ATLANTE
Cuadernos de Educación y Desarrollo (2ª Época)

Febrero 2018 - ISSN: 1989-4155

IMPLEMENTAÇÃO DE BACKUP COMO PROCESSO DE SEGURANÇA DA INFORMAÇÃO

Jesus, Guilherme Bindi Alencar.
Analista de Sistemas (Unianchieta). Analista de TI.
Rua Professor Benedito Loureiro de Lima, 236, Jardim Esplanada, Jundiaí - SP, CEP 13202-120, 0xx11 4587-5138, guilherme.bindi@gmail.com.

Juliano Schimiguel.
Professor no Centro Universitário Padre Anchieta, na Universidade Cruzeiro do Sul, e na Universidade Nove de Julho, schimiguel@gmail.com.

Para citar este artículo puede utilizar el siguiente formato:

Jesus, Guilherme Bindi Alencar y Juliano Schimiguel (2018): "Implementação de Backup como processo de segurança da informação.", Revista Atlante: Cuadernos de Educación y Desarrollo (febrero 2018). En línea:

http://www.eumed.net/2/rev/atlante/2018/02/backup-seguranca-informacao.html

RESUMO

O trabalho surgiu com o intuito de demonstrar, dentro do cenário corporativo a importância dos planos de continuidade de negócio, com foco na importância de cópias de segurança. O objetivo deste trabalho é demonstrar qual a melhor estratégia a ser adotada atualmente para a realização do backup. Foram pesquisadas diferentes estratégias, técnicas e equipamentos a fim de, por meio de estudo de caso, avaliar os aspectos positivos e negativos para determinar qual a melhor opção, levando em consideração a infraestrutura utilizada e disponível. Como resultado preliminar do trabalho, identificou-seque a falta de infraestrutura na internet brasileiradificultando a utilização do backup em nuvem.

Palavras-Chave: backup, continuidade de negócio, backup em nuvem.

ABSTRACT

The purpose of this work was to demonstrate the importance of business continuity plans within the corporate scenario, focusing on the importance of backup copies. Through the study, the objective of this work is to demonstrate the best strategy to be adopted for the backup. Different strategies, techniques and equipment were researched to achieve case study, to evaluate the positive and negative aspects to determine the best option, taking into account the infrastructure used and available. As preliminary results of the work, we identified that the lack of internet infrastructure in Brazil makes it difficult to use the cloud backup.

Keywords: backup, business continuity, cloud backup.

1.INTRODUÇÃO

Com o ganho de experiência, nota-se cada vez mais que existem diversos aspectos que precisam evoluir. Observou-se que por mais disseminada que as técnicas de backup estejam dentro das empresas, existem diversos aspectos que precisam ser revistos ou adicionados no pensamento dos gestores.

De acordo com Laudon e Laudon (1999) cada vez mais as organizações necessitam dos sistemas de informação para reagir aos problemas e oportunidades no ambiente dos negócios globais.

Sistema de informação é um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral. Estes interagem entre si para processar a informação e divulga-la de forma adequada em função dos objetivos da organização.

Segurança da Informaçãoestá relacionada com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem. Diferente de como comumente é interpretado, não se trata de uma ferramenta, mas sim de um processo, um conjunto de técnicas e ferramentas que utilizados pelosanalistas e usuários torna o ambiente seguro.

Atualmente, a técnica de backup está disseminada nas empresas na área de TI, pois garante ao gestor que, em caso de falhas, arquivos corrompidos, excluídos ou alterados indevidamentepossam ser facilmente recuperadoscaso a infraestrutura de backup tenha sido bem planejada.Segundo a GDSolutions (2016) O principal objetivo de um backup é a cópia de dados para restauração em caso de perda, alteração não autorizada ou danos a algum tipo de arquivo ou sistema digital.

O cenário de segurança nas empresas vem mudando nos últimos anos, decorrente do fato da informação estar ganhando mais importância para os gestores de um negócio, aumentando seu valor. Ademais, as ameaças de ataques hackers e vírus em ascensão, ocasionam a evolução das técnicas de segurança e backup nas empresas. Fazcom que as empresas tenham que evoluir suas técnicas de segurança e backup.

Para a realização deste trabalho foram pesquisados diversos artigos e livros sobre segurança da informação, voltado para backup. O objetivo geral deste trabalho é a análise de diferentes metodologias de backup, sendo elas em fita magnética e em nuvem, para analisar qual a melhor estratégia visando custo, tempo e benefícios.

2.SISTEMAS DE INFORMAÇÃO

Sistema de informação é um conjunto de elementos como pessoas, dados, atividades ou recursos em gerais. Através da interação, eles devem processar e gerar informações de acordo com o cenário onde estão aplicados e configurados.

Dentro de uma empresa existem diferentes necessidades de informação, sendo que cada área de atuação tem uma, com isso, existem diferentes tipos de sistemas de informação, neste trabalho será discutido o SAD (Sistemas de apoio a decisão).

“Um sistema computacional que auxilia o processo de tomada de decisão” Finlay (1994).

Definido mais especificamente como “um interativo, flexível e adaptável sistema de informação, especialmente desenvolvido para apoiar a solução de um problema gerencial não estruturado para aperfeiçoar a tomada de decisão. Utiliza dados, provê uma interface amigável e permite ao tomador de decisão ter sua própria percepção” Turban (1995).

O SAD – Sistema de apoio a decisão, tem como objetivo, auxiliar no planejamento estratégico, fornecendo informações para solucionar problemas organizacionais rotineiros, com o gerenciamento de dados específicos. O programa surgiu da necessidade de maior eficiência ocasionada pela competitividade de mercado.Resultando na necessidade de maior obtenção informacional atualizada da organização, rapidamente.

Segundo Popovic et al. (2012), os sistemas de BI (*Business Intelligence*) podem ser definidos como informação de qualidade em armazéns de dados bem estruturados, acoplados a softwares com interfaces amigáveis fornecendo aos trabalhadores do conhecimento acesso oportuno, análise efetiva e uma apresentação intuitiva da informação correta, habilitando-os a tomar ações ou decisões corretas.

Podemos interpretar o BI como sendo um SAD, em que seu principal objetivo é trazer para o gestor de forma simples, eficiente, rápida e segura, dados da organização que estão armazenados de maneira separada como o processo executado, o histórico da organização, transformando em informação para gestores, como montando um gráfico da quantidade de vendas por mês, o faturamento da empresa, possibilitando ao gestor a tomadade decisões ou montagemde estratégia.

Para todo sistema um dos principais critérios é a quantidade, e mais importante ainda a qualidade das informações geradas por ele. O sistema precisa gerar informações de acordo com a empresa, focada em seu ambiente de negócio, estratégia e no tempo certo, pois de nada adianta uma informação atrasada ou antiga.

Quando mais sistemas existem dentro da empresa, mais difícil é analisar, monitorar e gerenciar todas as informações, pois elas são geradas separadamente, o que gera a necessidade de um outro sistema apenas para realizar a comunicação entre os demais. Atualmente as empresas estão utilizando um sistema conhecido como ERP – Sistema de planejamento empresarial, que modela e automatiza os processos de negócio atendendo a maioria ou todos os níveis da empresa.

Segundo Haberkorn (2016), ERP (*Enterprise Resource Planning* ou Planejamento de Recursos Empresariais) é um software de gestão empresarial que busca automatizar suas rotinas,possibilitando a empresa um ambiente de integração entre todas as operações.Com o objetivo de fornecer suporte à tomada de decisão, e criar uma gestão empresarial profissional, o sistema

possibilitando antever cenários, otimizar recursos e potencializar as chances de sucesso de uma organização.

Através da tecnologia modular, dispõe de ferramentas integradas que informam dados únicos para cada departamento. Auxilia a organização oferecendo aos gestores, uma visão estratégica e detalhada de todos os processos e resultados que estão ocorrendo na organização, permitindo a correta distribuição de recursos e otimização de processos.

Abaixo está uma tabela contendo algumas vantagens e desvantagens dos ERPs.

Tabela 1 – Vantagens e desvantagens de um ERP para a empresa.

Vantagens	Desvantagens
Ajudar na comunicação interna;	Alto custo com customização e implementação;
Agilizar a execução de processos internos;	Implementação demorada.
Diminuir a quantidade de processos internos;	Risco de prejuízo ou queda de desempenho com erros inesperados do sistema;
Evitar erros — em cálculos de tributos e pagamentos, por exemplo;	Possíveis problemas com suporte e manutenção caso o fornecedor do software seja vendido ou encerre suas atividades;
Ajudar na tomada de decisões;	Dependência, que pode dificultar as atividades da empresa quando o sistema fica, por algum motivo, indisponível;
Auxiliar na elaboração de estratégias operacionais;	Adaptação e treinamento por parte de funcionários podem demorar mais tempo que o esperado;
Agilizar a obtenção de dados referentes a determinados cenários;	Resistência ao novo por parte de funcionários, em caso de implementações ou atualizações;
Diminuir o tempo de entrega do produto ou serviço ao cliente;	O sistema pode exigir mudanças em determinados aspectos da cultura interna da empresa;
Ajudar a lidar com grandes volumes de informação;	A longo prazo, as atualizações e acréscimos de módulos podem tornar o sistema mais complexo que o sistema inicial.
Evitar trabalho duplicado;	Ao longo do tempo, atualizações e acréscimos de módulos podem tornar o sistema excessivamente complexo ou lento.
Fazer a empresa se adaptar a mudanças de mercado ou legislação.	Dependência do fornecedor – ele pode descontinuar a sua versão de ERP sem aviso prévio;
Qualidade e eficácia;	Riscos de erros inesperados do sistema;
Redução de custos;	Possíveis problemas com atualizações, suporte e manutenção, caso o fornecedor do software seja vendido ou encerre suas atividades;
Extinção da redundância de atividades;	Treinamento da equipe de TI pode demorar mais tempo que o esperado;
Otimização do fluxo da informação e eficiência dentro da organização;	Resistência a novas implementações e atualizações;
Redução dos limites de tempo de resposta ao mercado;	A solução pode não oferecer a relação custo-benefício esperada;
Redução das incertezas do Lead Time ou tempo de aprovisionamento;	
Redução de estoque;	
Redução da carga de trabalho, já que atividades repetitivas podem e devem ser automatizadas;	
Melhoria do controle das operações da	

empresa.	

Fonte – https://www.mega.com.br/erp/ e http://www.ernestohaberkorn.com.br/o-que-e-erp/

A busca decorrente da competitividade empresarial, direciona os gestores a adquirirem sistemas que possibilitem o maior controle e gerenciamento de todas as áreas da empresa.Os sistemas de informação têm por finalidade auxiliar os gestores nas tomadas de decisões por meio dos dados que foram coletados, processados e entregues.

Tabela 2 – Importância de um sistema de informação na empresa.

Importância dos sistemas de informação gerencial para as empresas
Reduz os custos das operações
Disponibiliza um melhor acesso às informações, propiciando relatórios mais precisos e rápidos, com menor esforço
Melhoria na produtividade, tanto setorial quanto global
Estímulo de maior interação entre os tomadores de decisões
Melhoria na estrutura organizacional, para facilitar o fluxo de informações
Redução do grau de centralização de decisões na empresa
Melhoria na adaptação da empresa para enfrentar os acontecimentos não previstos.
Melhoria na estrutura de poder, proporcionando maior poder para aqueles que entendem e controlam o sistema

Fonte-http://www.administradores.com.br/artigos/academico/a-importancia-dos-sistema-de-informacao-gerencial-para-as-empresas/78358/

Segundo Lacombe e Heiborn, as decisões podem ser divididas em duas categorias: programadas e não programadas.As programadas ocorrem de maneira frequente, são as decisões tomadas durante reuniões, ou então sobre pequenos problemas do dia a dia. No entanto, as não programadas são decisões novas, sem precedentes anteriores, que requerem uma análise mais avançada. Muitas destas decisões são de nível estratégico, que envolvem decisões que terão impacto de médio e longo prazo para a empresa.

Os sistemas de informação, dentro das organizações, podem ser separados em 3 diferentes níveis.

- O nível estratégico, é onde são definidos missão, visão, valores e crenças.Onde são definidos os fundamentos estratégicos da organização, para curto, médio e longo prazo.
- O nível tático tem como objetivo o de desdobramento das estratégias impostas pelo nível estratégico, definindo como será realizado o caminho para o comprimento do objetivo.

- O nível operacional é voltado para a mão de obra, pois para que os objetivos impostos sejam cumpridos é necessário que alguém o faça. Ele é voltado para o acompanhamento e gerenciamento dos funcionários.

Para as empresas, a execução correta de suas atividades, é de vital importância. Compreender a aplicação das áreas de sistemas de informação nas empresas, sobretudo, as organizações precisam utilizar de softwares para alcançar decisões rápidas e corretas, devido ao mercado competitivo,fazendo a empresa alcance bons resultados.

Quando a empresa tem uma estrutura sólida, os sistemas de informação só têm a agregar em sua gestão empresarial durante as tomadas de decisões.

3.SEGURANÇA DA INFORMAÇÃO

Há muito tempo a informação se tornou um dos patrimônios mais importantes para as empresas,e como tudo que apresente valor, ela precisa ser protegida. Antigamente, com o grande uso de mídias impressas, a segurança estava na parte física, voltada para quem teria acesso ao local que contém a informação. Todavia, com a evolução das tecnologias, cada vez mais temos as informações salvas de forma digital seja em um arquivo PDF ou dentro de um sistema, como os ERPs. Os ativos das organizações passaram a estar acessíveis de todo o mundo, pela internet. Quando não ocorre o devido tratamento da segurança dessas informações, podem ocorrer fraudes como o uso ilegal de informações pessoais.

> *Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*
> *E pode ser obtida através da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. ISO 17799 (2005) pag. IX.*

Segundo Moreira (2008) para uma eficaz segurança da informação dentro de uma organização devemos ficar atentos para algumas questões como uma boa análise de riscos, a definição da Política de Segurança e por fim um plano de contingência. Segundo Médice (2013)*O primeiro passo a ser observado é que não existe risco zero.*

Para melhor compreendermos o que devemos buscar em uma solução, deve-se entender que não existe a ferramenta perfeita ou mágica. Existem diversos recursos que podem ser utilizados.

A segurança, diferente do que muitos acreditam, não é uma ferramenta, mas sim um comportamento e controle de todos que manipulam a informação, seja a pessoa responsável por inserir os dados no sistema ou o gestor que irá utilizar delas para tomar as decisões da organização. Há empresas, que limitam o acesso dos funcionários a equipamentos que possibilitem a captura de imagens, a fim de garantir a segurança da informação, outras empresas restringem o acesso as impressoras apenas aos gestores além das que se preocupam apenas com acesso que o usuário possui no sistema. De diversas formas, podemos notar que empresas adotam não apenas ferramentas, mas metodologias e costumes para garantir a segurança das informações.

Segundo a Alerta Security, a segurança da informação pode ser dividida me 3 tópicos ou bases;

- **Disponibilidade**: Garantir que as informações estejam disponíveis a qualquer momento para os usuários autorizados.
- **Confidencialidade**: É o sigilo da informação, estabelecendo níveis de acesso.
- **Integridade**: É disponibilizar as informações na mesma forma que foram gravadas.

Segundo Gazet (2010)ransomwares fazem um uso intensivo da criptografia de arquivos como um meio de extorsão, eles criptografam vários arquivos nos discos rígidos da vítima antes de pedir um resgate para que os arquivos sejam descriptografados

Segundo o relatório de junho 2017 divulgado pela Symantec, apenas em 2016, houveram 1209 violações, um total de 463,841 ataques deransomware e101 diferentes ransomwares, em comparação com apenas 30 no ano de 2015 para o ramo empresarial.

Um relatório divulgado no final de 2016 pela Trend Micro, mostrou que 2016 em comparação com 2015 teve um crescimento de aproximadamente 172% em ameaças de ransomware. Um vírus conhecido por criptografar os dados e solicitar um resgate para entregar os arquivos.

> *Segundo a CERT.br, A ação dos crackers (indivíduo que pratica a quebra de um sistema de segurança de forma ilegal) consiste em utilizar o ransomware para criptografar os dados dos usuários. Em seguida, fazem contato por e-mail exigindo o pagamento de resgate.*
>
> *A única proteção realmente efetiva contra o ransomware é proteger os dados fazendo backups periódicos.*

Caracterizado pelo modo operante do ransomware, de realizar a alteração do próprio arquivos, ao invés de impedir o acesso a ele, existem apenas duas alternativas para recuperar os arquivos sem realizar o pagamento, realizar a descriptografia, o que pode demorar um tempo indeterminado, ou restaurar o arquivo. Isso seria voltar uma cópia realizada em um local diferente, como pendrive, HD externo, nuvem.

3.1Continuidade do negócio

Segundo a ISO 17799, o plano de continuidade do negócio tem como objetivo, impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitosde falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.Através de diversas formas, é possível realizar o planejamento do plano de continuidade do negócio.

Segundo Hosni existem diversas ameaças que precisam de atenção, como intrusos, spam, engenharia social, ataques físicos, malwares, sniffing e scanning. E existem diferentes estratégias

para se proteger de cada um sendo elas educar os usuários, autenticação, firewall, sistemas de detecção de intrusos e criptografia.

É necessário para a organização, que disponha acesso do maior número possível deles, para dispor de um menor tempo e impacto sobre os usuários.

Segundo Teles, empresas que pensam na frente, planejam para a maioria dos desastres que podem acontecer, e não se arriscam, realizando desta forma um plano de continuidade. Contudo, não existe um procedimento especifico para atingir o plano ideal de continuidade do negócio. Teles propõem algumas etapas para direcionar a montar a melhor solução.

Tabela 3 – Etapas para desenvolver um plano de continuidade de negócio.

Etapas	Descrição
1. Desenvolver uma política geral de continuidade de negócios	Escrever uma política que entregue e guie os passos necessários para desenvolver o Plano de Continuidade de Negócios, e onde quem assine tenha autoridade para com toda a organização.
2. Conduzir uma Análise de Impacto de Negócios	Identificar as funções críticas e sistemas e permitir a organização priorizar dentre estas as suas necessidades reais. Identificar as vulnerabilidades, ameaças e calcular os riscos
3. Identificar controles preventivos	Uma vez as ameaças conhecidas, identificar e implementar os controles e paliativos para reduzir o nível de risco da organização em uma maneira econômica.
4. Desenvolver estratégias de recuperação	Formular métodos para garantir que sistemas e funções críticas possam ser trazidas de volta ao normal rapidamente.
5. Desenvolver um plano de contingência	Escrever os procedimentos para como a organização pode continuar funcionando em caso de um estado crítico.
6. Testar o plano e conduzir treinamento e exercícios	Testar o plano para identificar deficiências no Plano de Continuidade de Negócios e também conduzir treinamento para que os indivíduos estejam preparados para cumprir suas tarefas.
7. Manter o plano	Efetivar que os passos seguidos garantam que o documento esteja regularmente atualizado.

Fonte - https://www.tiespecialistas.com.br/2011/12/continuidade-de-negocios/

4.BACKUP

Segundo Pulia (2016), backup é uma apólice de seguro contra a perda de dados. Uma empresa depende das informações para sobreviver com seus negócios. Se as informações são extraídas de mensagens eletrônicas (e-mail), bases de dados, pesquisas e desenvolvimento, ou mesmo dados não estruturados (arquivos em Word, Excel, PDF).

O propósito do backup é criar uma cópia do dado em uma mídia secundaria. Esta cópia é armazenada e guardada para uso futuro caso o dado original tenha sido perdido, destruído, corrompido, atacado por vírus ou até mesmo sequestrado.

Podemos citar como objetivos do backup:

- Recuperação após desastres
- Arquivamento
- Backup Operacional
- Recuperação após dados corrompidos
- Estar em conformidade (compliance)

4.1 Definição e importância do backup

Segundo a empresa GDSolutions, o principal objetivo de um backup é a cópia de dados para restauração em caso de perda, alteração não autorizada ou danos a algum tipo de arquivo ou sistema digital.

Pode-se então utilizar uma frase muito comum,*"quem tem um, não tem nenhum"*que descreve muito bem um ambiente de informações digital.

Devido ao grande número de fatores que podem, de algum modo corromper a informações, seja através de vírus, falhas humanas como alteração indevida do arquivo ou exclusão acidental, queda de energia ao salvar o arquivo. E, o crescente uso computacional, temos cada vez mais dados cruciais para a organização, sendo financeiro, contábil, recursos humanos, área de atuação da empresa, sendo ela prestadora de serviço, produção, revenda. A perda dessa informação pode levar a multas, perda de clientes e até ao fechamento do negócio, dependendo de sua relevância.

> *Uma pesquisa feita pela empresa EaseUs mostrou que 44% das perdas de dados ocorreram por ações sem intenção, como apagar arquivos ou partições erradas, má colocação de cartões de memória ou ataque por vírus. Já 32% ocorrem por ações intencionais (como a formatação do disco rígido) e 21% por falhas (no software, HD ou energia, além de corrupção dos sistemas de arquivo do banco de dados). Active Solution (2017).*

O backup é uma estratégia de continuidade do negócio. Para garantir que independente do problema enfrentado, seja um simples arquivo corrompido, um banco de dados corrompido ou até mesmo a destruição da sede da empresa por incêndio ou enchente. Com o backup é possível

continuar com as atividades da empresa quase que instantaneamente, dependendo dos recursos disponíveis.

Empresas de pequeno e médio porte, apresentam preconceito e indisposição, contra medidas de backup, devido a sua natureza de ser criada, com a intenção de nunca usar. Criando um gasto não compreendido em um orçamento pequeno.

4.2 Dispositivos de backup

Segundo a GDSolutions, as estratégias mais utilizadas para backup são:

- HD EXTERNO
- FITA MAGNETICA
- SERVIDOR LOCAL
- SERVIDOR EM NUVEM

Tabela 4– Vantagens e desvantagens das estratégias de backup.

Estratégias	Vantagens	Desvantagens
HD	Mais portátil	Mais fácil de ser perdido, extraviado ou danificado.
FITA MAGNÉTICA	Um dos mais baratos e com grande capacidade	Lentas, complicada para voltar apenas parte do backup e precisa de um lugar para ser armazenado (Ocupa grande quantidade de espaço físico.).
LOCAL	Mais segurança, privacidade para as informações	Alto custo de instalação e requer mão de obra bem qualificada.
NUVEM	Baixo custo, alta escalabilidade, segurança e pode ser acessada de qualquer lugar (geograficamente) que tenha internet.	Dependem de conexão com a internet, possibilidade de ter os arquivos vazados devido a interceptação da linha de comunicação ou roubo de informações.

Fonte - https://gdsolutions.com.br/seguranca-da-informacao/entenda-a-importancia-do-backup-para-empresas/

Podendo ser divididos em duas categorias:

- ***Manual:*** Consiste na cópia manual dos arquivos. Como a cópia para um pendrive, um HD externo, ou computador ou na nuvem.
- ***Automática:***É a solução mais indicada para empresas. Requer um investimento financeiro para a aquisição de espaço e ferramentas, porém minimiza os riscos ao replicar os arquivos para um ambiente diferente.

Devido à popularidade, será discutido mais especificamente de duas estratégias, uma manual e uma automática, sendo elas backup em fita magnética e backup em nuvem.

4.2.1 Fita Magnética

Foi o primeiro meio de armazenamento de dados removível amplamente utilizado.Possui um dos melhores custos benefícios do mercado.

Podemos citar como vantagens ser uma das mídias de armazenamento mais baratas do mercado, apresentar confiabilidade (quando seguido o procedimento de armazenamento) e

segurança, pois está dentro do ambiente físico da empresa, podendo ser gerenciado por quem obtiver acesso.

E como Desvantagens estar sujeita a desgastes (necessário manter o registro de uso para descartá-las após o fim da vida útil), apresentar acesso aos dados de forma sequencial (Mais lento que os demais), possibilitar apenas um gerenciamento local, apresentar um custo dos equipamentos alto (unidade de fita) e requer uma boa análise de crescimento para garantir a compra do melhor equipamento tanto para a presente necessidade quanto para a futura, sendo ela normalmente de acordo com a garantia do equipamento.

Devido o grande risco de haver um problema com a fita, muitas empresas optam por realizar duas cópias para deixar armazenada. Fazendo com que não seja o ideal para pequenas empresas por causa do custo.

4.2.2 Backup em nuvem

Uma das mais novas técnicas de backup utilizadas, surgindo pelo grande crescimento da computação em nuvem, vem ganhando grande fatia do mercado, devido a sua simplicidade, custo e alta escalabilidade.

Falando de maneira estrutural, backup em nuvem é feito da mesma forma que o backup em servidor, porém é apresentado como forma de serviço para o usuário. Ao invés de comprar toda a estrutura necessária, é possível “alugar”, contratando o serviço e pagando apenas pelo consumo.

Podemos citar como vantagens o baixo custo de implementação, o auto nível de escalabilidade, a simplicidade de gerenciamento e possibilitar um gerenciamento remoto.

E como desvantagens dependerdiretamente do link de internet e o alto risco de violação, devido ao fato de estar disponível online.

4.3 Tipos de backup

4.3.1 Backup Completo

O backup completo, se trata de realizar uma cópia exata de todos os arquivos. Guardar todas as informações em uma cópia. É a mais comum quando falamos sobre backup.A primeira coisa que é pensada é em uma cópia idêntica de todas as informações e dados.

Ele é utilizado como ponto de início para todos os demais backups. Todos dependem do último backup completo realizado para conseguir restaurar os arquivos.

Tem como vantagem a facilidade para localizar arquivos que precisem ser restaurados. Porém apresenta como desvantagens o tempo, é o mais demorado e tamanho, como realizar uma cópia completa, requer sempre uma grande capacidade de armazenamento.

Este tipo de backup consiste um uma cópia de todos os arquivos, mesmo que eles não tenham sido alterados desde o último backup. Podendo com o decorrer da semana, realizar o backup do mesmo arquivo várias vezes sem ele ter sofrido nenhum tipo de alteração. Isso faz com que um backup de 5h com 100gb, sendo que seria necessário apenas 1h com 20gb. Devido a isso foram criados os backups incrementais.

4.3.2 Backup Incremental

O backup incremental primeiramente verifica se o arquivo sofreu algum tipo de alteração, caso não, ele ignora o arquivo, mas caso tenha ele realiza o backup. O backup incremental deve ser utilizado juntamente com o backup completo, por exemplo, um backup completo na sexta feira, com um backup incremental no demais dias da semana.

Tem como vantagem ser mais rápido que o backup completo, pois cópia apenas os arquivos que sofreram alterações, o espaço de armazenamento e o tempo de backup. Porém apresenta como desvantagens a restauração de um arquivo, é necessário procurar a cada backup incremental realizado para ver qual a última versão dele, para restaurar todos os arquivos, é necessário restaurar o backup completo, e todos os incrementas subsequentes e para restaurar os arquivos gastará mais tempo, pois precisará restaurar mais de um backup.

4.3.3 Backup Diferencial

O backup diferencial da mesma forma que o backup incremental, copia apenas os arquivos que foram alterados desde o último backup. Porém, ele mapeia as alterações com relação ao último backup completo realizado.

Como o backup é feito com base nas alterações do último backup completo, a cada alteração, o backup vai aumentando de tamanho de forma progressiva.

Tem como vantagens ocupar menos espaço que o backup completo e ser mais rápido que o backup completo. Porém apresenta como desvantagens vários arquivos que foram alterados desde o último backup completo serão copiados repetidamente.

Diferente do backup incremental que realiza o backup a partir do último backup feito, ou seja, caso tenha feito 3 backups incrementais após o backup completo, serão necessários todos os arquivos para realizar a restauração. O backup diferencial, realizar o backup a partir do último backup completo realizado, fazendo com que apenas dois arquivos sejam necessários, um backup completo e o último backup diferencial. Isso faz com que a restauração seja mais rápida, porém com o tempo faz com que o tamanho do backup vá ficando cada vez maior. Até a realização de um novo backup completo.

4.4 Estratégias de backup

Dentro do cenário de backup, podemos utilizar de diversas estratégias diferentes para a obtenção do mesmo resultado, podendo, desta forma, aproveitar ao máximo a estrutura disponível para a realização do backup. Dentre elas, podemos citar:

- DAB (Direct-Attached Backup) os dispositivos de armazenamento são conectados diretamente ao servidor.Sua vantagem é a rapidez do backup e o funcionamento simplificado. As desvantagens são a desorganização no armazenamento, custo elevado ao utilizar vários servidores com necessidade de várias unidades de fitas, dificuldade de compartilhar unidades de mídia e duplicação de dados semelhantes quando utilizado múltiplos servidores (NAIK, 2003).

Muito utilizado para modelos de backup em nuvem, pois cada servidor contém um client, que fica responsável por realizar o backup de seus arquivos.

- LBB (LAN Based Backup) ou NAS (Network Attached Storage), os servidores e os dispositivos de backup utilizam a LAN de forma compartilhada. Possui a vantagem da redução de custos. No entanto, as operações de backup elevam o volume de dados na LAN, necessitando segregar este tráfego de backup em segmento de LAN separado (NAIK, 2003).

Muito utilizado em backup em fita, pois devido ao custo, costuma-se ter apenas uma unidade para realizar o backup. Trabalhando com uma aplicação, que realiza a transferência dos dados de cada servidor para o servidor de backup onde está conectada a unidade de fita.

> *Define-se como Recovery Time Objetive (RTO) a quantidade máxima de tempo que um processo de negócios baseados em TI pode estar indisponível antes do início de consequências inaceitáveis a uma organização (perdas financeiras, impacto na satisfação do cliente, reputação, etc.).*
>
> *O tempo de retenção é o período de tempo em que os dados devem ser mantidos intactos antes da exclusão ou passar para outro nível de armazenamento para fins de arquivamento. A janela de backup é o período de tempo adequado para executar um procedimento de backup, sem prejuízo da aplicação (ISMAIL et al., 2013).*

Pode-se através da união das diferentesestratégicas otimizar ao máximo o ambiente de backup. Por exemplo, onde, no cenário de backup o servidor de arquivo apresenta a maior carga e tamanho e tempo, se pode reduzir através da técnica de DAB, em que a unidade de fita ficaria ligada diretamente nele para garantir um melhor desempenho e gerir um maior fluxo dos dados, mantendo os demais na técnica LBB, transmitindo os arquivos para serem guardados na fita.

5.CENÁRIOS DE BACKUP

5.1Cenário atual

A empresa atua na área de construção civil, dispõe de uma estrutura simples, porém robusta e eficiente. Atualmente, dispõem da construção de 4 condomínios além de sua matriz, sua central de atendimento ao cliente (CAC) e 5 plantões de venda posicionados em Jundiaí, Várzea Paulista, Vinhedo e Cabreúva.

A central de atendimento ao cliente é ligada diretamente com a matriz por meio de de rádio, utilizando toda sua infraestrutura, como internet, rede e servidores. Nas obras, existe uma internet que permite o acesso à rede VPN da empresa, em que é possível utilizar todos os sistemas através de Terminal Service. Cada obra utiliza um servidor para armazenar, gerenciar e copiar os arquivos em rede, possibilitando a todos, um acesso simultâneo e seguro aos usuários, sem comprometer a segurança dos arquivos. Nos plantões, possui uma conexão com a internet, que possibilita o acesso aos sistemas disponíveis via WEB.

A empresa dispõe de um cenário simples de backup que está descrito na tabela abaixo.

Tabela 5– Composição do backup atual.

Backup	Tamanho (Gb)	Tempo
BANCO DE DADOS MEGA ERP	29,53	7m 0s
BANCO DE DADOS WISE (Sistema de RH)	3,06	49s
BANCO DE DADOS SIECON (Antigo ERP)	1,25	26s
BANCO DE DADOS DIARIO E AXIAL	3,37	3m 5s
APLICAÇÃO DO MEGA ERP	4,31	4m 41s
SISTEMAS DE ARQUIVOS	433,15	6h 21m 53s
SISTEMA E BANCO DE DADOS DE CHAMADOS	7,14	2m 35s
COMPLETO	481,88	6h 40m 38s

É utilizada uma unidade de fita LTO 3, que não apresenta a possibilidade de múltiplas fitas para a realização do backup, tendo que ser armazenado em apenas 1 fita. Utiliza do ArcServer para o gerenciamento do backup e usa de uma estratégia LBB, pois o servidor responsável por realizar o backup não está conectado com nenhum dos itens citados na tabela acima.

5.2 Cenário Proposto

Segundo Moraes (2007), para um ambiente ser realmente seguro quando lidamos com backup, precisamos ter todas as informações da empresa presente, independendo de sua periodicidade. Pois apenas desta forma, poderemos voltar a operar da mesma forma que antes da perda dos dados.

Após análise da infraestrutura da empresa, foram propostas mudanças para melhor adequação a estrutura utilizada na empresa, adicionando todos os dados que não estavam presentes nos backups.

Tabela 6–Composição proposta para o backup.

Backup	Tamanho (Gb)	Tempo

BANCO DE DADOS MEGA ERP	29,53	7m 0s
BANCO DE DADOS WISE (Sistema de RH)	3,06	49s
BANCO DE DADOS SIECON (Antigo ERP)	1,25	26s
BANCO DE DADOS DIARIO E AXIAL	3,37	3m 5s
APLICAÇÃO DO MEGA ERP	4,31	4m 41s
SISTEMAS DE ARQUIVOS	433,15	4h
SISTEMA E BANCO DE DADOS DE CHAMADOS	7,14	2m 35s
HD EXTERNO MARKETING	368	2h 24m
HD EXTERNO ENGENHARIA	75	17m
HD EXTERNO PROJETOS	107	30m
DROPBOX	177,34	55m
ACTIVE DIRECTOR	19,1	10m
COMPLETO	1228,25	8h

Para um melhor desempenho do sistema, é essencial a utilização dos sistemas DAB e LBB, garantindo que a maior carga de trabalho esteja diretamente conectada com a unidade de fita e os demais sejam transferidos através da rede.

6.PROPOSTAS DE BACKUP

Agora serão apresentadas duas propostas distintas de backup que podem ser implementadas na empresa para suprir a atual necessidade, e projetada para suprir a demanda durante um período de aproximadamente 5 a 10 anos, variando de acordo com o crescimento da empresa.

Atualmente, é utilizada uma unidade de fita magnética que possibilita o uso de apenas 1 fita por backup, não sendo possível a utilização de fitas numeradas para a execução a empresa dispõe de uma unidade Dell PowerVault Lto3, onde é possível realizar o backup de até 400Gb por fita.

Porém conforme demonstrado anteriormente na tabela do cenário atual do backup, ela não está mais suprindo essa demanda, gerando a necessidade de finalizar o backup manualmente através da cópia para outra mídia dos arquivos restantes.

A estratégia de backup atual da empresa consiste na realização de um backup completo diário, mantendo todos os dados da empresa descritos no item 5.1. O armazenamento é realizado da seguinte maneira: O backup diário é guardado por um período de 30 dias, o backup semanal,realizado na sexta feira, é guardado por um período de 6 meses, o backup mensal é guardado sem data limite.

6.1 Backup Local

Junto a Dell Inc. foi realizo um orçamento para a aquisição dos equipamentos necessários para a realização do backup. Sendo eles a unidade de fita, a placa controladora para conectar a unidade no servidor. As fitas foram cotadas separadamente devido a diversidade de fornecedores disponíveis.

Tabela 7–Equipamentos necessários para backup local.

Produto	Valor
Controladora HBA externa SAS 12Gbps, Low Profile	R$ 1.307,68
Dell PowerVault LTO 5	R$ 18.767,30
Dell PowerVault LTO 6	R$ 19.243,99

Os itens descritos acima, foram cotados diretamente com a empresa Dell Inc. com um prazo de entrega de 30 dias.A empresa já dispõe de um servidor para conectar a unidade de fita, por esse motivo o mesmo não foi cotado.

Foi realizada a cotação de unidades de fita LTO 5 e LTO 6, sendo mostrado apenas o valor médio do produto.

Tabela 8–Comparação de custo das fitas magnéticas

Fita LTO 5	Fita LTO 6
R$ 180,00	R$ 200,00

Com a finalidade de suprir a atual demanda da empresa, foram verificadas as características das unidades de fita.

Tabela 9–Comparação das unidades de fita LTO5 e LTO6.

Dell PowerVault LTO 5	Dell PowerVault LTO 6
Tecnologia LTO-5 que permite capacidade de até 1.5Tb	Capacidade para até 2.5TB nativa por cartridge
Leitura e gravação compatíveis com mídiaLTO-4 e mídia LTO-3 compatível somente leitura	Compatibilidade de leitura/gravação com a mídia LTO-5 e a compatibilidade de leitura com LTO-4.
Taxa de transferência e taxa de backup Máximas, original: 140 MB/s; 504 GB/h	Performace de 576 GB/hora (160 MBps) taxa de transferência de dados nativos
Cabo de força C13/C14, 12A, 4 metros de comprimento	Cabo de força C13/C14, 12A, 4 metros de comprimento
Cabo 6Gb Mini para HD-Mini SAS, 2 Metros	Cabo 6Gb Mini para HD-Mini SAS, 2 Metros
3 anos de garantia ProSupport com atendimento on-site no próximo dia útil	3 anos de garantia ProSupport com atendimento on-site no próximo dia útil

Conforme informado na tabela acima, a unidade de fita LTO 5, possui compatibilidade de leitura com a fita LTO 3, atualmente utilizada na empresa. Porém a LTO 6 não, o que se torna um problema devido ao fato de “perder” todos os backups existentes, ou gerando um custo para a realização de cópias destes backups, como por exemplo, a realização de transferência do backup das fitas LTO 3 para a LTO 6.

Para a transferência dos backups seria utilizada a estratégia de copiar o backup semanal dos últimos 3 meses, com os backups mensais dos últimos 6 meses, um backup anual dos dados anteriores a estes segundo o modelo da tabela abaixo.

Tabela 10–Plano de transferência dos backups antigos.

Fitas	Backups
Fita 1	Backup das últimas 6 semanas
Fita 2	Backup das 2 semanas restantes Backup dos últimos 4 meses
Fita 3	Backup dos últimos 2 meses restantes Backup dos últimos 4 anos
Fita 4	Backup dos últimos 10 anos
Fita 5	Backup dos últimos 20 anos

Desta forma, se teria um custo de 5 fitas para se atualizar todo o backup. Mas gera um grande trabalho para os responsáveis do backup, devido ao fator de gerar a necessidade de voltar as fitas de backup uma a uma para poder gerar o novo backup.

As fitas LTO 3 não seriam descartadas, continuariam armazenadas para uma possível necessidade. Assim como a unidade de fita.

Seguindo a mesma estratégia de backup, podemos prever um custo médio de 3 fitas por semana, pois o backup seria realizado da seguinte maneira.

Tabela 11–Descrição de fitas da semana.

Dias da semana	Fitas
Segunda-Feira	Fita 1
Terça-Feira	Fita 1
Quarta-Feira	Fita 2
Quinta-Feira	Fita 2
Sexta-Feira	Fita 3

Posteriormente, de acordo com a necessidade, seria preciso a utilização de uma fita LTO 6 por dia, devido ao tamanho do backup.Existe a possibilidade de realizar uma alteração no backup, removendo itens como o dropbox do backup diário e realizando apenas no backup semanal,adiando a necessidade de utilizar uma fita por dia.

Sendo armazenada a fita de sexta-feira pelo mesmo período já armazenado, 30 dias para o diário, 6 meses para o semanal e o mensal continuaria a ser guardado sem data limite.

Para a realização/gravação do backup é necessário um sistema de gerenciamento de backup. Utilizando o ARCServer, a ideia seria de aproveitar as licenças e apenas complementar o restante. Atualmente, temos os valores conforme a cotação realizada com Geneses Consulting Comercio e Assessoria LTDA.

Tabela 12–Custo licenças ArcServer.

Licenças	Valor
CA ARCserve Backup for Windows - 1 Ano Enterprise Maintenance Renewal	$ 181,23
CA ARCserve Backup Client Agent for Linux	$ 94,27

Descrito no cenário apresentado, seriam necessárias 9 licenças para Windows e 1 para Linux, sendo separados da seguinte maneira.

Tabela 13–Distribuição das licenças do ArcServer.

Backup	Plataforma
BANCO DE DADOS MEGA ERP	LINUX
BANCO DE DADOS WISE (Sistema de RH)	WINDOWS
BANCO DE DADOS SIECON (Antigo ERP)	WINDOWS
BANCO DE DADOS DIARIO E AXIAL	WINDOWS
APLICAÇÃO DO MEGA ERP	WINDOWS
SISTEMAS DE ARQUIVOS	WINDOWS
SISTEMA E BANCO DE DADOS DE CHAMADOS	WINDOWS
HD EXTERNO MARKETING	WINDOWS
HD EXTERNO ENGENHARIA	
HD EXTERNO PROJETOS	
DROPBOX	WINDOWS
ACTIVE DIRECTOR	WINDOWS

Para a implementação do sistema local na capacidade de fita LTO 6, se preparando para o crescimento da empresa, teria-se um custo inicial de aproximadamente R$ 31.453,03 para a aquisição da unidade de fita, 20 fitas, o sistema de backup com os *clients* e a placa de conexão da unidade com o servidor. Tendo o custo adicional de aproximadamente 200 reais por fita.

6.2 Backup em Nuvem

Diferente do backup local, o backup em nuvem trabalha de maneira mais simplificada. Para a pesquisa deste trabalho, foi utilizado o Azure da Microsoft,porém o princípio de backup é o mesmo para diferentes plataformas que podem ser utilizadas, como Amazonws, ArcServer UDP, IBM BlueMix.

Através da ferramenta Azure calculator (2017), se pode simular quais seriam os valores para o mesmo cenário de implementação apresentado anteriormente. Lembrando que para a implementação do backup em nuvem, não existe custo inicial, pois sistema para backup é fornecido pela Microsoft, basta instalar e configurar.

Tabela 14–Custo periódico de backup em nuvem.

Tipo de backup	Quantidade Mensal	Redundância	Quantidade Anual	Valor Mensal	Valor Anual
Diário	22	LRS	66	R$ 5.106,26	R$ 15.318,78
	22	GRS	66	R$ 8.051,20	R$ 24.153,60
Semanal	4	LRS	24	R$ 928,41	R$ 5.570,46
	4	GRS	24	R$ 1.463,85	R$ 8.783,10
Mensal	1	LRS	12	R$ 232,10	R$ 2.785,20
	1	GRS	12	R$ 365,96	R$ 4.391,52
Total	27	LRS	102	R$ 6.266,77	R$ 23.674,46
	27	GRS	102	R$ 9.881,02	R$ 37.328,30

As redundâncias representam LRS(armazenamento com redundância local) e GRS(armazenamento com redundância geográfica).

A Microsoft oferece um serviço de suporte para os usuários, com um valor de R$96,28/mês.

E diferente do cenário encontrado para o backup local, para o armazenamento em nuvem, temos um agravante.Ele depende do link de internet disponível para realizar o backup, já que os arquivos serão transferidos para a nuvem,o que não pode ser esquecido para o cálculo do custo. Dentro do cenário da empresa, temos um custo de aproximadamente 7 mil reais com dois links de internet dedicado (30 Mb/s de download e upload).

Realizando um cálculo médio, dizendo que o link dedicado entrega em sua média 20Mb/s, e colocando ele apenas para subir os arquivos,pode-se dizer que possui uma capacidade de aproximadamente 70Gb/h. Caso ele entregue os 30Mb/s teria uma capacidade aproximada de 105Gb/s. O que é uma capacidade baixa, considerando que existem aproximadamente 1Tb de backup.Ultrapassariam 10h para a realização do backup.

Assim como na estratégia local, é possível alterar as técnicas de backup, para reduzir o custo do backup. Tem-se dados que não são atualizados diariamente, como os contidos nos HDs externos. Esses poderiam estar apenas no backup semanal, reduzindo o backup para aproximadamente 600 Gb, que, além de reduzir o tempo para a realização do backup, também diminuiria o custo. Ao invés

de 232 reais, teria-se um custo diário médio de 131 reais, conseguindo reduzir o custo anual para algo aproximado de 15000 reais.

7.ANÁLISE E DISCUSSÃO

Após a análise de diversos itens, aspectos e infraestruturas, é possível dizer que existem diversos aspectos positivos e negativos referentes a cada metodologia e estratégia de backup.

Pode-se citar para backup em nuvem, segundo a EcoIT, como sendo aspecto positivo a alta escalabilidade, devido ao fato de a cada momento, as organizações estão gerando mais dados e informações.Isso cria uma continua mudança no cenário de backup, pois todos os dados devem ser devidamente guardados. No caso de backups em fita, é necessária uma grande, rigorosa e cuidadosa análise de crescimento, porque a aquisição de componentes caros e de recursos limitados geram uma limitação referente a ampliação dos recursos de armazenamento.

Menor custo de instalação e manutenção. Um dos aspectos que merecem mais destaque no backup em nuvem, é o fato dele utilizar de um sistema completamente automático para a realização do backup. Desta forma, o responsável de TI, tem apenas que realizar o acompanhamento diário, verificando se o backup foi realizado com sucesso. Diferente do backup em fita, que demanda além da verificação, o gerenciamento, armazenamento, manutenção e compra e descarte das mídias. Mesmo podendo realizar o agendamento do backup, a troca da fita tem que ser realizada manualmente, a cada backup realizado, e mídia de backup tem que receber o devido cuidado e armazenamento, por causa de sua fragilidade por utilizar de tecnologia magnética para manter os dados. Tem que manter com os devidos cuidados solicitados pelos fabricantes, como falta de umidade, pouca iluminação, longe de circuitos elétricos. Diferente do backup em fita, o backup em nuvem não requer nenhum investimento inicial, apenas a contratação e configuração do serviço. Lembrando que ele depende de um link de internet, que se apresenta extremamente caro no Brasil e afetará diretamente a velocidade de seu backup.

Maior controle é apresentado pelo sistema de fita, devido ao fato de ser um sistema mais completo, apresenta um maior detalhamento e configurações mais detalhadas.Como direcionar arquivos específicos ao invés de pastas, a possibilidade de executar scripts junto a operação de backup, preparando o ambiente que será copiado.Entre outros recursos, não disponíveis para o backup em nuvem, que possibilita apenas o direcionamento e configuração do tempo de armazenamento.

Muito comumente, o backup em fita é apenas uma cópia dos arquivos e dados da empresa, não contendo nenhum tipo de segurança lógica, como senha para acesso, criptografia. O backup em nuvem, dispõem de acesso restrito a conta de gerenciamento, que permite monitoramento, alertas de acesso,dispõe de criptografia para o armazenamento dos dados.Desta forma, fazendo em casos de roubo de dados, os arquivos continuem inacessíveis sem a chave de acesso.

Um dos grandes problemas presentes é o erro humano, decorrente da manipulação física nas fitas, podem ocorrer problemas como a perda de fitas, a falta de documentação pode levar a sobreposição indevida dos dados.A falta de capacitação pode levar a manipulação indevida do equipamento danificando-o, a alocação indevida da fita nas prateleiras pode gerar atrasos e perdas na recuperação de informações.

Devido as fitas terem que ser armazenadas com fácil acesso em casos de recuperação, normalmente estão dispostas dentro da empresa de forma a facilitar o manuseio, deveriam ficar presente em um local diferente, garantindo em casos de grandes desastres, como incêndios, enchentes e desabamentos, que os dados estão seguros e intactos. Para restringir acesso indevido, é necessária a criação de um sistema de segurança física, como acesso biométrico, acesso apenas com acompanhamento, câmeras, controle de temperatura, umidade. No backup em nuvem não existe esta preocupação, os dados são acessados através da internet, sendo realizado o controle, através do sistema de gerenciamento, tendo a senha apenas o responsável e seu superior.

Para o cenário de restauração, existem divergências, pois dependendo do tipo, um leva vantagens sobre o outro. Para restaurações completas, em que todos os arquivos foram perdidos, como o caso de queima de um HD, ou pane no servidor. O Backup em fita é melhor, pois possui maior velocidade e está de fácil acesso. Já no backup em nuvem o tempo para download do backup influencia muito em seu tempo (varia de acordo com a velocidade de internet contratada e entregue). Em casos de backup parcial, como uma pasta deletada acidentalmente, ou uma planilha alterada indevidamente, o backup em nuvem é melhor, pois não trabalha com acesso sequencial como a fita, e o tamanho dos dados a serem armazenado é inferior. Compensando o tempo de localização da fita, leitura e restauração do arquivo.

Uma tarefa muito importante no processo de backup é o teste. De nada adianta fazer o backup e não telo quando mais precisar devido a uma falha ou problema. Desta forma o teste previne isso. A realização de testes deve ser constante e aleatória, selecionando sistemas e arquivos diferentes para sua realização. O backup local, para o teste de grandes quantidades de arquivos, banco de dados ou sistemas, é muito bom, pois sua velocidade de restauração é compensada pela grande carga de informação. Em testes menores, como sistemas secundários, pequenos controles o backup em nuvem é melhor, devido ao fato de conseguir baixar com facilidade os arquivos.

Devido ao custo, para armazenar 1,5Tb e 2,5Tb de dados em fita é de aproximadamente 180 e 200 reais, respectivamente. E segundo a calculadora Azure, o custo para armazenar estas mesmas quantidades em nuvem é de, respectivamente, 298,02 e 473,21 reais,o que demostra um custo maior.

Foi identificado que o pacote máximo entregue na localidade da empresa utilizada no estudo é de aproximadamente 100 Mb. Se tratando de um link dedicado (100Mb de download e upload) e se utilizarmos toda sua carga para o backup durante o período noturno, considerando que a empresa fecha as 18h e abre as 7h, retira-se um período de 13h para a realização do backup. Com uma transferência máxima caso não tenha oscilação é de 351,5 Gb/h com o período de 13 horas, permite apenas a transmissão de 4,4 Tb. Sabendo que a internet apresenta oscilações e que isso dependeria de um consumo completo da banda,o que é impossível, pois existem sistemas que se comunicam externamente e dependem do link de internet. Uma quantidade de 5Tb, o equivalente a 2 fitas LTO 6, que pode ser gravado em aproximadamente 12 horas (variando de acordo com a estrutura e dados a serem salvos).

Lembrando que este custo está apenas para a quantidade de armazenamento, e sabermos que o backup requer muito mais, como mão de obra qualificada, espaço de armazenamento adequado, sistemas de gerenciamento. O que equilibra o custo variando do tamanho do backup.

Se compararmos um custo da realização de backup de 1.5Tb, de 180 reais local e 298,02 reais em nuvem, reparamos que existe uma diferença de aproximadamente 120 reais.Porém se disseminar o custo inicial de aproximadamente 20.000 reais, tem-seum grande período de tempo, em que o valor seria inferior ou equivalente.

8.CONSIDERAÇÕES FINAIS

Após a realização comparativa das distintas ferramentas, pode-se analisar que tem duas estratégias completamente diferentes. Uma requer uma manutenção diária, tanto para a realização do backup, quanto para o gerenciamento, devido ao fato de ser necessária a troca e deslocamento das fitas. Já o backup em nuvem, é completamente automatizado, sendo necessária a interferência do usuário apenas para a realização dos testes e restaurações.

O gerenciamento é uma das maiores vantagens do backup em nuvem, trazendo de fato, a falta de interação do gerenciador do backup. No backup em nuvem, a interação se restringe a configuração, testes e restaurações. No backup em fita, toda ação realizada requer algum tipo de interação, para a realização do backup é necessária a troca da fita, no armazenamento, é necessário o gerenciamento. Na unidade de fita, existe a necessidade de manutenção rotineira, como a fita de limpeza do cabeçote. Por mais simples que aparente, o armazenamento das unidades de fita requer uma grande atenção e cuidado, sua durabilidade é gravemente afetada variando as condições de armazenamento, como umidade temperatura.

Para empresas que utilizam serviço na nuvem, o ambiente de backup é completamente diferente, devido a estrutura encontrada.Para empresas que assim como a utilizada no estudo, dispõem de sua infraestrutura quase que inteira local, exceções de sites, o backup em nuvem apresenta diversas vantagens dependendo do tamanho de seu backup.

Conforme imposto inicialmente para o trabalho, pode-se dizer que:

Para backup de pequeno e médio portea solução de backup em nuvem apresenta grandes vantagens, devido ao fato de seu tamanho ser pequeno. Além da vantagem de utilização do backup em nuvem, que permite a inexistência de um local para armazenamento, e a escalabilidade, aumentando gradualmente o tamanho do backup de acordo com a necessidade, não requer um custo inicial. A empresa irá adquirir o sistema para realizar o backup através do download gratuito, e irá configura-lo de maneira muito simples, apenas direcionando quais pastas da máquina deseja realizar o backup, qual sua periodicidade, sendo diária, semanal, mensal e quanto tempo o backup deverá ficar armazenado.A Azure dispõe de um período máximo de 99 anos segundo seu site.

Para backups maiores, que dispõem de uma maior quantidade de informações para ao backup, o backup em nuvem se torna inviável, devido ao tempo de realização e custo. A estrutura disponível no Brasil em relação a internet é muito precária e custosa, o backup em nuvem se torna inviável para grandes volumes de dados,por sua baixa capacidade de transferência e alto custo.

Já para infraestruturas em nuvem, se utilizada a mesma plataforma, como por exemplo tanto os servidores, quanto os bancos de dados, o backup em nuvem se torna extremamente vantajoso desde que se utilize da mesma plataforma.Pois dispõem de uma excelente infraestrutura interconectando os servidores,eliminando a necessidade de transferência de dados pela internet. Esse fator, torna o backup em nuvem a melhor opção.

Porém existe um custo muito grande envolvido pelo link utilizado.A empresa do estudo apresenta atualmente 30Mb/s, onde apenas 15 Mb/s estão disponíveis para a realização do backup, desta forma, o tamanho atual superior a 1Tb de backup não pode ser realizado dentro do período de tempo disponível, pois tem uma capacidade aproximada de 500Gb no período disponível, tornando o backup em fita a melhor solução.

Para a empresa apresentada no estudo de caso, a solução analisada que apresenta o melhor comparativo, é uma solução hibrida, envolvendo o backup local em fita LTO 6 no escritório, onde são armazenados os servidores, possibilitando uma larga demanda de armazenamento e gerenciamento, com um baixo custo, porém para as demais localidades, um serviço de armazenamento em nuvem, configurado de maneira que possibilite além da utilização de backup momentâneo em todas as obras com um simples gerenciamento através de plataforma online, mantendo uma cópia de todos os dados presentes em todas as obras no escritório. Desta forma possibilitando o backup em fita de maneira mais completa, possibilitando o armazenamento por longos períodos de tempo.

Futuramente pretende-se verificar a possibilidade de uma infraestrutura duplicada através de 2 data center em locais diferentes, para garantir que em casos de perda, não seja necessário nenhum minuto de indisponibilidade do sistema, possibilitando retorno imediato as atividades da empresa.

9.REFERÊNCIAS BIBLIOGRÁFICAS

ABDO, Rafael. Saiba como se proteger do ransomware SAMAS, o vírus temido até pelo FBI. Disponível em: <https://www.tiespecialistas.com.br/2016/05/saiba-como-se-proteger-do-ransomware-samas-o-virus-temido-ate-pelo-fbi/>. Acessado em: 07/11/2017

ALECRIM, Emerson. O que é ransonware? Disponível em: <https://www.infowester.com/ransomware.php>.Acessado em: 07/11/2017

AMADO, Wesley Ricardo. Análise do Software BSN para a Realização de Backups na Nuvem. Disponível em: <http://revistatis.dc.ufscar.br/index.php/revista/article/view/180.pdf>. Acessado em: 07/11/2017

ÁVILA, Alessandra.*A importância de fazer backup de dados em sua empresa. Disponível em: <http://www.activesolutions.com.br/blog/a-importancia-de-fazer-backup-de-dados-em-sua-empresa/>. Acessado em: 07/11/2017*

CERT.br. Ransomware: saiba como se prevenir desse código malicioso com as orientações do CERT.br. Disponível em: <https://www.tiespecialistas.com.br/review/ransomware-saiba-como-se-prevenir-desse-codigo-malicioso-com-as-orientacoes-do-cert-br/>.Acessado em: 07/11/2017

DOMINGUES, Jenifer. *A importância dos sistemas de informação gerencial para as empresas. Disponível em: <http://www.administradores.com.br/artigos/academico/a-importancia-dos-sistema-de-informacao-gerencial-para-as-empresas/78358/>.Acessado em: 07/11/2017*

ECOIT.*Por que trocar o backup em fita pelo backup em nuvem? Disponível em: <https://ecoit.com.br/blog/seguranca/backup-em-fitas-vs-backup-em-nuvem/>. Acessado em: 07/11/2017*

EITI. *Checklist: Como fazer backup corporativo. Disponível em: <https://eitisolucoes.com.br/blog/checklist-como-fazer-backup-corporativo/>. Acessado em: 07/11/2017*

FIALHO, Mozart. Guia essencial do backup. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=lang_pt&id=RP8R90IysJQC&oi=fnd&pg=PA6&dq=backup&ots=dUTbjVwqcq&sig=m1oHA7BGuZ5auobP_26-7zk-XBc#v=onepage&q=backup&f=false>.Acessado em: 07/11/2017

GDSOLUTIONS. *Entenda a importância do backup para empresas. Disponível em: <https://gdsolutions.com.br/seguranca-da-informacao/entenda-a-importancia-do-backup-para-empresas/>.Acessado em: 07/11/2017*

GDSOLUTIONS. *4 motivos para fazer backup na nuvem. Disponível em: <https://gdsolutions.com.br/seguranca-da-informacao/4-motivos-para-fazer-backup-na-nuvem/>. Acessado em: 07/11/2017*

HABERKORN, *Hernesto.* O guia definitivo sobre o que é ERP. Disponível em: <http://www.ernestohaberkorn.com.br/o-que-e-erp/>.Acessado em: 07/11/2017

ISMAIL, B. I.; MYDIN, M.; NIZAM, M.; KHALID, M. F. Architecture of scalable backup service for private cloud. In Open Systems (ICOS), 2013 IEEE Conference on (pp. 174-179), 2013.

ISO 17799 Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwiMn_Xe5azXAhXLH5AKHewbBU4QFghHMAQ&url=http%3A%2F%2Fwww.ciencianasnuvens.com.br%2Fsite%2Fwp-content%2Fuploads%2F2014%2F09%2F215545813-ABNT-NBR-177991.pdf&usg=AOvVaw3AYH1JQK6nZ_rEbMag4_1m>.Acessado em: 07/11/2017

JAMIR, Thiago. UMA ARQUITETURA DE CLOUD STORAGE PARA BACKUP DE ARQUIVOS Disponível em: <http://repositorio.ufpe.br/handle/123456789/18013.pdf>.Acessado em 07/11/2017

JUNIOR, Pereira. Plano de continuidade de negócios aplicado à segurança da informação Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15974/000695265.pdf?sequence=1>.Acessado em: 07/11/2017

MACÊDO, Diego. *Backup: Conceito e Tipos. Disponível em: <http://www.diegomacedo.com.br/backup-conceito-e-tipos/>.Acessado em: 07/11/2017*

MÉDICE, Roney. A importância da Segurança da Informação – Visão Corporativa Disponível em: <https://www.profissionaisti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/>.Acessado em: 07/11/2017

MESSIAS, João - Análise de um sistema de backup/recovery para grandes volumes de dados. Disponível em: <http://plutao.sid.inpe.br/col/sid.inpe.br/plutao/2015/12.04.12.17.16/doc/1_silva8.pdf>.

GAZET**, ALEXANDRE. COMPARATIVE ANALYSIS OF VARIOUS RANSOMWARE VIRII, FEVEREIRO 2010, DISPONIVEL EM:*<HTTPS://LINK.SPRINGER.COM/ARTICLE/10.1007%2FS11416-008-0092-2?LI=TRUE>. ACESSADO EM 19/10/2017***

MICROSOFT.*O que é ransomware?Disponível em: <https://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx>. Acessado em: 07/11/2017*

Militelli, Leonardo. Ransonware: o perigo dos softwares desatualizados. Disponível em: <https://www.tiespecialistas.com.br/2016/12/ransomware-o-perigo-dos-softwares-desatualizados/>.Acessado em: 07/11/2017

MORAES, Eliana Marcia. PLANEJAMENTO DE BACKUP DE DADOS. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjYzqfF56zXAhVHjZAKHZyHABAQFggmMAA&url=http%3A%2F%2Fwww.ppga.com.br%2Fmestrado%2F2007%2Fmoraes-eliana_marcia.pdf&usg=AOvVaw08KZHCyg23eMwPeke8ilRp>.Acessado em 07/11/2017

MOREIRA, Ademilson.A importância da segurança da informação. Disponível em: <https://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>.Acessado em: 07/11/2017

MOREIRA, Leonardo. Inclua segurança da informação no seu plano de contingência. Disponível em: <https://www.tiespecialistas.com.br/2016/05/inclua-seguranca-da-informacao-no-seu-plano-de-contingencia/>.Acessado em: 07/11/2017

NAIK, D. C. Backup and Restore - Technologies for Windows, 2003. Disponível em:<http://www.informit.com/articles/article.aspx?p=99985>. Acessado em: 23/10/2017.

PING, Y.; BO, K.; JINPING, L.; MENGXIA, L. Remote disaster recovery system architecture based on database replication technology. In Computer and communication Technologies in Agriculture Engineering (CCTAE), 2010 International Conference On (Vol. 1, pp. 254-257), 2010.

RAMALHO, Neilson Carlos Leite. Um Estudo Sobre Adoção da Computação em Nuvem no Brasil, Disponível em: <http://www.teses.usp.br/teses/disponiveis/100/100131/tde-06032013-124239/publico/Dissertacao_Neilson_Ramalho.pdf&sa=U&ved=0ahUKEwi3oM7E5KzXAhUFJ8AKHVGMCgQQFggEMAA&client=internal-uds-cse&cx=011662445380875560067:cack5lsxley&usg=AOvVaw2E_s1i0NiTcBMQW03VODDH>.Acessado em: 07/11/2017

SYMANTEC. Internet Secutiry Thread Report Vol.22 Disponível em: <https://www.symantec.com/pt/br/security-center/threat-report.pdf>.Acessado em: 07/11/2017

SYMANTEC. Relatório sobre Segurança da Informação nasEmpresas. Disponível em: <https://www.symantec.com/content/pt/br/enterprise/images/theme/enterprise-security/State-of-Security-Survey-Report-LAM-port.pdf>. Acessado em 07/11/2017

TELES, Guilherme. Continuidade de Negócios. Disponível em: <https://www.tiespecialistas.com.br/2011/12/continuidade-de-negocios/> Acessado em: 07/11/2017

TRENDMICRO. Cibercrime As a Service: Trend Micro detecta crescimento de 172% em novas famílias de ransomware. Disponível em: <https://www.tiespecialistas.com.br/review/cibercrime-as-service-trend-micro-detecta-crescimento-de-172-em-novas-familias-de-ransomware/> Acessado em: 07/11/2017