção
  - O dados precisam ser consultados continuamente
  - Para atendimento a padrões de segurança

- Contratação de site de *backup* remoto

  Considerar no mínimo:

  - Segurança física e lógica, que deve ser igual ou melhor que a do *backup* local

- Distância geográfica, e a probabilidade de acontecer um desastre que atinja o *backup* local e remoto
- Acessibilidade, ou tempo necessário para se recuperar o *backup*
- Conformidade da empresa contratada com padrões de segurança

- Transmissão dos dados para *Backup* Remoto

  Considerar no mínimo:

  - Facilidades de velocidade e segurança de conexões de rede e de Internet
  - Criptografia para os dados sigilosos

- Transportes de mídias

  Considerar no mínimo:

  - Confiança e comprometimento de todo o pessoal que manipula as mídias.
  - Criptografia para os dados sigilosos.

- Agendamento do *backup*

  Considerar no mínimo:

  - Freqüência do *backup* de acordo com a criticidade, atualizações e outros atributos das informações
  - Tecnologias que permitam executar o *backup* quando o sistema está em operação

- Período de retenção das mídias e guarda de mídias

  Considerar no mínimo:

  - Instruções de guarda e tempo de vida útil das mídias
  - Local de armazenamento das mídias

- Testes de recuperação e *backup*

  Considerar no mínimo:

  - Resultados dos testes de *backup* e recuperação
  - Documentação de medidas adotadas
  - Estimativa do tempo de recuperação, incluindo o tempo para identificar o problema e a solução, de acordo com tipo o armazenamento.

- Revisão do plano

  Considerar no mínimo:

  - Auditoria do plano visando maior segurança e rapidez através de automação dos processos de *backup* e recuperação dos dados.

- Definição de responsabilidades

  Considerar no mínimo:

  - Uma equipe, ou pelo menos um responsável para todas as etapas acima, com treinamento constante para esse(s) responsável(is).

- Política de Segurança da Informação e Plano de Continuidade de Negócios
    - Todos os procedimentos acima devem estar contidos, ou terem referências na Política de Segurança e no Plano de Continuidade de Negócios da organização.

Todo o planejamento e recursos destinados ao *backup* devem estar de acordo com o valor da informação.

Esta proposta contém recomendações revisadas na literatura e de profissionais da área de Tecnologia da Informação, estudadas anteriormente neste trabalho, porém está colocada de maneira organizada e resumida.

5 CONCLUSÃO

O risco de perda, inacessibilidade ou acesso não autorizado aos dados mantidos nos computadores devido às ameaças, aumenta a preocupação em se manter a disponibilidade, confidencialidade e integridade das informações para a continuidade dos negócios. Para segurança dos dados, além de outras medidas, é necessário que as estratégias para *backup* de dados sejam aplicadas, testadas e analisadas continuamente para serem válidas, mesmo com mudanças no ambiente de negócios.

Através deste trabalho, que evidencia as principais recomendações para *backup* de dados, é possível facilitar o planejamento, segundo as melhores práticas, tendo em mente que cada organização terá estratégias de *backup* de dados personalizadas de acordo com as características de cada negócio.

Na Revisão da Literatura, observou-se a importância de estratégias de *backup* de dados para políticas de Segurança da Informação e para o Plano de Continuidade de Negócios, procurando garantir a preservação da Segurança da Informação e continuidade dos negócios. Também com a análise e entendimento da literatura foi possível a formulação de maior parte do questionário destinado aos profissionais da área de Segurança da Informação.

Com a aplicação do questionário verificou-se que nem todas as estratégias indicadas pela literatura são aplicadas e recomendadas pelos profissionais de Segurança da Informação. Apesar de todos os respondentes serem responsáveis por informações críticas que precisam de segurança, as opiniões sobre *backup* de dados divergem bastante. Esse fato pode ser explicado pela falta de guias e/ou cursos específicos para o planejamento de *backup* de dados.

No questionário foi dada a oportunidade para que os respondentes manifestassem alternativas não encontradas na pesquisa bibliográfica e até inéditas. Mesmo sendo poucas as recomendações advindas dos questionados a base de conhecimento sobre *backup* de dados aumentou com relação ao descrito na literatura pesquisada.

Foi dado um enfoque técnico no levantamento dos procedimentos de *backup* de dados para saber e destacar o que é mais relevante no seu planejamento. Através da pesquisa de campo foi constatada a importância dos conhecimentos técnicos para o planejamento de alguns procedimentos como o de segurança no local de guarda do *backup*.

Foi apontada a importância da participação da área administrativa no planejamento de *backup* de dados para a liberação de recursos para os processos de *backup* de dados, e para a conscientização sobre a importância da Segurança da Informação.

O problema de pesquisa foi então solucionado, pois a comparação da literatura com a experiência de profissionais da área de Segurança da Informação permitiram a identificação das principais variáveis e estratégias para o planejamento de *backup* de dados, do ponto de vista de gestão de Segurança da Informação.

O objetivo inicial do trabalho foi alcançado, isto é, pôde-se elaborar uma proposta com etapas para planejamento de *backup* de dados, através da reunião das principais estratégias sobre *backup* de dados baseada na literatura existente e na pesquisa de campo.

Um dos benefícios deste trabalho foi mostrar que o processo de *backup* de dados deve ser estratégico, pois engloba toda a organização, desde a parte

técnica, que deve conhecer o funcionamento das tecnologias, até a parte administrativa, que deve, além de liberar os recursos, auxiliar na classificação das informações e em outros procedimentos necessários ao plano de *backup* de dados.

Este trabalho foi além dos objetivos propostos, pois salientou a divergência de opiniões entre responsáveis pela Tecnologia da Informação, bem como a falta de recursos, principalmente manuais e cursos específicos sobre *backup* de dados, para auxiliar no planejamento de *backup* de dados.

A proposta final é um conjunto formado pelas estratégias da literatura, pelas respostas ao questionário, e por algumas consultas informais com os respondentes da pesquisa, apresentada de forma organizada para facilitar seu entendimento e aplicação.

Como um subproduto deste trabalho, houve interesse de profissionais de Segurança da Informação em utilizar as estratégias, aqui propostas, como um guia prático para o planejamento de *backup* de dados em suas organizações.

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.

Constatou-se que mais investigações devem ser elaboradas a fim de levar aos profissionais de Segurança da Informação melhores esclarecimentos sobre a contribuição destas estratégias para *backup* de dados.

Este trabalho serve como base para outras pesquisas, por exemplo: cada recomendação para *backup* de dados pode ser explicada em artigos

separados e específicos, pois merecem muita atenção e podem ser avaliadas aplicações das estratégias para diferentes tipos de organizações e negócios.

Outros assuntos, a serem explorados para o planejamento de *backup* de dados, podem ser: como classificar a informação, como definir o quanto investir de acordo com o custo de disponibilidade e indisponibilidade, como calcular o retorno do investimento em *backup* de dados, entre outros.

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.

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

_____. **Speed up your *Backups* by pruning your data**. 2006b. Disponível em: http://searchstorage.techtarget.com/tip/1,289483,sid5_gci1164361,00.html. Acesso em 06 set. 2006, 22:26:25.

DAFT, R.L. **Administração. Tradução,** 6. ed. São Paulo: Thomson, 2005.

DORION, P. **Best practices: Optimizing your *Backups***. 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.

EGAN, M. E. **Seis Desafios Significativos para a Segurança da Informação**. 2005. Disponível em: https://www-secure.symantec.com/region/br/enterprisesecurity/content/expert/BR_4779.html .Acesso em: 27 mai. 2007, 17:45:50.

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, 22:30hs

GHERMAN, M. **Controles internos: buscando a solução adequada - Parte I.** 2005. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=445&pagenumber=0&idiom=0. Acesso em: 29 jun. 2005, 22:30:20.

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.

IT WEB. **Pequenas empresas tendem a deixar dados vulneráveis**, 2006. Disponível em: http://www.itweb.com.br/index.php?option=com_noticia&id=20411&section=14. Acesso em 21 jan. 2007, 21:30:00.

KIRK J. **Gerentes de tecnologia são displicentes com prática de *backup***, 2006. Disponível em: http://idgnow.uol.com.br/computacao_corporativa/2006/02/16/idgnoticia.2006-02-16.4799349716/IDGNoticia_view. Acesso em 14 jan. 2007, 20:45:00.

LAKATOS, E. M.; MARCONI, M. A. **Técnicas de Pesquisa**. São Paulo: Atlas S.A., 1999.

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

PRADO, L. **Quatro Passos no Gerenciamento de Riscos,** 2002**.** Disponível em: http://www.securenet.com.br/artigo.php?artigo=114. Acesso em 22 ago. 2005, 20:20:30.

SÊMOLA, M. **Gestão da Segurança da Informação: Uma Visão Executiva da Segurança da Informação**. Rio de Janeiro: Elsevier, 2003.

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.

VERGARA, S.C. **Projetos e Relatórios de Pesquisa em Administração**. São Paulo: Atlas, 2000.

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.

ANEXO A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado para participar, como voluntário, em uma pesquisa. Após ser esclarecido(a) sobre as informações a seguir, no caso de aceitar fazer parte do estudo, assine ao final deste documento, elaborado em duas vias de um só teor. Uma delas é sua e a outra é do pesquisador responsável. Em caso de recusa você não será penalizado (a) de forma alguma.

INFORMAÇÕES SOBRE A PESQUISA:

Título do Projeto: **Estratégias de Planejamento de *Backup* de Dados**
Pesquisadora Responsável: Eliana Márcia Moraes
E-mail: eliana@unitau.br
Telefone para contato (inclusive ligações a cobrar): (0XX12) 9131-8002

Esta pesquisa tem, como objetivo, colher subsídios para compor o conhecimento da atualidade de Gestão de *Backup* de Dados, visando auxiliar os profissionais da área de Segurança da Informação no Planejamento de *Backup* de Dados.
Os respondentes são os responsáveis pela Segurança da Informação, com mais de um ano de trabalho em organizações que possuem dados críticos, que precisam ser mantidos por, no mínimo, dois anos.
Garante-se que não há riscos de qualquer natureza para os participantes desta pesquisa.
Os respondentes são livres para recusarem-se a participar, retirarem seu consentimento ou interromper a participação a qualquer momento. A participação é voluntária e a recusa em participar não irá acarretar qualquer penalidade.
As respostas serão consideradas confidenciais, com finalidade estritamente acadêmica, e utilizadas apenas para fins de pesquisa. Assim, não serão, sob qualquer hipótese, repassados a outras pessoas ou instituições, ou utilizadas para outros fins.
Os resultados consolidados da pesquisa serão divulgados posteriormente, especialmente aos colaboradores, mas isso será feito sem apontar as respostas específicas de qualquer respondente.
Estas respostas obtidas serão analisadas e consolidadas em um relatório, identificando o que é utilizado e indicado, pelos profissionais da área de Segurança da

Informação, como principais estratégias para gestão e planejamento de *Backup* de Dados.

• **Instruções para preenchimento do questionário:**

O questionário é dividido em duas partes: Definição do perfil de quem está respondendo o questionário e Colaboração para o entendimento da atualidade do assunto *Backup* de Dados. entre perguntas fechadas e abertas.

O tempo médio de preenchimento das 25 perguntas é de 40 a 60 minutos.

Se por alguma razão (confidencialidade, informação incompleta ou quaisquer outras) uma questão não puder ser respondida, esta poderá ser ignorada. Apenas solicita-se que não se deixe de responder às demais.

Quaisquer informações adicionais podem ser enviadas em folhas avulsas anexas ao questionário.

Ressalta-se que isso não é um teste, onde deveriam ser dadas as “respostas exatas”, mas sim um instrumento de coleta de dados.

Para esclarecimento de eventuais dúvidas, contate a pesquisadora responsável.

Nome e Assinatura da pesquisadora: Eliana Márcia Moraes _____

CONSENTIMENTO DA PARTICIPAÇÃO DA PESSOA COMO SUJEITO

Eu, _____, RG_____, abaixo assinado, concordo em participar do estudo “Estratégias de *Backup* de Dados”, como sujeito. Fui devidamente informado e esclarecido pela pesquisadora Eliana Márcia Moraes sobre a pesquisa, os procedimentos nela envolvidos, assim como os possíveis riscos e benefícios decorrentes de minha participação. Foi-me garantido que posso retirar meu consentimento a qualquer momento, sem que isto leve a qualquer penalidade.

Local e data _____ ____/____/_____

Nome: _____

Assinatura: _____

ANEXO B - QUESTIONÁRIO

QUESTIONÁRIO DE PESQUISA SOBRE ESTRATÉGIAS DE PLANEJAMENTO DE *BACKUP* DE DADOS

PARTE 1: DEFINIÇÃO DO PERFIL DE QUEM ESTÁ RESPONDENDO O QUESTIONÁRIO

Nome: _____

1- Você é responsável pela Segurança da Informação onde trabalha?

( ) Diretamente

( ) Indiretamente (através de consultoria terceirizada)

2- **Há quanto tempo você trabalha na área de Segurança da Informação?**

( ) 1 ano ( ) 2 anos ( ) mais de 2 anos

3- **Você fez/faz cursos na área de Segurança da Informação?**

( ) sim ( ) não

4- **Como você se mantém atualizado na área de Segurança da Informação?**

( ) cursos ( ) palestras ( ) revistas ( ) internet

( ) outros: _____

_____

_____

_____

5- **A(s) Empresa(s), onde você trabalha, possui dados críticos, que precisam ser mantidos por dois anos ou mais?**

( ) sim ( ) não

PARTE 2: COLABORAÇÃO PARA O ENTENDIMENTO DA ATUALIDADE DO ASSUNTO *BACKUP* DE DADOS

Em todas as questões você pode assinalar várias respostas e, ainda, acrescentar outras considerações que julgar importante.

A – PLANO DE *BACKUP* DE DADOS

1- O que você considera como principais razões para se ter um Plano de *Backup* de Dados?

( ) Conformidade com leis e regulamentos nacionais

( ) Conformidade com leis e regulamentos internacionais

( ) Conformidade com padrões de segurança, mesmo que não obrigatórios

( ) Confiabilidade e crédito de clientes

( ) Concorrência

( ) Proteção dos Dados

( ) Outros: _____

_____

_____

_____

_____

2- **Qual(is) grupo(s) deve(m) participar do desenvolvimento do Plano de *Backup* de Dados?**

( ) Alta Administração

( ) Supervisão de TI

( ) Corpo técnico de TI

( ) Corpo técnico Administrativo

( ) Outros: _____

_____

_____

3- **Classifique de 0 (nenhuma) a 3 (muita), a importância de cada um dos itens e, ao final, acrescente o que falta para um Plano de *Backup* de Dados.**

( ) Definição de responsabilidades

( ) Procedimentos para a Documentação dos métodos e recursos utilizados para o *backup* de dados

( ) Procedimentos para classificação da informação

( ) Procedimentos para se determinar o período de retenção das informações

( ) Procedimentos de nomeação de arquivos

( ) Procedimentos de como agendar o *backup*

( ) Procedimentos de armazenamento

( ) Procedimentos de escolha de *software*

( ) Procedimentos de escolha de *hardware*

( ) Procedimentos de escolha das mídias

( ) Procedimentos para transportes e guarda de mídias

( ) Procedimentos para se determinar o período de retenção das mídias

( ) Procedimentos para definir o local dos dados a serem armazenados

( ) Procedimentos para transmissão dos dados para *Backup* Remoto

( ) Periodicidade da revisão do plano

( ) Outros: _____

_____

_____

_____

_____

4- **Quem faz o que, em um Plano de *Backup* de Dados? Preencha as lacunas com números, de acordo com as seguintes definições:**

1 - Alta administração
2 - Supervisão de TI
3 - Corpo técnico de TI
4 - Corpo técnico Administrativo
( ) Outros:
5 - _____
6 - _____
7 - _____

Obs.: Cada lacuna poderá ser preenchida com mais de um, ou com todos os números.

( ) Definição de responsabilidades

( ) Procedimentos para a Documentação dos métodos e recursos utilizados para o *backup* de dados

( ) Procedimentos para classificação da informação

( ) Procedimentos para se determinar o período de retenção das informações

( ) Procedimentos de nomeação de arquivos

( ) Procedimentos de como agendar o *backup*

( ) Procedimentos de armazenamento

( ) Procedimentos de escolha de *software*

( ) Procedimentos de escolha de *hardware*

( ) Procedimentos de escolha das mídias

( ) Procedimentos para transportes e guarda de mídias

( ) Procedimentos para se determinar o período de retenção das mídias

( ) Procedimentos para definir o local dos dados a serem armazenados

( ) Procedimentos para transmissão dos dados para *Backup* Remoto

( ) Periodicidade da revisão do plano

( ) _____

( ) _____

( ) _____

B – POLÍTICAS, RECOMENDAÇÕES E CERTIFICAÇÕES

5- **Na Política de Segurança da Informação o que é necessário considerar sobre *Backup* de Dados?**

( ) Responsabilidades gerais de *backup* de dados

( ) Responsabilidades gerais de Recuperação de dados

( ) Obrigações para documentação de processos e recursos para *Backup* de Dados

( ) Referencias de documentações para apoiar os procedimentos sobre *Backup* de Dados.

( ) Conseqüências do não atendimento às normas sobre *backup* de dados

( ) Outros: _____

_____

_____

_____

_____

6- **No Plano de Continuidade de Negócios o que é necessário considerar sobre *Backup* de Dados?**

( ) Procedimentos de Recuperação de dados

( ) Contato dos Responsáveis pela Recuperação e *Backup* de Dados

( ) Referências de documentações dos procedimentos de Recuperação e *Backup* de Dados

( ) Outros: _____

_____

_____

_____

_____

7- **Você usa algum manual específico para elaborar um Plano *Backup* de Dados? Se sim, qual ou quais?**

( ) sim, _____

_____

( ) não

8- **Quais as normas e/ou recomendações que contém 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: _____

_____

_____

_____

_____

9- **Você conhece alguma certificação em Gestão ou Planejamento de *Backup* de Dados? Se sim, qual ou quais?**

( ) sim, _____

_____

( ) não

C – TRATAMENTO E CLASSIFICAÇÃO DOS DADOS

10- Quais tratamentos que os dados precisam receber antes de serem armazenados?

( ) Classificação

( ) Criptografia

( ) Compactação

( ) Permissões de acesso

( ) Outros: _____

_____

_____

_____

_____

11- O que você considera necessário para classificar os dados a serem "*backapeados*"?

( ) Separação de arquivos, de programas e aplicações

( ) Análise de riscos

( ) Prioridade de Recuperação

( ) Período de retenção

( ) Permissões de acesso

( ) Datas de criação e atualização

( ) Locais de armazenamento

( ) Outros: _____

_____

_____

_____

_____

D – FACILIDADES DE *BACKUP*, DISPONIBILIDADE E RECUPERAÇÃO

12- **O que você considera como melhores estratégias para minimizar o tempo para se fazer o *Backup*?**

( ) Classificar a informação

( ) Fazer o *Backup* apenas dos dados necessários

( ) Determinar a freqüência dos *backups*

( ) Executar o *backup* quando o sistema não está em operação

( ) Documentar os procedimentos e recursos utilizados para o *Backup* de Dados

( ) Outros: _____

_____

_____

_____

_____

_____

_____

_____

_____

13- **O que você considera como melhores estratégias para se ter o *Backup* de Dados sempre disponível, e de rápida e fácil Recuperação?**

( ) Manter uma equipe dedicada ao planejamento de *Backup* de Dados

( ) Nomear responsáveis pelos *Backups* e Recuperação dos dados

( ) Estimar o tempo de Recuperação, incluindo o tempo de identificar o problema e a solução, de acordo com tipo o armazenamento

( ) Estabelecer prioridades nos procedimentos de Recuperação

( ) Selecionar e utilizar tecnologias (*hardware*, *software* e meios de armazenamento) de *Backup* e Recuperação mais apropriadas

( ) Documentação dos métodos de Recuperação e *Backup* de Dados

( ) Documentação com todas as responsabilidades e responsáveis pela Recuperação e *Backup* de Dados

( ) Ter planos para desastres, ou acontecimentos inesperados

( ) Outros: _____

_____

_____

_____

_____

_____

_____

_____

_____

E – TECNOLOGIAS PARA *BACKUP* DE DADOS

14- **O que você considera necessário para escolher tecnologias de *hardware* e *software* para *Backup* de Dados?**

( ) Criticidade da informação classificada

( ) Período de retenção dos dados

( ) Espaço a ser ocupado pelos dados

( ) Rapidez para o *backup* e Recuperação dos dados

( ) Administração e Gerenciamento simplificado do *Backup* e Recuperação de dados

( ) Facilidade de utilização

( ) Preço do produto/equipamento

( ) Outros: _____

_____

_____

_____

15- **O que você considera necessário para escolher mídias para *Backup* de Dados?**

( ) Criticidade da informação classificada

( ) Período de retenção dos dados

( ) Espaço a ser ocupado pelos dados

( ) Facilidade de utilização

( ) Rapidez para o *backup* e Recuperação dos dados

( ) Preço do produto

( ) Outros: _____

_____

_____

_____

F – *BACKUP* EM SITE REMOTO

16- **Quando é imprescindível, ou obrigatório o *Backup* Remoto?**

( ) Quando os dados precisam de um longo período de retenção

( ) Para dados que precisam ser consultados continuamente

( ) Para atendimento a padrões nacionais e internacionais

( ) outros: _____

_____

_____

_____

17- **O que você considera necessário para contratar um site de *Backup* Remoto?**

( ) Distância geográfica, e a probabilidade de acontecer um desastre que atinja o *backup* local e remoto.

( ) Acessibilidade, ou tempo necessário para se recuperar o *backup*

( ) Facilidades e velocidade de Conexões de rede e Internet

( ) Segurança física e lógica dos dados armazenados

( ) Estrutura do ambiente onde os dados são armazenados, como controle de temperatura, umidade, prevenção contra incêndio, controles de energia elétrica

( ) Conformidade da empresa contratada com padrões de segurança

( ) Tecnologias avançadas

( ) Garantia de compatibilidade de *software* e aplicações

( ) Preços

( ) outros: _____

_____

_____

_____

G – DOCUMENTAÇÃO

18- **O que você considera como melhores estratégias para se criar e manter a documentação de *Backup* e Recuperação de Dados?**

( ) Política para documentar todos os processo e recursos de *Backup* e Recuperação de dados

( ) Padrões e ferramenta de *software* adequada para documentação

( ) *Backup* da documentação de *Backup* e Recuperação de dados

( ) Avaliação e revisão da documentação de *Backup* e Recuperação

( ) Outros: _____

_____

_____

_____

_____

_____

_____

H – TESTES E AVALIAÇÕES DO PLANO DE *BACKUP* DE DADOS

19- **Qual(is) grupo(s) deve(m) ser responsáveis por testar e avaliar o Plano de *Backup* de Dados?**

( ) Alta administração

( ) Supervisão de TI

( ) Corpo técnico de TI

( ) Corpo técnico Administrativo

( ) Outros: _____

_____

_____

_____

_____

20- **Qual a periodicidade, você considera importante, para testar e avaliar os Planos de *Backup* de Dados?**

( ) trimestralmente

( ) semestralmente

( ) anualmente

( ) Outra: _____

_____