FUNDAÇÃO DE ASSISTÊNCIA E EDUCAÇÃO - FAESA

CENTRO DE PÓS-GRADUAÇÃO

CURSO DE PÓS-GRADUAÇÃO *LATO SENSU* EM INFRAESTRUTURA DE REDES DE COMPUTADORES

Marcos da Silva Furlan

Naziro Hamed de Assis

Backup:
Proteção e segurança de dados e informações em ambientes corporativos

Vitória
2015

Marcos da Silva Furlan

Naziro Hamed de Assis

Backup:
Proteção e segurança de dados e informações em ambientes corporativos

Monografia apresentada ao Centro de Pós-graduação da FAESA, como requisito parcial para a obtenção do título de especialista em Infraestrutura de Redes de Computadores, sob orientação da Profa. MSc. Maria da Gloria Moraes de Castro.

Vitória
2015

Marcos da Silva Furlan

Naziro Hamed de Assis

Backup:
Proteção e segurança de dados e informações em ambientes corporativos

Monografia apresentada ao Centro de Pós-graduação da FAESA, como requisito parcial para a obtenção do título de especialista em Infraestrutura de Redes de Computadores.

Vitória, ____ de _____ de 2015.

Nota de Aprovação: _____

_____

Professor(a) Orientador(a)

Profª MSc. Maria da Gloria Moraes de Castro.

Assis, Naziro Hamed de
Backup: Proteção e segurança de dados e informações em ambientes corporativos / Naziro Hamed de Assis; Marcos da Silva Furlan. Vitória – ES: Fundação de Assistência e Educação – FAESA, 2015.
53p.

Orientação de Maria da Glória Moraes de Castro

Trabalho de Conclusão de Curso (Pós Graduação) – FAESA – Fundação de Assistência e Educação, Pós Graduação em Infraestrutura de Redes de Computadores, 2015.

1. Introdução 2. Conceito de *Backup*
3. Aspectos Técnicos do *Backup* 4. Ferramentas de *Backup*
5. O Valor da Informação para as Corporações
6. Relatos: Casos Reais de Perda de Dados 7. Metodologia
8. Considerações Finais

I. Castro, Maria da Glória Moraes de
II. FAESA – Fundação de Assistência e Educação
III.Título.

DEDICATÓRIA

Dedicamos primeiramente à Jesus Cristo que é o autor e Senhor de nossas vidas. Aos nossos pais e as nossas famílias. Aos nossos amigos, que participaram direta ou indiretamente desta conquista. E, por fim, à nossa professora e orientadora Maria da Glória Moraes de Castro.

AGRADECIMENTOS

Agradecemos ao Senhor Deus por ter nos concedido capacidade, força, dedicação, sabedoria e coragem para vencer as adversidades. Às nossas famílias, por estarem sempre ao nosso lado, nos apoiando em todos os momentos, às nossas companheiras que nos ensinaram a termos mansidão, aos professores por transmitirem seus conhecimentos e à orientadora Maria da Gloria Moraes de Castro que dedicou seu tempo, conhecimento e paciência, para que pudéssemos obter sucesso na elaboração deste fazer.

“Apegue-te à instrução, e não a largues; guarda-a, pois ela é a tua vida.”

Bíblia Sagrada – Provérbios 4.13

RESUMO

Backup: Proteção e segurança de dados e informações em ambientes corporativos

O presente estudo reporta-se a uma revisão de literatura acerca das vantagens do uso de *backup* em ambientes corporativo. Buscou-se evidenciar os aspectos técnicos de *backup*, assim como algumas ferramentas pagas e gratuitas, que podem ser utilizadas para definir uma política de *backup* eficiente e eficaz. Considera-se que a proposta de estudo possa expor a importância do uso de *backup* em ambientes corporativos. Conclui-se que, embora o termo *backup* e seu conceito sejam populares, muitas corporações ainda não o utilizam ou o utilizam de forma equivocada, e não mensuram o impacto que pode ser acarretado em suas estruturas, no caso de perda permanente de dados e informações que sejam necessários para garantir a continuidade e expansão do negócio da corporação, concordando com os casos reais de perda de dados apresentados no decorrer deste estudo.

Palavras-chave: *Backup*, Dados, Informações, Corporações, Ferramentas de *backup*, Política de *Backup*, Perda de Dados.

ABSTRACT

Backup: Safety and security of data and information in enterprise environments

This study refers to a literature review about the benefits of backup use in corporate environments. It sought to highlight the technical aspects of backup, as well as some paid and free tools that can be used to define an efficient and effective backup policy. It is considered that the proposed study will expose the importance of using up in corporate environments. We conclude that, although the backup term and its concept are popular, many corporations still do not use it or use it wrongly, and do not measure the impact that can be brought about in their structures, in the case of permanent loss of data and information It is necessary to ensure the continuity and expansion of the corporation's business, agreeing with actual cases of loss of data presented throughout this study.

Keywords: Backup, Data, Information, Corporations, Backup Tools, Backup Policy, Data Loss.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

TI – Tecnologia da Informação

LTO – *Linear Tape-Open*

DAT – *Digital Audio Tape*

DLT – *Digital Line Tape*

IRF – Imposto de Renda na Fonte

INSS – Instituto Nacional do Seguro Social

FGTS – Fundo de Garantia por Tempo de Serviço

RAIS – Relação Anual de Informações Sociais

CAGED – Comunicação de Admissão e Demissão ao Ministério do Trabalho

PCMSO – Programa de Controle Médico de Saúde Ocupacional

DIPJ – Declaração de Informações Econômico-Fiscais da Pessoa Jurídica

DIRF – Declaração de Imposto de Renda Retido na Fonte

DCTF – Declaração de Débitos e Créditos Tributários Federais

DACON – Demonstrativo de Apuração de Contribuições Sociais

TLF – Taxa de Licença para Funcionamento

ISS – Imposto sobre Serviço

IRPJ – Imposto de Renda de Pessoa Jurídica

DARF – Documento de Arrecadação de Receitas Federais

CSLL – Contribuição Social sobre o Lucro Líquido

PIS – Programa de Integração Social

COFINS – Contribuição para o Financiamento da Seguridade Social

NF – Nota Fiscal

SMAS – Secretaria Municipal de Assistência Social

WTC – *World Trade Center*

SUMÁRIO

1 INTRODUÇÃO

A informação é um ativo intangível de extrema importância para manutenção e continuidade dos negócios de uma organização e as corporações estão se informatizando cada vez mais, buscando atender a sua demanda crescente por novas informações que agreguem valor de mercado aos seus produtos e serviços, com o uso intensivo das redes de computadores e da *Web*. Por outro lado, surge a questão da manutenção da segurança das informações, uma vez que a *Web* e as redes de computadores, assim como as informações armazenadas nos computadores que as constituem, estão cada vez mais expostas aos riscos de ataques *hackers*, vírus e outras ameaças virtuais.

Neste contexto, o *backup* torna-se um poderoso recurso no auxilio à segurança e manutenção dos dados e informações das corporações, uma vez que a implementação adequada, manutenção e utilização do mesmo, mitiga os impactos provenientes da perda de dados e informações digitais, dado o fato que, tais dados e informações podem ser recuperados e utilizados, garantindo a continuidade dos negócios das organizações.

Com a elaboração deste trabalho, busca-se ampliar o conhecimento sobre o que é *backup* e qual a sua importância e vantagens de uso em ambientes corporativos.

Esse estudo desenvolveu-se em capítulos. O capítulo 1 é constituído desta introdução, onde consta o tema, a justificativa e os objetivos os quais nortearam o desenvolvimento deste trabalho. Nos capítulos 2 e 3 apresentam-se os conceitos básicos, as modalidades, tipos, política e dispositivos de armazenamento de dados de *backup*. O capítulo 4 norteou o leitor quanto às ferramentas gratuitas e pagas, seguido do capítulo 5, ressaltando sobre a valoração das informações com auxílio do *backup* nos ambientes corporativos. Para ilustrar os fundamentos teóricos relatou-se no capítulo 6, casos reais de perdas de dados nas organizações. No capítulo 7 explicou-se os procedimentos metodológicos, relatando todas as etapas na elaboração do presente trabalho. Finalmente no capítulo 8 apresentaram-se as considerações finais, fazendo reflexões de todo trabalho, e ressaltando a importância desse tema no processo contemporâneo e tecnológico organizacional.

1.1 Objetivos

1.1.1 Geral

Apresentar a importância do processo de *backup*, nos ambientes corporativos.

1.1.2 Específicos

- Conceituar *backup*.
- Apresentar modos, tipos e política de *backup*.
- Apresentar dispositivos de armazenamento de dados.
- Listar algumas das ferramentas de *backup* mais utilizadas na atualidade (2015), assim como apresentar algumas de suas características.
- Expor a necessidade e as vantagens de utilização de *backup* em ambientes corporativos.
- Apresentar casos reais de perdas de dados em ambientes corporativos.

REVISÃO DE LITERATURA

2 CONCEITO DE *BACKUP*

Backup é a palavra utilizada para designar uma cópia de dados digitais, armazenada em um dispositivo de armazenamento virtual ou físico, diferente do dispositivo onde encontram-se os dados de origem. O *backup* representa a base de garantia para restauração dos dados, em seu estado original no momento da cópia, caso ocorra perda dos mesmos dentro de um sistema de informação. Quaisquer tipos de dados podem ser *backupeados*, sejam eles de cunho pessoal ou institucional e corporativo.

> "É um termo inglês que tem o significado de cópia de segurança. É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos." (Significados.com.br, 2012.http://www.significados.com.br/*backup*/> Acesso em 16 de novembro de 2015)

Segundo Innarelli (2003, pág. 24), *Backup* é uma cópia de segurança dos dados armazenados no sistema de informação da instituição ou dos dados de uso pessoal. Este *backup* é fundamental para qualquer sistema de informação ou pessoa, pois ele é a garantia da restauração dos dados caso haja uma pane nos equipamentos da instituição ou pessoa.

Para Sant'Ana (2002, pág. 72) o *Backup* significa proteção e segurança de qualquer tipo de informação dada como importante para uma empresa, seja na forma impressa ou digital, independentemente da área de atuação sendo um recurso de extrema importância.

3 ASPECTOS TÉCNICOS DO *BACKUP*

Os principais aspectos técnicos do *backup* são: modalidades, tipos, política e dispositivos de armazenamento.

3.1 Modalidades de *Backup*

A modalidade de *backup* corresponde à disponibilidade dos dados, aos usuários, no momento em que os mesmos estão sendo *backupeados* por uma ferramenta de *backup*.

3.1.1 *Backup Online*

É a modalidade de armazenamento de dados em que os arquivos, pastas ou todo o conteúdo de uma mídia de armazenamento estão disponíveis para acesso e/ou alteração por usuários e/ou sistemas.

Os *backups online* geralmente são realizados em um servidor remoto ou computador com conexão de rede.

Cardozo (2006, p. 13) aponta que a vantagem do *backup online* é a não interrupção do serviço de disponibilização dos dados, enquanto que as desvantagens são: a redução do desempenho do servidor e dados ou arquivos em uso não são atualizados.

3.1.2 *Backup Off-line*

É a modalidade de armazenamento de dados em que a mídia de armazenamento está indisponível para acesso de seu conteúdo, enquanto o processo de *backup* é efetuado na mesma. Em outras palavras, significa que os dados, arquivos, pastas e outros ficheiros estão indisponíveis para acesso ou alteração durante o processo de cópia.

Cardozo (2006, p. 14) aponta que a vantagem do *backup off-line* é a realização de *backup* de todos os dados, já que os mesmos não estão em processo de execução por usuários e/ou sistemas, enquanto que a desvantagem é a não disponibilização dos dados, arquivos e outros ficheiros durante a execução do processo de cópia.

3.2 Tipos de *Backup*

Vários tipos de *backup* podem ser usados para modalidade de *backups online* e *off-line*. Os aspectos do ambiente que determinam os tipos ou combinações de tipos de *backup* são ideais para atender determinadas demandas.

3.2.1 *Backup* Total ou Completo

O *backup* completo corresponde à cópia integral de todos os ficheiros para um determinado dispositivo de armazenamento. O *backup* total independe de versões anteriores ou de alterações dos ficheiros que foram realizadas desde o último *backup* efetuado.

O *backup* total ou completo é tido como o tipo tradicional de *backup* e através dele, todos os outros tipos de *backup* são implementados.

Conforme Sant'Ana (2002, p. 17), os *backups* totais possuem a vantagem de apresentarem rápida localização e restauração dos dados e como desvantagem geram um grande volume de dados, uma vez que copiam todos os dados, alterados ou não.

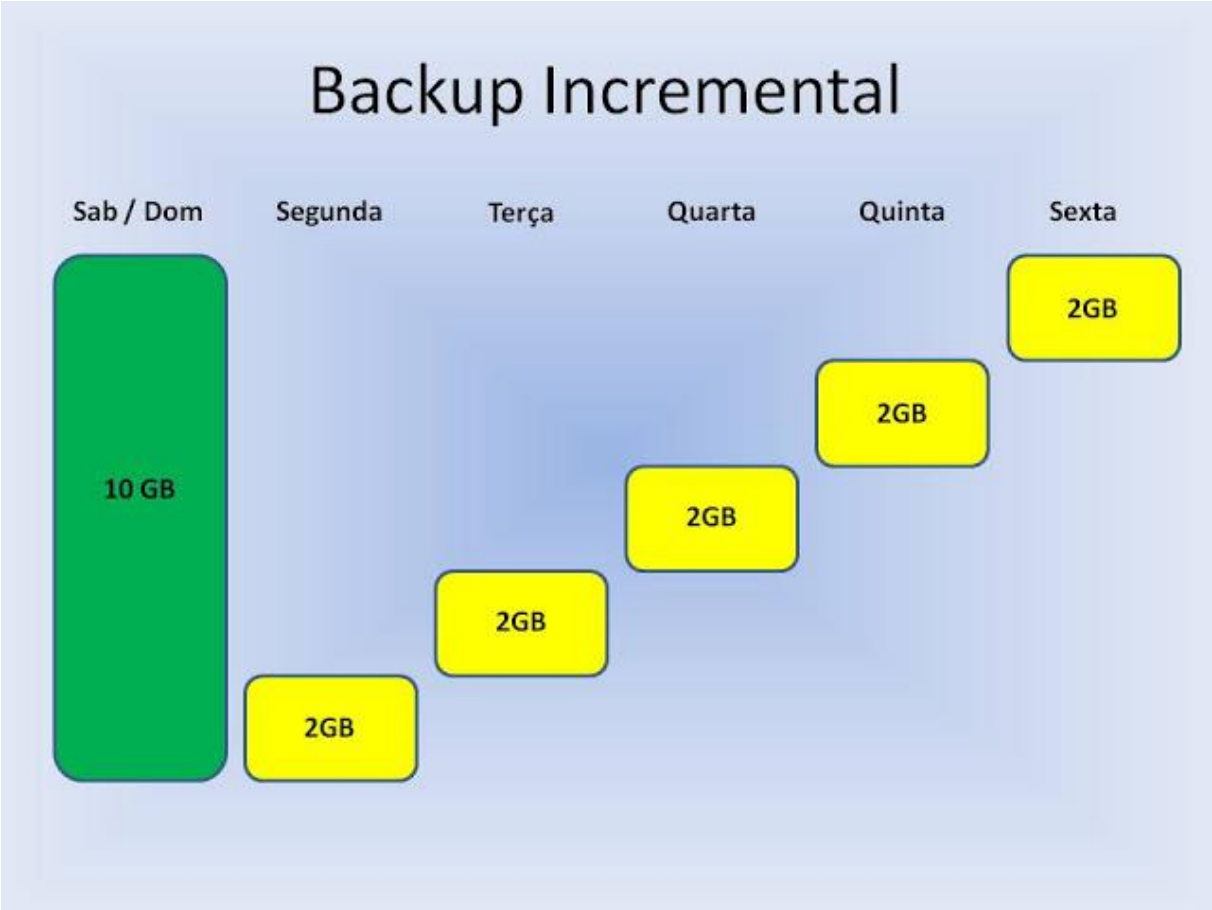
3.2.2 *Backup* Incremental

Os *backups* incrementais verificam se o horário de alteração de um arquivo é mais recente que o horário do último *backup* realizado, seja um *backup* completo ou outro incremental. Caso o arquivo não tenha sido modificado desde o último *backup* ele não é copiado novamente. Caso contrário, efetua-se a cópia da última versão do arquivo.

Os *backups* incrementais são usados em conjunto com *backup* completo frequente (ex.: um *backup* completo semanal, com incrementais diários).

> "A vantagem principal em usar *backups* incrementais é que rodam mais rápido que os *backups* completos. A principal desvantagem dos *backups* incrementais é que para restaurar um determinado arquivo, pode ser necessário procurar em um ou mais *backups* incrementais até encontrar o arquivo. Para restaurar um sistema de arquivo completo, é necessário restaurar o último *backup* completo e todos os *backups* incrementais subsequentes. Numa tentativa de diminuir a necessidade de procurar em todos os *backups* incrementais, foi implementada uma tática ligeiramente diferente. Esta é conhecida como *backup* diferencial." (MACEDO, 2012, p. 3. Disponível em: <http://www.diegomacedo.com.br/*backup*-conceito-e-tipos//> Acesso em: Acesso em 20 de novembro de 2015)

Figura 01 – Representação do *Backup* Incremental



Fonte: Página do Fernando Almeida no *Blogspot* [1].

A Figura 01 mostra a rotina diária do *backup* incremental durante o período de uma semana. No sábado e domingo é realizado o *backup* completo da base dos dados. Considerando que o volume de dados produzidos diariamente, em uma dada organização seja de 2 GB por dia. Na segunda-feira foi realizada cópia de *backup* somente dos 2 GB de dados produzidos no decorrer da segunda-feira, e no final da terça-feira foi realizado o *backup* somente dos dados produzidos na terça-feira, que eram diferentes dos dados da segunda-feira. Na quarta-feira foi realizado o *backup* dos 2 GB de dados produzidos durante a quarta e que eram diferentes dos dados gerados na terça-feira, e assim por adiante, até o sábado, quando inicia-se o *backup* completo de toda a base, o qual será composto pelo último *backup* completo realizado anteriormente e por todos os *backups* incrementais realizados durante a semana, ou seja, *backup* incremental de segunda-feira, terça-feira, quarta-feira, quinta-feira e sexta-feira.

[1] Disponível em < http://fernandopsalmeida.blogspot.com.br/2011/11/backup-diferencial-e-backup-incremental.html> Acesso em 23 de novembro de 2015.

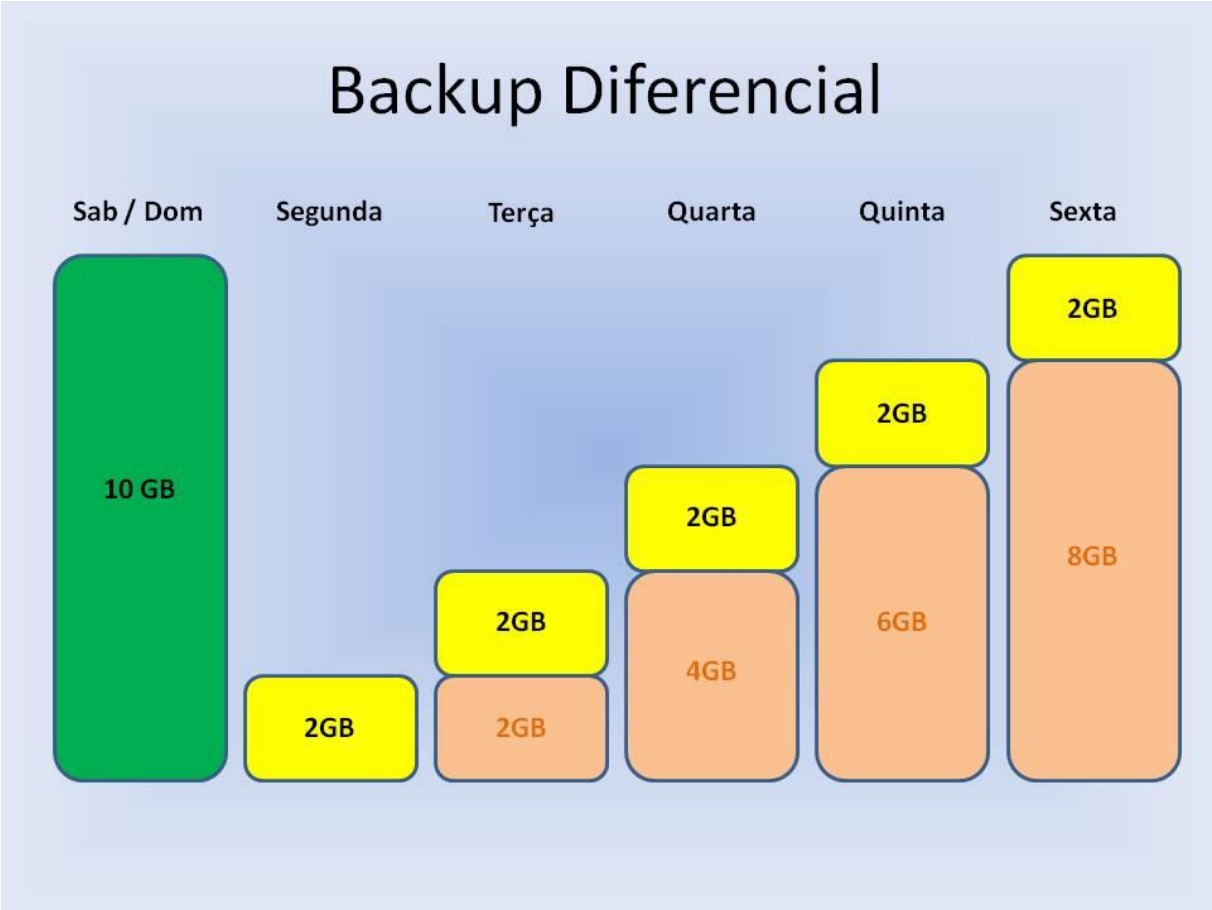
3.2.3 *Backup* Diferencial

O *backup* diferencial copia arquivos alterados desde o último *backup*. A diferença deste para o integral é que cada *backup* diferencial mapeia as alterações em relação somente ao último *backup* completo ou total.

Como o *backup* diferencial é efetuado com base nas alterações do último *backup* completo, a cada alteração de arquivos, o tamanho do *backup* aumenta de forma progressiva.

> Em relação ao *backup* completo, ele é mais rápido, salva espaço e é mais simples de restaurar que os *backups* incrementais. A desvantagem é que vários arquivos que foram alterados desde o último *backup* completo serão repetidamente copiados. *Backups* diferenciais são similares aos *backups* incrementais pois ambos podem fazer *backup* somente de arquivos modificados. No entanto, os *backups* diferenciais são acumulativos, em outras palavras, no caso de um *backup* diferencial, uma vez que um arquivo foi modificado, este continua a ser incluso em todos os *backups* diferenciais (obviamente, até o próximo *backup* completo). Isto significa que cada *backup* diferencial contém todos os arquivos modificados desde o último *backup* completo, possibilitando executar uma restauração completa somente com o último *backup* completo e o último *backup* diferencial. Assim como a estratégia utilizada nos *backups* incrementais, os *backups* diferenciais normalmente seguem a mesma tática: um único *backup* completo periódico seguido de *backups* diferenciais mais frequentes. O efeito de usar *backups* diferenciais desta maneira é que estes tendem a crescer um pouco ao longo do tempo (assumindo que arquivos diferentes foram modificados entre os *backups* completos) (MACEDO, 2012, p. 4 e 5. Disponível em: <http://www.diegomacedo.com.br/*backup*-conceito-e-tipos//> Acesso em: Acesso em 20 de novembro de 2015)

Figura 02 – Representação do *Backup* Diferencial



Fonte: Página do Fernando Almeida no *Blogspot* [1].

3.3 *Backup* Incremental e Diferencial – Vantagens e Desvantagens

A Figura 02 mostra a rotina diária do *backup* diferencial durante o período de uma semana. No sábado e domingo é realizado o *backup* completo da base dos dados. Considerando que o volume de dados produzidos diariamente, em uma dada organização seja de 2 GB por dia. Na segunda-feira foi realizada cópia de *backup* somente dos 2 GB de dados produzidos no decorrer da segunda-feira, e no final da terça-feira foi realizada o *backup* de todos os dados diferentes do último *backup* completo, ou seja, foi realizado o *backup* dos dados produzidos na segunda-feira e na terça-feira. No final da quarta-feira, todos os dados que

[1] Disponível em < http://fernandopsalmeida.blogspot.com.br/2011/11/backup-diferencial-e-backup-incremental.html> Acesso em 23 de novembro de 2015.

estavam presentes na base e que se diferenciavam dos dados do último *backup* completo, foram copiados, ou seja, os dados produzidos na segunda-feira e terça-feira foram copiados novamente junto com os dados produzidos na quarta. Os backups diferenciais da quinta-feira e sexta-feira seguirão a mesma lógica para a cópia dos dados. No sábado e domingo o *backup* completo consistirá na cópia do último *backup* completo juntamente com o último *backup* diferencial efetuado na semana (*backup* diferencial de sexta-feira), o qual possuirá todos os dados produzidos no decorrer de toda a semana.

Após o entendimento de como funciona cada um dos tipos básicos de *backup*, torna-se mais fácil entender as vantagens e desvantagens de cada tipo. Segue o Quadro 01, o qual correlaciona os tipos de *backup* incremental e diferencial, suas vantagens e desvantagens.

Quadro 01 – Tipos de *Backup* – Vantagens x Desvantagens

TIPO DE *BACKUP*	**VANTAGENS**	**DESVANTAGENS**
Incremental (todos os ficheiros novos ou alterados desde o último *backup* completo ou parcial)	- *Backup* mais rápido porque há menos ficheiros - Desgaste reduzido no equipamento de *backup* e na *tape*. - São necessárias menos *tapes*.	- Reparação mais lenta porque pode ser necessário mais de duas *tapes* (a *tape* de *backup* completo e cada uma das *tapes* de *backup* incremental). - Aumento dos custos de *downtime* em caso de quebra no sistema.
Diferencial (todos os ficheiros novos ou alterados desde o último *backup* completo)	- Reparação mais rápida porque só são necessários dois conjuntos de *tapes* (as *tapes* de *backup* completo e de *backup* diferencial). - Custos reduzidos de *downtime* em caso de quebra no sistema.	- Processo de *backup* mais lento, porque são copiados mais ficheiros. - Aumento de desgaste no equipamento de *backup* e na *tape*. - Podem ser necessárias mais *tapes*.

Fonte: MOUTA, 2002, p. 31.

3.4 Política de *Backup*

A política de *backup* é o passo mais importante para garantir a preservação íntegra e confiável de documentos digitais e sistemas informatizados. É ela que define a estratégia de *backup* que assegura a cópia dos dados e informações considerados indispensáveis e críticas para a continuidade do negócio de uma corporação.

No geral, os dados que necessitam ser armazenados correspondem aos dados e informações fiscais, de configurações dos sistemas e dados da base de informações estratégicas e de negócios, os quais são fundamentais para a manutenção da continuidade do negócio da corporação.

A política é definida através da análise macro e micro dos processos ou atividades operacionais do ambiente corporativo em questão e no geral define os dados que deverão ser armazenados, a periodicidade e os tipos de *backup* que serão utilizados, o volume dos dados a ser armazenado, a infraestrutura necessária e como será realizada a auditoria da política.

Para que seja definida uma política de *backup* eficiente e eficaz, torna-se necessária uma boa integração e um bom alinhamento entre os gestores corporativos e a equipe responsável pela Tecnologia da Informação (TI) da corporação.

3.4.1 Periodicidade e os Tipos de *Backup*

A periodicidade do *backup* será proporcional ao tempo de inserção de novos dados e informações relevantes, para a gestão, na base de origem dos dados, sendo de competência da gestão da corporação, estimar o tempo para a inserção de novas informações de valia.

Segundo Sant’Ana (2002, p. 14) a perda de dados e informações gerados há dias ou horas, podem ter grandes impactos e isso dependerá da informação, por esse motivo as organizações devem analisar cuidadosamente o quê deve estar à salvo o quanto de perda de tempo com perda de informação é aceitável.

Segundo Swanson et al (2002), apud Moraes (2007, p. 31), a política de *backup* deve especificar a frequência do *backup*, por exemplo, diário ou semanal, incremental ou completo, baseada na criticidade dos dados e na frequência em que informação nova é introduzida.

3.4.2 Volume de Dados Gerados e Infraestrutura Necessária

Após a definição exata do volume e tipos de dados que serão armazenados, compete à equipe de TI realizar um estudo de caso para levantamento de quais *softwares* de *backup* e infraestrutura serão capazes de atender a demanda da corporação com o melhor custo benefício.

Segundo Gonçalves (2002), apud Moraes (2007, p. 31), 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 *backup* tem a finalidade de garantir que os dados armazenados sejam confiáveis e disponíveis.

Segundo Swanson et al (2002, apud Moraes, 2007, p. 31), a política de *backup* também deve designar o local para armazenamento dos dados, procedimentos de nomeação de arquivos, frequência de trocas dos dispositivos de armazenamento, e método para transportar os dados.

3.4.3 Auditoria da Política de *Backup*

A auditoria consiste na análise de conformidade de todos os aspectos da política, tais como: se os dados que devem ser armazenados realmente estão sendo armazenados com a periodicidade correta e através do tipo de *backup* definido para uma determinada base de dados e se o volume de dados gerados está sendo similar ao previsto, se a infraestrutura de TI está suportando a demanda crescente dos

dados armazenados e principalmente se a restauração dos dados e informações *backupeados* está funcionando de forma a manter a disponibilidade, integridade, confidencialidade e autenticidade dos mesmos.

Em suma, a auditoria é utilizada para checar se a política de *backup* definida está sendo seguida de forma efetiva e se ajustes serão necessários a fim de aperfeiçoá-la.

É de grande valia que a auditoria não seja realizada pela equipe responsável pela execução do *backup*, mas por outras pessoas que possuam competência técnica para auditá-la e com imparcialidade em relação à execução da atividade de *backup* e às pessoas responsáveis pelo mesmo, com o intuito de fazer um julgamento rigoroso dos fatos analisados durante a execução da auditoria.

Conforme a 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.

3.5 Dispositivos de Armazenamento de Dados

Há diversos tipos de mídias ou dispositivos de armazenamento de dados digitais que são utilizados para armazenamento de *backup* e as principais categorias dos dispositivos de armazenamento são: óptico, magnético e eletrônico.

3.5.1 Dispositivos Ópticos

Os dispositivos de armazenamento ópticos são os de custo mais baixo e considerável capacidade de armazenamento de dados, quando os dados a serem armazenados representam arquivos de texto, planilhas, slides e outros formatos de arquivos comuns muito utilizados em escritórios. Nesta categoria encontramos o Minidisco, CD, DVD e Blu-*Ray*.

> Armazenamento óptico usa um *laser* para queimar covas pequenas e escuras na superfície de um disco. No caso de CDs, CD-ROM, e discos de DVD, são criadas as *pits* (covas) quando a superfície do disco é forçada em um molde. As covas são escuras e os lugares sem covas (chamado de *lands*), permaneça brilhante e liso. Um dispositivo de *playback* pode ler este revezamento de manchas escuras e claras como sendo 0s e 1s. (Dispositivos de Armazenamento de Dados, 2007. Disponível em: <https://infocp.*wordpress*.com/armazenamento/> Acesso em: 22 de novembro de 2015)

A leitura, das mídias ópticas, é efetuada através da interpretação dos *pits* e *lands* pelo leitor de disco de unidade óptica, como 0s e 1s, os quais são processados e passam a apresentar a informação que foi armazenada.

3.5.2 Dispositivos Magnéticos

Os dispositivos de armazenamento por meio magnético são os mais antigos e mais utilizados, permitindo a gravação de uma grande densidade de dados. Estão presentes nesta categoria o Disco Rígido, Disquetes e Fitas de armazenamento de dados como a LTO, DAT, DLT e outras.

> Polaridades opostas se atraem, e polaridades idênticas se repelem. Dispositivos de armazenamento magnéticos usam estes dois estados magnéticos para registrar dados em um disco ou fita.
> Quando um disco gira ou uma fita se move, sinais elétricos nas cabeças *read/write* do drive mudam a polaridade de partículas magnéticas minúsculas na superfície magnética da mídia para registrar 0s e 1s. Quando você recobra um arquivo, o efeito é invertido. A polaridade da mídia induz uma corrente elétrica imediatamente abaixo da cabeça de *read/write* na cabeça de *read/write* que é transmitida ao computador na forma de 0s e 1s. (Dispositivos de Armazenamento de Dados, 2007. Disponível em: <https://infocp.*wordpress*.com/armazenamento/> Acesso em: 22 de novembro de 2015)

O resultado do processamento dos 0s e 1s corresponde à informação que está armazenada na mídia.

3.5.3 Dispositivos Eletrônicos

Os dispositivos de armazenamento eletrônico são os mais atuais e práticos e também são os que apresentam a melhor perspectiva para evolução do desempenho na atividade de armazenamento. A tecnologia de armazenamento eletrônico também é chamada de memória de estado sólido. Os equipamentos representantes desta categoria são: *pendrive*, cartão de memória *flash* e disco rígido de estado sólido.

> A gravação das informações em um dispositivo de armazenamento por meio eletrônico se dá através dos materiais utilizados na fabricação dos *chips* que armazenam as informações. Para cada dígito binário (*bit*) a ser armazenado nesse tipo de dispositivo existe duas portas feitas de material semicondutor, a porta flutuante e a porta de controle. Entre estas duas portas existe uma pequena camada de óxido, que quando carregada com elétrons representa um *bit* 1 e quando descarregada representa um *bit* 0. (Vieira, 2012. Disponível em: <http://www.ebah.com.br/content/ABAAAgsE8AB/codificacao-armazenamento-informacao/> Acesso em: 22 de novembro de 2015)

3.6 Dispositivos de Armazenamento – Capacidades e Velocidades

Os dispositivos de armazenamento variam de capacidade de armazenamento e velocidade de leitura e gravação dos dados, conforme as tecnologias que são utilizadas em sua fabricação.

Segue quadro de referência de alguns dispositivos:

Quadro 02 – Dispositivos de Armazenamento – Capacidade e Velocidade

Dispositivo	Capacidade	de Leitura	de Gravação
Disquete	1,44 MB	62,5 KB/s	62,5 KB/s
MiniDisco	160 MB	-	352 KB/s
CD	700 MB	7800 KB/s (52x)	7200 KB/s (48x)
DVD	4,7 GB e 8,5 GB	32,4 MB/s (24x)	32,4 MB/s (24x)
Blu-*ray*	25 GB e 50 GB	54 MB/s (12x)	54 MB/s (12x)
Cartão de memória *flash*	até 48 GB	40 MB/s	12 MB/s
Pendrive	até 128 GB	30 MB/s	15 MB/s
Fita magnética	até 400 GB	80 MB/s	80 MB/s
Disco de estado sólido	até 256 GB	700 MB/s	250 MB/s
Disco rígido	até 2,5 TB	70 MB/s	70 MB/s

Fonte: Página do Dan *Scientia* no *Blogspot* [2].

3.7 Propensão à Falha

Todos os dispositivos de armazenamento estão propensos às falhas ou danos e consequentemente dados e informações neles armazenadas também estão propensos à perda, variando conforme o dispositivo e o incidente que levou à falha.

Segue quadro com alguns fatores que podem acarretar falha nos dispositivos:

Quadro 03 - Dispositivos de Armazenamento x Fatores de Falha

Dispositivo	Fator de Falha
MiniDisco/CD/DVD	Arranhão, corrosão por fungo.
Floppy	Desgaste pelo uso, campo magnético forte.
Memória *Flash*	Desgaste pelo uso, pico de energia.
Disco Rígido	Desgaste pelo uso, queima de circuito, pico de energia e impacto forte.
Pendrive	Desgaste pelo uso, uso incorreto, pico de energia.
E-mail	Problemas no servidor de *e-mail.*

Fonte: POZZER, 2006, p. 4.

[2] Disponível em: <http://dan-scientia.blogspot.com.br/2010/07/o-que-sao-dispositivos-de-armazenamento.html> Acesso em 20 de novembro de 2015.

4 FERRAMENTAS DE *BACKUP*

As ferramentas disponíveis para a realização de *backup* são as mais variadas. Desde ferramentas pagas às ferramentas gratuitas. Sendo que cada ferramenta apresenta suas próprias particularidades.

Algumas características que essas ferramentas podem possuir são: arquitetura cliente/servidor, criptografia do *backup*, cópia de arquivos abertos, compressão de dados, agendamento e assistente de tarefas, implementação de tipos diferentes de *backup* e compatibilidade com sistemas operacionais diferentes.

4.1 Ferramentas Gratuitas

Há ferramentas gratuitas de *backup* que se destacam no mercado por apresentarem vasta gama de recursos, as quais permitem o gerenciamento e monitoramento de políticas complexas de *backup*. A seguir serão apresentadas três dessas ferramentas.

4.1.1 *Amanda Backup*

O *software Amanda Backup* possui arquitetura cliente/servidor, e disponibiliza recursos como criptografia do *backup*, cópia de arquivos abertos, agendamento de tarefas e compressão de dados. O Amanda usa utilitários nativos para efetuar *backup* de um grande número de servidores e estações de trabalho com várias versões de Linux ou Unix e usa um cliente nativo do Windows para fazer *backup* de *desktops* e servidores Microsoft Windows.

Mais informações sobre a ferramenta Amanda *Backup*, assim como o instalador e o manual, encontram-se disponíveis na página oficial da ferramenta.

4.1.2 *Bacula Backup*

A ferramenta de *backup Bacula* é um sistema com arquitetura cliente/servidor que pode operar através de processos distribuídos que permite a realização da cópia e salvaguarda dos dados de forma centralizada ou distribuídas. O *Bacula* pode ser instalado e utilizando em Sistemas Operacionais (SO) *Linux* e *Windows*. Possui recursos de criptografia de dados, cópia de arquivos abertos, agendamento de tarefas e compressão de dados.

Mais informações sobre a ferramenta de *backup Bacula*, assim como o instalador e o manual, encontram-se disponíveis na página oficial da ferramenta.

4.1.3 *Cobian Backup*

O *Cobian* é um programa de *backup* que permite agendamento de tarefas de *backup* de pastas e arquivos em um computador local ou remoto. O *Cobian* possui recursos de criptografia e compressão das cópias e apresenta uma interface gráfica intuitiva com vários utilitários que auxiliam o administrador na utilização dos recursos da ferramenta.

Mais informações sobre a ferramenta de *backup Cobian*, assim como o instalador e o manual, encontram-se disponíveis na página da ferramenta.

4.2 Ferramentas Pagas

As ferramentas pagas geralmente são mais robustas e apresentam uma grande variedade de recursos e utilitários que buscam automatizar as tarefas de *backup*, simplificando-as para os usuários da ferramenta. Seguem breves descrições de duas ferramentas de *backup* pagas que se destacam no mercado.

4.2.1 *Brightstor ARCserve Backup r15*

Trata-se de uma ferramenta de *backup* com arquitetura cliente servidor, que permite o armazenamento dos dados de forma integrada e escalável para discos rígidos, fitas e nuvem. O *ARCserve* possui interface intuitiva e disponibiliza recursos de criptografia, compressão dos dados e a possibilidade de efetuar *backup* de arquivos abertos. O *ARCserve* busca otimizar o armazenamento visando a redução de custos e maior disponibilidade de espaço livre em dispositivos de armazenamento. A fabricante disponibiliza também, versões de teste do *software ARCserve Backup*.

Mais informações sobre a ferramenta de *backup Brightstor ARCserve Backup r15*, assim como o instalador e o manual, podem ser encontrados na página oficial da ferramenta.

4.2.2 *Virtos S.O.S Backup*

É uma ferramenta de *backup* também de arquitetura cliente/servidor. Permite a criptografia e compreensão de dados. Pode efetuar o armazenamento em fitas, discos rígidos, nuvem e outras mídias de destino. A fabricante disponibiliza também, versões de teste do *software S.O.S Backup*.

Mais informações sobre a ferramenta de *backup Virtos S.O.S Backup*, assim como o instalador e o manual, podem ser encontrados na página oficial da fabricante.

4.3 Outras Ferramentas de *Backup*

Seguem descrições de outras ferramentas de *backup*, entre elas estão ferramentas pagas e gratuitas, voltadas para ambientes corporativos e outras voltadas para uso doméstico.

4.3.1 *SyncBack*

Realiza cópia de arquivos abertos, sincronização de pastas, controle de versão de arquivos, *backup* remoto e compressão de dados.

4.3.2 *Max Backup*

Realiza sincronização de pastas, agendamento de tarefas, cópia de configurações do sistema e *backup* remoto.

4.3.3 *Backup Maker*

Realiza agendamento de tarefas, *backup* remoto, criptografia do *backup* e possui interface intuitiva.

4.3.4 *Comodo Backup*

Realiza agendamento de tarefas, tipos diferentes de *backup* de forma automática e apresenta uma interface bastante intuitiva.

4.3.5 *Easeus Backup*

Realiza *backup* na nuvem, apresenta fácil usabilidade e possui uma grande diversidade de utilitários para auxiliar.

5 O VALOR DA INFORMAÇÃO PARA AS CORPORAÇÕES

As informações são conhecimentos adquiridos e gerados através da análise continua e registrada das atividades, processos e conhecimentos existentes dentro de um ambiente ou organização.
A informação é um ativo intangível das organizações e permite que as mesmas tomem decisões precisas para os seus negócios.

> [...] a informação é o item ideal e primário a que todos devem recorrer para antecipar decisões em todos os sentidos, pois não há tomada de decisão sem conhecimento antecipado, posto que tudo é baseado em conhecimento e este advém da informação. Ou seja, tudo o que acontece resulta em um conhecimento e este é a mola propulsora para, de acordo com as informações que o constitui, originar novas tomadas de decisão, novas informações e, consequentemente, novos conhecimentos (GONÇALVES; GOUVEIA; PETINARI, 2008, p.42/43).

As corporações conservam suas informações como um meio de adquirir vantagens, uma em relação ás outras, perante a concorrência que o mercado às impõe, sendo as informações consideradas o bem, com o maior valor de mercado, que uma corporação pode possuir.

> 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. (MORAES, 2007, p. 13).

Devido à necessidade de crescimento das organizações, o foco passou a ser a busca da informação, visando à sobrevivência e vantagem no mercado competitivo, sendo que a ferramenta tecnológica mais utilizada para alcançar este objetivo passou a ser a internet e as redes de computadores, o que ampliou a informatização

dos ambientes e mais do que nunca, tornou-se necessário manter as informações em segurança.

Conforme a NBR ISO/IEC (17799:2005, pág. 9) os ambientes informatizados das organizações estão expostos a uma grande diversidade de ameaças à segurança de seus dados e informações armazenadas digitalmente, desde falhas humanas na manipulação de dados, até roubos virtuais que comprometam a estrutura do *software* e incidentes naturais; que possam comprometer a estrutura de *hardware*.

5.1 A Necessidade do *Backup* em Ambientes Corporativos

A necessidade de *backup* em uma organização pode ser expressa por três aspectos básicos, os quais serão abordados a seguir.

5.1.1 *Backup* para Histórico Legal e Fiscal

Representa a cópia dos dados relacionados diretamente aos departamentos fiscais, recursos humanos, jurídico, controladoria e outros. Em suma, são documentos que compõem livros fiscais, contábeis e trabalhistas.

Documentação contábil: receitas e despesas, balanços patrimoniais anuais e mensais, distribuição de lucros isentos de Imposto de Renda na Fonte (IRF).

Documentação trabalhistas/previdenciárias: folhas de pagamentos de salários, fichas de registros de empregados, guias de recolhimento ao Instituto Nacional de Seguro Social (INSS), do Fundo de Garantia por Tempo de Serviço (FGTS), de contribuição sindical patronal, carnês INSS, folhas de pagamento de *Pro-Labore*, Relação Anual de Informações Sociais (RAIS), Comunicação de Admissão e Demissão ao Ministério do Trabalho (CAGED), dossiês de empregados, com exames médicos de admissão e renovação, contrato de trabalho, rescisões contratuais, comprovantes de entrega de vale-transporte, avisos e recibos de férias,

guias de recolhimento de contribuição sindical e assistencial de empregados, Programa de Controle Médico de Saúde Ocupacional (PCMSO) e outros.

Documentação fiscal: Declaração de Informações Econômico-Fiscais da Pessoa Jurídica (DIPJ), Declaração de Imposto de Renda Retido na Fonte (DIRFs), Declaração de Débitos e Créditos Tributários Federais (DCTF), Demonstrativo de Apuração de Contribuições Sociais (DACON), Taxas de Licença para Funcionamento (TLF) recolhidas, guias de recolhimento de Imposto Sobre Serviços (ISS), guias de recolhimento de Imposto de Renda de Pessoa Jurídica (IRPJ) – Documentos de Arrecadação de Receitas Federais (DARFs) e Contribuição Social sobre o Lucro Líquido (CSLL), guias de recolhimento DARFs de IRF, guias de recolhimento de DARFs do Programa de Integração Social (PIS), guia de recolhimento DARFs de Contribuição para o Financiamento da Seguridade Social (COFINS), comprovantes de compra de bens (Escrituras, Notas Fiscais, etc), Notas Fiscais (NF) de serviços prestados por terceiros, para comprovação e fiscalização do INSS, locação de imóveis e outros.

Documentação jurídica: contratos, alterações contratuais, aditivos contratuais, processos jurídicos e outros.

5.1.2 *Backup* para Configurações dos Sistemas

Os sistemas operacionais são complexos, com muitos arquivos, pastas e diretórios, *drivers*, fontes e outras configurações e recursos que dão suporte ao seu funcionamento adequado, enquanto que as aplicações, que rodam sobre o sistema operacional, executam atividades diretamente relacionadas aos processos da empresa e que por sua vez possuem configurações específicas para cada setor e/ou usuário da corporação. Cabe mencionar a complexidade das configurações do ambiente de rede que são personalizadas conforme as diversidades dos *hardwares* e *softwares*.

O *backup* de arquivos e aplicações, assim como as configurações dos mesmos e da rede é de grande auxílio e vantagem, uma vez que podem restaurar as condições adequadas de funcionamento do ambiente digital da corporação em pouco tempo.

5.1.3 *Backup* para Gestão de Negócios

Representa a cópia dos dados relacionados diretamente às atividades operacionais e administrativas da empresa, ou atividades de suporte que sejam essenciais à atividade fim.

Estes dados e informações auxiliam na monitoração de desempenho e no suporte funcional, decisório e estratégico da empresa. Correspondem aos dados com maior valor de mercado presentes em uma corporação.

5.2 Consequências da Perda de Dados em Ambientes Corporativos

Em detrimento do *backup* dos dados e informações relacionados aos aspectos mencionados anteriormente (dados fiscais, de sistemas e de negócios), os prejuízos podem ser incalculáveis no caso de perda de tais informações e os impactos podem variar de acordo com a criticidade das mesmas em garantir a continuidade do negócio da corporação.

No caso de perda de dados e informações sobre legalização ou fiscalização, a empresa poderá ser comprometida juridicamente perante as esferas do Governo Federal, Estadual e Municipal, perante os seus clientes, seus fornecedores e até mesmo os seus funcionários. Há grandes riscos de prejuízos financeiros, por multas ou indenizações, ou até mesmo, denegrição da imagem da corporação.

Em caso de falhas dos sistemas de TI, a restauração do ambiente sem o uso de *backup* poderia levar várias horas, dias ou mesmo semanas, o que acarretaria em improdutividade provocada pela ociosidade de funcionários ou mesmo suspensão de

atividades essenciais como venda e faturamento, com consequentes prejuízos financeiros ou danos morais, dependendo das atividades comprometidas e clientes e fornecedores afetados.

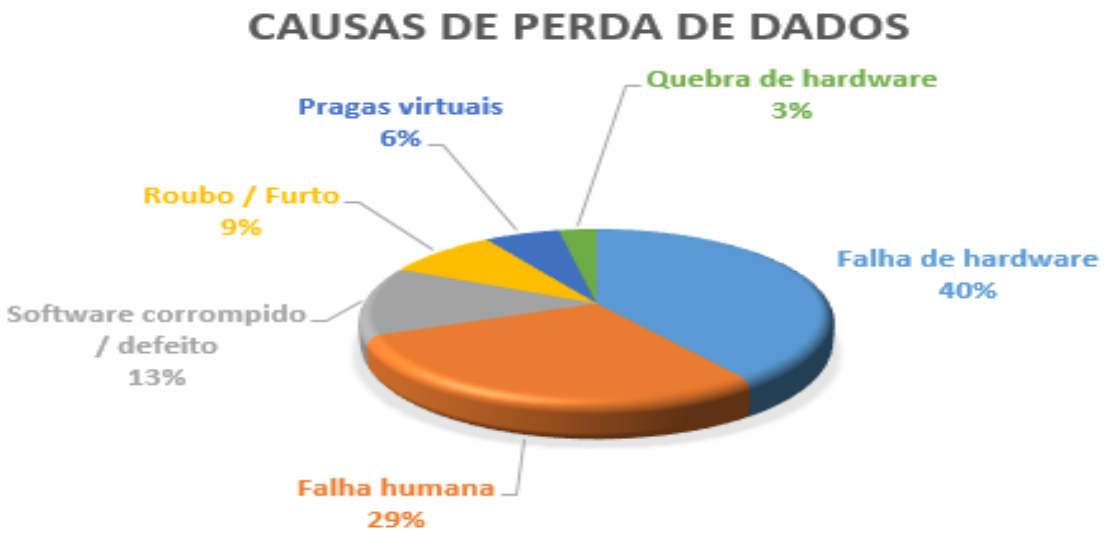
No caso de perda de dados e informações de negócios, as consequências podem variar desde retrabalho de funcionários e gestores para repor registros de atividades administrativas ou operacionais, conhecimentos e planejamentos (caso exista alguma possibilidade de repor tais informações), até a paralisação de atividades essenciais que comprometam moral e financeiramente a empresa, podendo levá-la à falência.

5.3 Causas de Perda de Dados em Ambientes Corporativos

Os tipos de incidentes mais conhecidos que provocam perda de dados são: falhas de *hardware*, falhas humanas, *softwares* corrompidos, furto, pragas virtuais e quebra de *hardware*.

Segue ilustração apresentando a porcentagem de tipos de incidentes por ocorrência de incidentes de perda de dados:

Figura 03 – Causas de Perda de Dados



Fonte: Página da *Recovy Labs* na *Web* [3].

[3] Disponível em < http://cdsb.com.br/apresentacao_parte001.php> Acesso em 26 de novembro de 2015.

6 RELATOS: CASOS REAIS DE PERDA DE DADOS

Os casos reais de perdas de dados relatados neste capítulo têm como base ilustrar a importância do *backup*, como instrumento de arquivo seguro, para as organizações. A seguir citaremos os referidos casos, com análises, confrontando a prática com a teoria.

6.1 Caso – Incêndio no Instituto Butantan

As informações apresentadas sobre o caso do incêndio do Instituto Butantan, foram publicadas no site de notícias Ultimo Segundo em 17/05/2010.

O Instituto Butantan é uma instituição pública estadual, subordinada à Secretaria de Estado da Saúde de São Paulo. Fundado em 1901, o Instituto Butantan é um centro produtor de vacinas e um importante centro de pesquisa biomédica em nível mundial.

No dia 15/05/2010 o Instituto Butantan passou por um incêndio, o qual comprometeu parte do acervo da coleção de registro de serpentes. Conforme os pesquisadores, o conhecimento adquirido, registrado e catalogado em mais de 100 anos de história e pesquisas foram expostos. Os arquivos em papel foram consumidos pelas chamas, dentre eles estão arquivos referentes aos livros, que tinham sido copiados e arquivados e material didático que seria encaminhado às escolas.

Foram recuperadas as informações de 42 livros, cujos originais estavam armazenados em local distante da área atingida pelo fogo, entretanto 03 (três) livros não foram localizados. O acervo digitalizado também pode ter sido perdido. Uma funcionária estava catalogando digitalmente documentos, livros e projetos científicos. O trabalho, que não estava concluído, poderia diminuir o impacto do incidente, uma vez que, os pesquisadores não precisariam recomeçar as pesquisas e projetos do zero.

6.2 Caso – Incêndio no Cemitério Parque de Goiânia/Goiás

As informações apresentadas, sobre o caso do incêndio do Cemitério Parque, foram extraídas da matéria publicada no site de notícias O Popular, no dia 21 de maio de 2014.

O Cemitério Parque de Goiânia foi inaugurado em 1961, um ano após o decreto de criação da Central de Óbitos de Goiânia. O Cemitério Parque ocupa uma área de 4 alqueires e meio e possui cerca de 260 mil jazigos, sendo o maior cemitério público da capital de Goiás.

No dia 20/05/2014 o cemitério foi acometido por um incêndio, supostamente criminal. A sala de arquivos, no prédio da administração, a qual era armazenava basicamente autorizações de sepultamento de 1970 até 2011, reformas e construções de jazigos, as quais estavam em dezenas de pastas plásticas acomodadas em prateleiras de madeiras. Todas as autorizações de sepultamento dos últimos 41 anos foram destruídas no incêndio.

Com a ocorrência do incêndio, tornou-se difícil estimar o número total de sepultados porque a cada dez anos há rotatividade. Os jazidos possuem de duas a três gavetas, sendo que há casos de até dez sepultados em cada jazido. Com o incêndio a administração terá dificuldades também para atender casos de exumação exigidos pela Justiça ou até mesmo de acionar legalmente aqueles que cometem irregularidades no cemitério. A queima do arquivo também pode prejudicar as investigações sobre desaparecidos da ditadura militar, como também os corpos de quatro vítimas do acidente com o césio-137, sepultados neste cemitério, em caixões de chumbo em meio a protesto de populares e políticos.

A administradora tranquiliza os proprietários de jazigos perpétuos no Cemitério Parque, uma vez que os títulos de perpetuidade ficaram à salvos em outro local longe do incêndio.

A vulnerabilidade dos arquivos dos quatro cemitérios públicos da capital foi percebida pela Secretaria Municipal de Assistência Social (SMAS), responsável por

sua administração. A guarda municipal, atualmente em greve, por falta de efetivo só faz a segurança nesses locais durante o dia. Para os assessores da SMAS, somente a digitalização dos documentos vai garantir a sua perenidade.

6.3 Caso – Ataque Terrorista ao *World Trade Center*

As informações apresentadas sobre o ataque terrorista ao WTC foram extraídas da matéria publicada no site de TI Especialistas, no dia 09 de novembro de 2012 e do site do *Wikipedia*.

O *World Trade Center* (WTC) era um complexo de sete edifícios, inaugurado em 4 de abril de 1973, localizava-se em *Manhattan*, no coração de *New York*. As duas construções mais famosas do conjunto eram as Torres Gêmeas.

Em 11 de Setembro de 2001, acontecia um das maiores tragédias da humanidade, as quedas das torres gêmeas do WTC, provocadas por dois atentados terroristas.

Logo após o momento do atentado às Torres Gêmeas, diversas empresas de diversas áreas de atuação, que estavam lotadas nas torres, passaram pelo mesmo problema imediato, os quais foram: primeiro, encontrar os empregados sobreviventes e, segundo, recuperar os dados para colocar a empresa novamente em operação.

Algumas empresas possuíam *backup* remoto em *Data Centers* localizados em outros estados ou mesmo países, e essas com um plano de recuperação e execução da reconstrução de dados, puderam ser remontadas em outros locais e retomaram suas atividades em um tempo relativamente pequeno e com danos mínimos, entretanto outras empresas não possuíam *backup* de seus dados em outro local fora das torres, o que resultou na perda de todas as suas informações, com prejuízos irreversíveis e posterior decretação de falência.

O episódio ocorrido em 11 de setembro de 2001 no WTC, em *New York* é um dos exemplos que mostra o quanto é importante para as organizações preservarem a segurança dos dados e informações através de *backup*.

6.4 Caso – Perda de Dados no Brasil – Perda Financeira

As informações apresentadas sobre perda de dados no Brasil foram extraídas da matéria publicada no site Momento Editorial, no dia 04 de dezembro de 2014.

Entre dezembro de 2013 e dezembro de 2014, as empresas brasileiras tiveram um prejuízo estimado em US$ 26 bilhões com perda de dados e tempo de inatividade não planejado.

Dos recursos perdidos pelas empresas brasileiras, US$ 2,8 bilhões são referentes à perda de dados e US$ 24,1 bilhões decorrentes do tempo perdido com problemas na área tecnológica. 46% das empresas brasileiras tiveram tempo não planejado de inatividade dos sistemas e 26% relataram perda de dados.

O EMC *Global Data Protection Index* mostrou que apenas 9% das 125 empresas brasileiras pesquisadas estão no mais “alto grau” de práticas de proteção de dados, mas como adotantes e não líderes. E 91% estão desatualizadas nessa área. Ainda revela que 61% das organizações não têm plano de recuperação de desastres para cargas de trabalhos emergentes e apenas 4% têm planos para ambientes de *big data*, nuvem híbrida e dispositivos móveis. Além disso, 62% não estão muito confiantes em conseguir uma recuperação total após uma interrupção.

6.5 Análises dos Casos

Após a apresentação dos casos podemos perceber a importância de armazenar dados e informações para todas as corporações, sejam de pequeno, médio ou grande porte.

No caso do incêndio do Instituto Butantan, a simples digitalização dos arquivos com a devida armazenagem dos dados digitais em local diferente do local de origem dos dados e informações originais (registros e livros de pesquisas armazenados em

papel no prédio incendiado), poderia ter protegido todos os retornos provenientes dos investimentos e conhecimentos adquiridos ao longo de aproximadamente 100 anos de pesquisas biomédicas. Outro ponto perceptível, conforme a reportagem, é que a digitalização dos documentos não estava completa, o que corresponde à definição incorreta da periodicidade de *backup*, ou seja, a política de *backup* estava propícia à melhoria, uma vez que o *backup* existente não garantiu a recuperação completa de todos os dados e informações que foram perdidos durante o incêndio.

No caso do incêndio no Cemitério Parque de Goiânia, de forma similar ao incêndio no Instituto Butantan, a digitalização de todos os documentos da sala de administração do Cemitério, poderia servir de base para recuperação de todas as informações sobre sepultamentos e outros, cujas mídias de armazenamento (papel) foram consumidas pelas chamas. Neste caso específico, a gestão do cemitério, sequer se preocupara em ter *backup* das informações dos clientes, nem mesmo em outra mídia física (papel), que poderia ter sido armazenado em outro local isolado e seguro, longe do local de armazenamento dos registros originais.

O caso da perda de dados provenientes do ataque terrorista às Torres Gêmeas do WTC é um dos mais conhecidos e comentados em todo o mundo. Uma grande parte das empresas, que funcionavam nas Torres Gêmeas, não respeitou uma das regras básicas que são definidas na política de segurança da informação, quando se refere ao *backup*, ou seja, o local para armazenamento das cópias dos dados e informações. O aconselhável é que as cópias das informações sejam armazenadas à distância mínima de 10 Km dos dados de origem. No caso em questão, a maior parte dos *backups* de uma das torres, estavam armazenados na outra torre Gêmea. Impensável que as duas torres poderiam cair quase que simultaneamente, porém, aparentemente os terroristas não somente pensaram como as derrubaram dessa forma. O que levou à falência de grande parte das empresas situadas nas torres e consequentemente gerou uma crise financeira em várias áreas do mercado americano e internacional, dado que o WTC correspondia a um dos maiores centros comerciais do planeta no ano de 2001.

O caso da perda de dados no Brasil como um agravante de perda financeira, corresponde ao fato de que, várias empresas brasileiras tratam o *backup* com descaso, não atentando para a política do mesmo, uma vez que não realizam

auditoria da política, para identificar se há aspectos que possam ser corrigidos para garantir, caso seja necessária, a reposição de informações *backupeadas* de forma que as mesmas estejam disponíveis, íntegras e confidenciais, ou ainda, que a tecnologias dos *softwares* e *hardwares* de *backup* estejam em perfeito funcionamento e não obsoletas para atender a política definida para uma corporação.

7 METODOLOGIA

Com relação à classificação da pesquisa, em conformidade com os pressupostos de Vergara (2003, p. 46), há dois critérios básicos para pesquisa, quantos aos fins e quanto aos meios. Quantos aos fins a pesquisa pode ser exploratória, descritiva, explicativa, metodológica aplicada e intervencionista. Neste caso em particular a metodologia utilizada para a realização deste trabalho é indutiva com procedimento monográfico de caráter descritivo.

A pesquisa de natureza básica trouxe uma perspectiva do tema, através do olhar de observação dos pesquisadores, cuja experiência e a vivência no dia-a-dia, associadas aos fundamentos teóricos, possibilitou uma compreensão clara e objetiva da importância da realização do *backup* para segurança de dados e informações em ambientes corporativos.

Esta pesquisa de caráter bibliográfico e qualitativo constituiu-se em fontes primárias para fundamentar a revisão de literatura, com levantamentos em artigos científicos, apostilas de cursos de TI e eletrônica e sites de empresas da área de TI e sites de notícias.

8 CONSIDERAÇÕES FINAIS

No cenário atual, em que as empresas dependem cada vez mais dos recursos de TI, para garantirem acesso e geração de novos dados e informações, no tempo exigido pela demanda do mercado, almejando a continuidade e ampliação de seus negócios, é vital garantir a segurança adequada dos dados e informações que estão presentes no ambiente corporativo.

O *backup* é um recurso imprescindível para garantir ou mitigar os efeitos da perda de dados e informações em qualquer ambiente, independente da causa da perda. Para isso, é necessário o estabelecimento de uma política de *backup* que garanta a integridade, disponibilidade e confidencialidade de todos os dados e informações considerados críticos para o funcionamento do negócio de uma corporação.

O uso do *backup* em ambientes corporativos ainda é tratado sem a devida importância, de forma equivocada, e até mesmo com desdenho, muita das vezes por falta de tempo ou até mesmo ciência da importância desse recurso, por parte dos gestores das corporações.

Com base nos aspectos técnicos de *backup* foi possível avaliar que a política de *backup* pode utilizar modos, tipos e infraestruturas de *hardware* e *software* diferentes, buscando a melhor eficácia e melhor custo-benefício para implementação do recurso em um dado ambiente, visto que as consequências, no detrimento do uso de *backup,* podem ser incalculáveis, com prejuízos que podem ir além do financeiro, atingindo clientes, fornecedores e sociedade, o que pode impactar diretamente na integridade moral da empresa, podendo levá-la, muitas das vezes, à falência.

REFERÊNCIAS

ALMEIDA, Fernando. ***Backup* Diferencial e *Backup* Incremental**. Disponível em <http://fernandopsalmeida.*blogspot*.com.br/2011/11/*backup*-diferencial-e-*backup*-incremental.html/> Acesso em 23 de novembro de 2015.

Associação Brasileira de Normas Técnicas. Tecnologia da Informação – **Técnicas de Segurança** – Código de Prática para a Gestão da Segurança da Informação. NBR ISO/IEC 17799. Segunda edição 31.08.2015 (Válida a partir de 30.09.2005), 2005.

CARDOZO, Glauco. **Administração de Redes de Computadores**. Apostila da Matéria de Administração de Redes de Computadores – Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina – Campus São José, Santa Catarina, Brasil, 2006.

FERREIRA, Wanise. **Perda de dados e tempo de inatividade causam prejuízos de US$ 26 bi a empresas brasileiras**, 2014. *Site* de notícias Momento Editorial. Disponível em <http://www.momentoeditorial.com.br/inovacao/2014/12/perda-de-dados-e-tempo-de-inatividade-causam-prejuizo-de-us-26-bi-a-empresas-brasileiras/> Acesso em: 09 de dezembro de 2015.

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

GONÇALVES; Marcos Rogério, GOUVEIA; Sônia Mara, PETINARI; Valdinéia Sonia. **A Informação como produto de alto valor no mundo dos negócios**, 2008. Disponível em: <http://revista.crb8.org.br/*index*.php/crb8digital/*article/viewFile*/42/43/> Acesso em 21 de novembro de 2015.

INNARELLI, Humberto Celeste. **Preservação de Documentos Digitais**. Apostila do Arquivo Central do Sistema de Arquivos – Agência para Formação Profissional – UNICAMP/AC/SIARQ/AFPU – Universidade Estadual de Campinas, Campinas, São Paulo, Brasil, 2003.

MACEDO, Diego. ***Backup*: Conceito e Tipos**, 2012. *Site* do Diego Macedo. Disponível em: <http://www.diegomacedo.com.br/*backup*-conceito-e-tipos//> Acesso em: 20 de novembro de 2015.

MORAES, Eliana Márcia. **Planejamento de *Backup* de Dados**. Dissertação (Mestrado em Gestão e Desenvolvimento Regional) – Departamento de Economia, Contabilidade e Administração, da Universidade de Taubaté, Taubaté, São Paulo, Brasil, 2007.

MOUTA, Rui Miguel Amorim da. **Ferramentas e Estratégias de *Backup* e Manutenção em Ambientes *Heterogéneos***. 31 f. *Projecto* - Computadores e Sistemas - Engenharia de Informática, Instituto Superior de Engenharia do Porto, Portugal, 2002.

Página da ferramenta de *backup Amanda*. ***Amanda Network Backup***. Disponível em: <www.*amanda*.org/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup Arcserve*. ***Arcserve® Backup***. Disponível em: <*http://www.arcserve.com/br/products-solutions/products/server-backup-software*.aspx/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup Bacula. **The Bacula® Open Source Network Backup Solution***. Disponível em: <http://www.*bacula*.org/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup Cobiansoft.* ***Cobiansoft***. Disponível em: <www.*cobiansoft*.com/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup Comodo**. Get Comodo's Free Backup & Online Cloud Storage***. Disponível em: <https://*backup.comodo*.com/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup EaseUs.* ***EaseUs Make your life easy!***. Disponível em: <*http://br.easeus.com/backup-software*/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup MaxFocus.* ***MaxFocus™ From LogicNow***. Disponível em: <https://www.*maxfocus*.com/*backup*/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup SyncBack Pro.* ***SyncBackPro* V7.5.5.0**. Disponível em: <http://www.*2brightsparks*.com/*syncback/sbpro*.html/> Acesso em: 17 de novembro de 2015.

Página da ferramenta de *backup Virtos*. ***Virtos***. Disponível em: <https://www.*virtos*.com.br/> Acesso em: 17 de novembro de 2015.

Página *Dan-Scientia* no *Blogspot*. **O Que São Dispositivos de Armazenamento**, 2010. Disponível em: <http://dan-*scientia.blogspot*.com.br/2010/07/o-que-sao-dispositivos-de-armazenamento.html/> Acesso em: 20 de novembro de 2015.

Página do fabricante *Ascomp.* ***Ascomp Software GMBH***. Disponível em: <http://www.*backupmaker*.com/> Acesso em: 17 de novembro de 2015.

Página InfoCP. **Dispositivos de Armazenamento de Dados**, 2013. Disponível em: <https://infocp.*wordpress*.com/armazenamento/> Acesso em: 22 de novembro de 2015.

POZZER, Cesar Tadeu. **Dispositivos de Armazenamento**. Apostila (Introdução à Informática) – Departamento de Eletrônica e Computação – DELC. Universidade Federal de Santa Maria – UFSM, Santa Maria, Rio Grande do Sul, Brasil, 2006.

SANT'ANA, Fábio Eduardo Queiroz. **Solução profissional de *Backup e Restore***. Monografia (Bacharelado em Ciência da Computação) – Curso de Ciência da Computação, Faculdade de Jaguariúna, Jaguariúna, São Paulo, Brasil, 2008.

Site da Cofre Digital. **Causas de Perda de Dados**, 2014. Disponível em <http://cdsb.com.br/apresentacao_parte001.php/> Acesso em 26 de novembro de 2015.

Site de Notícias O Popular. **Fogo leva 41 anos de registros em cemitério**, 2014. Disponível em: < http://www.opopular.com.br/editorias/cidades/fogo-leva-41-anos-de-registros-em-cemit%C3%A9rio-1.552614/> Acesso em: 09 de dezembro de 2015.

Site de Notícias Último Segundo IG. **MP vai investigar incêndio no Instituto Butantan,** 2010. Disponível em: http://ultimosegundo.ig.com.br/brasil/sp/mp-vai-investigar-incendio-no-instituto-butantan/n1237623577872.html/> Acesso em: 09 de dezembro de 2015.

Site Significados. **Significado de *Backup* – O que é *Backup***, 2012. Disponível em: <http://www.significados.com.br/*backup*/> Acesso em: 16 de novembro de 2015.

Site TI Especialistas. **Por que cuidar bem dos dados de sua empresa?**, 2012. Disponível em: <http://www.tiespecialistas.com.br/2012/11/porque-cuidar-bem-dos-dados-de-sua-empresa/> Acesso em: 09 de dezembro de 2015.

Site Wikipedia. ***World Trade Center***. Disponível em: <https://pt.*wikipedia*.org/*wiki*/*World_Trade_Center*/> Acesso em: 09 de dezembro de 2015.

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.

VERGARA, S. C. **Projeto e relatórios de pesquisa em administração**. Atlas Editora. São Paulo, Brasil, 2003.

VIEIRA, Sylvio. **Codificação para o Armazenamento da Informação**. Apostila de Curso de Graduação (Sistemas de Informação - CPT303). Centro Universitário Franciscano – Unifra, Santa Maria, Rio Grande do Sul, Brasil, 2012. Disponível em: <http://www.ebah.com.br/content/ABAAAgsE8AB/codificacao-armazenamento-informacao/> Acesso em: 22 de novembro de 2015.

ÍNDICE ONOMÁSTICO