Gestão na Segurança de Dados Adotado no Instituto de Tecnologia em Informática e Informação do Estado de Alagoas – Itec

Ronaldo Ribeiro Fernandes
ronaldosmo@hotmail.com
UFAL

Ana Paula Lima Marques Fernandes
lm.apaula@gmail.com
UFAL

Resumo:A tecnologia da informação afeta a todos que trabalham com computadores ou com algum meio tecnológico que tenha como finalidade guardar dados e informações. O mais relevante dentro de uma organização não é a consequência do serviço prestado, mas as informações referidas com esse bem de consumo. O Objetivo geral dessa pesquisa foi implantar normas e procedimentos referentes à segurança das informações no Instituto de Tecnologia em Informática e Informação do Estado de Alagoas - ITEC. E os específicos foram: Analisar a política de backup do ITEC; Monitorar o armazenamento e a segurança de informações e analisar o risco econômico para a segurança. A presente pesquisa tem como sustentação a classificação metodológica que propõe os critérios essenciais: quanto aos fins e quanto aos meios. Destaca-se de uma maneira geral que o sistema de integração de monitoramento e cópias dos dados, assim como gerenciamento de riscos trás várias vantagens para as organizações e se utilizado de maneira adequada, pode ser armazenado de forma segura e ser reutilizadas sempre que necessárias.

Palavras Chave: Backup - Monitoramento - Segurança de Dados - $4 -

1. INTRODUÇÃO

A tecnologia da informação afeta a todos que trabalham com computadores ou com algum meio tecnológico que tenha como finalidade guardar dados e informações. A internet é cada vez mais acessada, devido o crescimento da globalização, causando impacto no crescimento da popularidade e por sua vez despertar nas organizações o cuidado de possuir registro de dados e suas informações.

A ciência que visa o tratamento de informações no setor público esteve agregada ao domínio sócio-político da sociedade em geral. Por décadas dependeu de grandes computadores, que carecia de especialista e solicitavam centralização do processamento, dificultando o acesso direto aos usuários. O setor da informática era a filosofia predominante destinada a conter o fluxo tributário que amparar as ações administrativas.

O papel de um modo global, atualmente, na informática vem sendo exercido ligeiramente de maneira a meditar e adaptar toda a Gestão Pública, facultando um enorme conhecimento e uma melhor fiscalização.

O mais relevante dentro de uma organização não é a consequência do serviço prestado, mas as informações referidas com esse bem de consumo. Normalmente muitas organizações reservam para certo fim o amparo de seus ativos físicos e financeiros e desprezam a segurança dos dados que possuem.

O ser humano em qualquer ocasião sempre buscou o controle sobre as informações que lhe eram mais importantes de uma maneira geral, ao longo de sua vida. O que foi alterado desde então foram às formas de anotações oficiais e armazenamento das informações. A principal maneira no passado de armazenamento de informações era através da memória humana, com o surgimento e evolução da tecnologia, muitos valores foram alterarados gerando a importância nas organizações humanas no âmbito do domínio e gerenciamento das informações.

As possibilidades de perdas em relação às informações guardadas em uma organização, segundo CARUSO e STEFFEN (2006) são agravados em sucessão geométrica à proporção que os principais dados ao gerenciamento dos negócios são centralizados. É preciso, destaca o autor, cercar o recinto de informações com regras que garantam sua segurança efetiva a um orçamento de acordo, em consequência de ser difícil atingir a segurança absoluta.

Nesse contexto quanto mais eficaz for à ferramenta computacional, relacionada à memória, capacidade de armazenamento e desempenho, os dados armazenados devem ser sempre protegidos. É um recipiente incomparável para armazenar muitas informações, em função da sua grande habilidade e capacidade. A melhor maneira de gerenciar a defesa dos dados de um sistema é realizando cópias de segurança, ou backups, com certa periodicidade.

Nas organizações que derivam de sistemas de computadores, a perda de dados representa prejuízo. Tendo esse fato no dia a dia, no qual o computador é usado como ferramenta de trabalho, ficar sem essas informações significa ausência de tempo, e ficar sem tempo, resulta na ausência de recursos financeiros e, por fim, o cliente. Em outras palavras, dependendo do porte da empresa, a carência das informações pode ter o sentido de falência.

A segurança dos dados é essencial para uma empresa ser bem sucedida. Apesar de ser prioridade da Tecnologia de Informação, não deve ser interesse somente de grandes empresas, contudo de profissionais da área de sistemas e demais usuários de computador. Quantas vezes são perdidas informações sem registros para adquiri-las novamente? Quantas vezes acontecem problemas relacionados à falta de espaço ou de mídia apropriada?

Esta pesquisa fundamenta-se em razão que os Institutos, empresas, em particular, o ITEC, necessita adotar um projeto ou modelo de gestão de segurança para preservar suas informações de encontro a diversos tipos de ameaças, ou seja, cópias de seguranças em computadores são ações fundamentais para compensar problemas advindos de hardware, como, por exemplo, falha no disco rígido, ou invasão do sistema por hackers, ataque de vírus, destruição de arquivos, conflitos no sistema operacional, etc.

Diante do abordo o objetivo geral desse trabalho é Implantar normas e procedimentos referentes à segurança das informações no ITEC. E os objetivos específicos: Analisar a política de backup do ITEC; Monitorar o armazenamento e a segurança de informações e analisar o risco econômico para a segurança.

2. CONSIDERAÇÕES TEÓRICAS

A implantação de políticas voltadas para a integridade dos dados digitais não é uma tarefa fácil. De acordo com ARELLANO (2004) é necessário que as cópias sejam realizadas de uma forma programada, visto que estão envolvidos os equipamentos para criação do procedimento, sendo limitados em termos de espaço e vida útil.

Outro fator que merece destaque, é que as empresas devem ter atenção da forma de como as informações são guardadas, não podendo passar despercebido que as mesmas serão empregadas para os próprios ou futuros gestores.

O avanço no setor da informática está proporcionando várias alterações na sociedade em geral, seja nas maneiras de comunicação ou de relacionamento. As empresas passam a ser subsidiadas por tal avanço tornando-se cada vez mais dependentes.

As informações, por estar envolvida nos meios tecnológicos, segundo COSTA et al. (2009) passam a ser acessadas por certa muitos indivíduos e de forma aleatória

O presente estudo realiza uma abordagem geral sobre backup, como também sobre como as empresas precisam comportar-se sobre cópias e preservação das informações digitais, e como mantê-las seguradas de quaisquer contrariedades que possam surgir derivada de problemas em equipamentos ou desastres de maneira geral.

2.1 A IMPORTÂNCIA DO BACKUP

As copias de segurança (backups) em computadores são de fundamental importância para reparar ou tentar sanar um grave problema que acontece com hardwares. As panes ou problemas externos que danificam as mídias ou até mesmo acaba com tudo que levou um período curto ou longo para ser conquistado são grandes malefícios para qualquer pessoa ou empresa que preze e careça bastante de seus arquivos. Com todas esses possíveis perigos as copias de segurança ou backups estão ganhando espaço na busca por garantia a arquivos relevantes, a copia de segurança é a melhor forma de prevenção e recuperação dos dados, visto que as informações podem retornar normalmente ao dispositivo quando for necessário.

É preciso solicitar sempre novas políticas e estratégicas de forma a manter as informações seguras, confiáveis, acessíveis e autênticas.

ARELLANO (2004) afirma que a implementação de políticas direcionadas para a preservação das informações digitais não são tão fácil quanto aparenta. Demanda-se que seja realizada com bastante atenção e de forma pensada, uma vez que está comprometida literalmente com equipamentos eletrônicos, os quais possuem toda uma arquitetura restringida a diversas questões, como: ao estado de aquecimento do hardware, à vida útil do equipamento, entre outras. Deve haver também a preocupação com o uso indevido ou

excessivo desses dispositivos eletrônicos, destaca o autor, visto que podem provocar danos ao ambiente de forma agravante.

Outro fator importante o qual as empresas necessitam ter responsabilidade e atenção na visão de INNARELLI (2003) é na maneira de como as informações vão ser arquivadas. As mesmas deverão ser guardadas em padrões de forma que possam ser reconhecidas e utilizadas no futuro. Tornar esse comprometimento efetivo é uma grande meta e desafio para as empresas, as quais procuram cada vez mais a menor ocorrência de incompatibilidades de equipamentos frisa o autor.

Em grandes organizações que derivam das informações e da informática a perca de arquivos ou dados representam também a perca de recursos por consequente, o cliente e/ou o emprego. O backup nada mais é que a prevenção.

Nesse contexto abordado, destaca-se a importância de gestão na área de backup como auxiliadoras no seguimento de preservação dos dados, as quais têm como meta a realização de cópias de segurança das informações do sistema de informação da empresa.

2.2 UMA ABORDAGEM GERAL SOBRE BACKUP

O armazenamento de informações é o pilar da informática. As tecnologias evoluem com imensa escala, sem dúvida o computador foi uma das grandes inovações tecnológicas do mundo atual, em visto disso, essas tecnologias interferem consideravelmente no nosso cotidiano (GARRIDO, p.1).

Atualmente a informática está em ascensão e com crescimento escalável de pessoas, ao passo que os usuários utilizam computadores, surgem os problemas. Isso leva a reflexão o quão de confiança que o computador deve usufruir para guardar informações de maneira adequada e segura, as quais são de imenso apreço para o seu responsável.

Tendo em vista o atual contexto da sociedade, a ferramenta computacional se torna indispensável para o funcionamento do mundo, por causa disso todos as pessoas devem dispor ferramentas para preencher essa carência de segurança de dados, que começaram surgir logo em meados da utilização intensa de computadores (por empresas, governos e centros de pesquisas), que trouxeram com elas a preocupação de armazenar as informações e documentos digitais de maneira eficiente e segura, o qual só seria possível por mediação de bom plano de cópias de segurança, isso porque caso os dados fossem perdidos, recorria-se à cópia de segurança mais atualizada. Se houvesse qualquer problema na restauração do backup mais atualizado, recorria-se a segunda forma mais atualizada e assim por diante, na circunstância dessas falhas continuassem a acontecer. (SANT'ANNA, 2005, p.11).

Observa-se que se faz necessário uma boa política de segurança de dados, pois isso é primordial para uma boa interação entre ser humano e computador, além de tornar o computador mais eficiente. Segundo os autores SOUZA et al., (2009, p. 02) ratificam e adicionam, relatando que Backup significa cópia de segurança, e o mesmo é de grande valor, não somente para recuperar dados de eventuais prejuízos do computador, mas também para interromper as mudanças ou inconsistências dos dados, provenientes de uma eventual infecção por vírus ou uma invasão do sistema de dados.

O atentado ao World Trade Center em Setembro de 2001, é considerado um exemplo no tocante à importância de possuir uma cópia de segurança, isso porque por causa desse desmoronamento, diversas organizações que se encontravam nesse prédio perderam todas informações de seus clientes, histórico de contas, vendas e outras informações relevantes para o funcionamento dessas empresas. Em virtude desse fato muitas empresas foram levadas a falência. Dessa maneira “[...] usufruir de cópia de informações importantes se torna cada vez

mais imprescindível, no entanto realizar cópia de segurança é algo difícil ser realizado pelo usuário do computador [...]" (RIBEIRO, 2009, p. 193).

Segundo SILVA (1999) quando se trata de segurança de informações de uma empresa, alguns aspectos devem ser considerados. O primeiro deles, o autor sugere um sistema de controle de acesso ao sistema, visando impedir a entradas de pessoas sem autorização.

2.3. REALIZAÇÃO DA CÓPIA DE SEGURANÇA

SILVA (1999) destaca que para se por em prática uma cópia de segurança, é preciso que o usuário siga algumas etapas:

- Escolha dos dados

Os arquivos que vão ser copiados devem possuir procedência confiável, ou seja, não serem infectados, pois quando a restauração for estabelecida, pode trazer uma série de problemas para o computador.

- Mídia utilizada

Há inúmeras formas para realizar um procedimento de cópia de segurança, a mesma pode ser efetuada por meios da utilização de CD, DVD, Pen-drive, Blue Ray, HD e entre outras variadas mídias que o backup pode ser realizado. A escolha de qual mídia utilizar vai depender do que está sendo armazenada, a quantidade de informações que estão sendo armazenados, os níveis de confiabilidade que essa cópia deve possuir, ou seja, para a escolha de um dado para realizar a cópia de segurança é preciso que o usuário tenha um conhecimento do que está pretendendo armazenar.

- Local de armazenamento

As cópias devem ser guardadas em um ambiente restrito e diferente do local que foi efetuado a cópia, isso devido diminuir as chances de perdas de todos os dados em caso de desastre ambiental.

De acordo com RIBEIRO (2009) há diversos métodos para realizar uma cópia secundária, dentre elas destacam-se:

- Cópia de segurança total

O método de backup total tem a pretensão de copiar os documentos selecionados e armazená-los em um ambiente seguro, esse método é muito seguro e eficaz, devido caso uma cópia de segurança vier dar problema, a cópia anterior a ela será restaurada, e assim futuramente diante caso a falha continue a persistir. No entanto esse modo de backup é muito lento e requer uma enorme capacidade de armazenamento, isso devido a cada backup que for realizado, o ultimo backup não será excluso.

- Cópia de segurança incremental

Consiste em um backup que registra somente os arquivos que foram modificados desde o último backup e irá acrescentá-los ao ultimo procedimento, esse tipo de backup requer uma pequena quantidade de memória, contudo a sua restauração é a mais lenta dentre os modos transitados.

- Cópia de segurança diferencial

O modo de cópia de segurança diferencial tem como objetivo copiar os documentos inalterados do computador, o grande mérito desse método é que, a realização do backup é feita de forma rápida e eficiente, mas esse sistema é muito vulnerável a falhas, isso pode ser explicado caso o usuário não tenha cópias dos arquivos inalterados, esse sistema de backup se tornará obsoleto.

2.4. USO DE BACKUP NAS EMPRESAS

A disputa entre as organizações está cada vez mais acirrada, visualiza-se o diferencial entre elas na maneira de como as informações são utilizadas. Elas sintonizam o mundo, comenta BARRETO (1994, p. 01). No entanto, não diferenciam somente empresas, elas mudam perspectivas, outras organizações, como ONGs e nações. Destaca-se a cada vez o acumulo de informações, muitas delas de forte importância. A grande discussão referente a essa temática é a forma como são armazenados essas informações. Diante do abordado, é possível entender a mudança que as novas tecnologias acarretam nesse mundo tão competitivo.

De maneira global, as pequenas e médias empresas não possuem sistemas informatizados, que são deslocados na maioria dos casos por maneiras rústicas de armazenamento de dados. Porém, com o pequeno custo dos computadores e o desenvolvimento de softwares de gestão integrada, os micros empresários ficam cada vez mais estimulados a investir nesse setor, a fim de se tornar mais forte frente à concorrência. A consequência é que houve um aumento enorme do uso de tecnologia nesses setores empresariais.

Um pouco diferente das pequenas organizações, o uso da tecnologia por parte das médias e grandes empresas é maciça. Teoricamente a maior parte delas faz uso em grande volume dos sistemas de ERP (Sistemas Integrados de Gestão Empresarial) e CRM (Gestão de Relacionamento com o Cliente).

Os relatórios de produção, além dos dados cadastrais de consumidores, como também das informações referentes à própria empresa são obtidos através desses sistemas. O cenário fica claro com o quanto que a relação da organização com a informática torna=se mais indissolúvel cada vez mais.

Existem tantas informações que são estratégicos para as nações. Banco de dados contendo projetos de invasão, identidade de agentes secretos, armamentos atualizados e até dados sobre a fiscalização de centrais nucleares. Informações que são alvo de ataques em todo o mundo e que podem causar desastres de grande proporção se forem perdidos.

É percebível a importância das informações para pequenas, médias e grandes empresas. O aumento dos riscos também é real com a mesma proporção do aumento da dependência tecnológica. O eventual extravio dos dados poderia enfraquecer a empresa a ponto de levá-la a falência. Em várias organizações que dependem de sistemas e de computadores, a ausência de informações representa a perda de capital (FIALHO, 2007). Nesse contexto, investir em medidas de segurança é bastante viável destaca o autor.

Quando se cogita em segurança da informação, o que surge inicialmente é que é a proteção das informações, mesmo não envolvendo o ambiente onde as informações estão armazenadas. Um computador é considerado livro de qualquer perigo se houver uma responsabilidade de que é capaz de atuar exatamente como o esperado. Todavia a segurança não é apenas esse procedimento. Todos os usuários têm a expectativa de que ao dados armazenados no computador diariamente, permaneçam, por todo tempo, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo (DIAS, 2000).

Já destacado a relevância que os dados e as informações possuem para as empresas, e que na sua grande maioria eles são armazenados em mídias, pode-se perceber que, de uma maneira geral eles são vulneráveis. A maioria dos dados é armazenada nos computadores, em seus HDs, equipamentos considerados muitos sensíveis. Como por exemplo, sensíveis às quedas de energia, à poeira, à queda, às temperaturas elevadas e até aos vírus.

Muitas vezes ocorre perda por descuido humano, adquirido por intermédio de exclusão/modificação acidental dos arquivos, existem também os ataques cibernéticos. Há a probabilidade de perda de dados por causas naturais, como inundação, incêndios, furacões e terremotos. HEDSTROM (1996) destaca que o intuito do backup nada mais é que preservar as informações e prevenção como também assegurar proteção à informação de valor permanente para acesso pelas gerações presentes e futuras

Diante do que foi exposto é importante frisar quatro etapas: a) Importância - é necessário ter conhecimento de quais são as informações importantes para a organização e se eles precisam de cópias em outro dispositivo, destaca DUARANTI (1994); b) Periocidade – baseia-se na observação dos dados, se eles foram alterados e qual o período necessário para fazer as cópias de seguranças; c) Destino – local onde serão armazenadas as informações, como também o ambiente que as mesmas serão armazenadas; d) Exame de Integridade – consiste em saber se os dados salvos possuem condições de serem utilizados em caso de necessidade.

2.5. GERENCIAMENTO DE RISCO

A concepção de perigo está relacionada com a incerteza e a variabilidade. A sua gestão envolve tudo que uma empresa fabrica ou fornece. De uma maneira geral são observados os riscos para as organizações humanas.

A evolução da tecnologia acarretou mudanças importantes nas organizações humanas. Algumas delas tiveram uma cota para uma melhoria da sociedade, enquanto outras contribuíram de forma negativa. Houve contribuições para a melhoria de qualidade de vida, outras criaram novos problemas de ordem econômica, social, política, ambiental ou de segurança e saúde. Alguns tipos de riscos são destacados:

- ALARP - As Low As Reasonably Praticable (Risco Tão Baixo Quanto Possível)

O risco pode ser considerado do tipo individual, onde está para uma pessoa presente na vizinhança de um problema, tendo em conta a gravidade deste e o período de tempo em que o dano pode acontecer. É visto como risco social está para um agrupamento de pessoas expostas aos danos decorrentes de um ou mais cenários acidentários.

Um dos principais objetivos de uma análise de riscos é *"conhecer o processo"*. Nem sempre é óbvio saber como as coisas funcionam ou o que faz com que elas não saem confirme desejado. É servir de instrumento para uma tomada de decisões para a seleção de atividade. Permite uma melhor alocação de recursos financeiros e humanos, para que as atividades sejam efetuadas dentro dos períodos determinados.

- PDCA

A utilização do ciclo PDCA é uma maneira de certificar que realmente existe a preocupação com os riscos, avaliando a eficácia deste tratamento e efetuando novas atividades quando necessário. Examinar a identificação dos perigos que podem gerar riscos e estabelecer controles envolve em tomar atitudes corretivas, o que representa obter melhoria em uma atuação constante. Dependendo da probabilidade de ocorrência, esses perigos podem influenciar em muito ou pouco o serviço, resultando na necessidade de recomeçar com consequentes perdas de tempo, mão-de-obra, materiais e acréscimo de custos.

- M.A.S.P

Por que necessitamos de um processo de solução de problemas? Visto que os problemas fazem parte do dia a dia. O processo pode ser utilizado por indivíduos e grupos, além de todas as etapas de uma organização. É um instrumento de fácil de ser utilizado. É baseada nos seguintes critérios: Identificar o problema; observá-lo; analisá-lo; atuar; segui-lo

através de fluxogramas impedindo que qualquer problema apareça em virtude do não cumprimento aos padrões estabelecidos (controle).

Os meios mais empregados para análise de riscos e perigos são:

- APP ou APR – Análise Preliminar de Perigo/Risco

A APP procura pesquisar quais são os pontos de maior risco do sistema e estabelecer uma priorização destes quando da continuação dos estudos de segurança ou de uma análise de riscos quantificada. A técnica pode ser utilizada durante as etapas de desenvolvimento, estudo básico, implantação e mesmo nas análises de revisão de segurança de uma instalação existente.

- What if – O que aconteceria se?

É uma técnica utilizada na identificação de perigos e operabilidade. Tem como meta: Determinar nos fluxogramas disponíveis os perigos presentes nas instalações, em projetos existentes; Apresentar problemas operacionais; Relatar as diferentes ações de melhoria complementares que concedam obter um nível de segurança aceitável. Recomenda-se, sempre que possível, uma vistoria às instalações. Atribui-se então o exame através de uma geração livre de questões que devem ser formuladas na forma: "*O que aconteceria se...?*".

- AAF – Análise da Árvore de Falhas (Fault Tree Analysis - FTA)

A Análise da Árvore de Falhas é denominada com este nome devido partir de um único evento, que é o acidente ou uma indesejável condição denominada evento de topo.

É uma das ferramentas mais úteis para a análise de risco. A abordagem é *dedutiva*, o que a torna adequada para examinar as condições que causaram ou influenciaram em evento indesejável. A ocorrência de um acidente é muito raro devida apenas um fator iniciante, mas sim por uma conjunção de condições. O triunfo deste método é que ele representa graficamente as relações entre os componentes do sistema, tornando-as mais óbvias.

- HAZOP – HAZard and OPerability studies

É um método sistemático de questionamento criativo e aberto que prevê uma visão completa do processo, discutindo-se qualquer parte deste para levantar como poderiam acontecer desvios e determinar quando estes podem gerar riscos. A HAZOP consiste na busca de uma análise detalhada do processo a fim de identificar os problemas operacionais através de muitas reuniões, durante as quais profissionais de várias áreas discutem o projeto/processo da instalação.

- FMEA – Failure Mode and Effect Analysis

É um instrumento preventivo que busca impedir a ocorrência de falhas no processo através da análise das falhas potencias e propostas na melhoria das ações. O objetivo é detectar falhas antes que se produza um serviço. Sua utilização diminui as chances do produto/serviço ou processo falhar, crescendo a confiabilidade. O setor automotivo utiliza muito a FMEA.

2.6. NORMAS DE SEGURANÇA (ABNT)

A ISO - "International Organization for Standardization" é uma organização que foi fundada em 1946 sediada em Genebra, na Suíça. A sigla ISO foi originada da palavra isonomia. O objetivo da ISO é criar e promover normas que possam ser utilizadas igualmente por todos os países. O Brasil é representado pela Associação Brasileira de Normas Técnicas (ABNT).

Os padrões utilizados para segurança da informação foram explicados pela ABNT recebendo a nomenclatura de NBR ISO/IEC 27001:2006 – Tecnologia da Informação –

Técnicas de Segurança – Sistema de Gestão de Segurança da Informação - Requisitos e NBR ISO/IEC 27002:2005 - Tecnologia da Informação – Técnicas de Segurança – Gestão de Segurança da Informação. Serão baseadas respectivamente por ISO 27001 e ISO 27002.

A norma ISO 27001 refere-se à quais requisitos de sistemas de gestão da informação precisam ser implementados e a ISO 27002 é um guia que orienta a utilização de controles de segurança da informação.

A Segurança da Informação é definida pela ISO/IEC 27002:2005 define como proteção da informação contra diversos tipos de ameaças para garantir o desenvolvimento dos negócios, minimizar os danos e maximizar o retorno dos investimentos e as oportunidades de negócio.

A organização deve estabelecer, implementar, operar, monitorar, analisar detalhadamente, manter e aperfeiçoar um SGSI registrado dentro do contexto das atividades de negócios globais da empresa e dos perigos que ela enfrenta. O sistema deve ser documentado, implementado, produzido, sustentado e adaptado. Ou seja, cada sistema é composto por processos que se relacionam.

Os domínios que mais se sobressaem são: Política de Segurança; Organização da Segurança da Informação; Administração de Ativos; Segurança no setor de Recursos Humanos e do Ambiente; Gerenciamento das atividades e comunicações; Fiscalização de Acesso; Desenvolvimento e Manutenção de Sistemas; Gestão da Segurança da Informação; Gestão da Continuidade do Negócio.

3. MATERIAIS E MÉTODOS

A presente pesquisa foi desenvolvida no Instituto de Tecnologia em Informática e Informação do Estado de Alagoas (ITEC) localizado na cidade de Maceió, em Alagoas.

3.1. HISTÓRICO

Em 1977, por intermédio de convênio ratificado entre a SERPO (Serviço Federal de Processamento de Dados) e o Governo do Estado de Alagoas, foi formado um núcleo de informática com o objetivo de, sob gerência do primeiro, juntar-se e organizar as atividades de processamento de dados no setor Público do Estado de Alagoas.

O Instituto de Processamento de Dados do Estado de Alagoas (IPD) surgiu em 1980, que ao longo dos 17 anos de sua existência constituiu o nome da informática pública do Estado como precursor e a coragem dos primeiros tempos aliados ao apuro técnico e a contínua inovação tecnológica oriunda da modernidade.

O ITEC foi criado no dia 30 de abril de 2002 (lei 6313). É o setor da Administração Pública, com autonomia administrativa e financeira, atrelada à Secretaria de Estado do Planejamento.

Compete-lhe: Assessorar o Secretário de Estado e Planejamento na elaboração da Política Estadual de Informática e Informação do Estado; Promover a informatização dos órgãos governamentais; Encaminhar as demandas de serviços referentes ao uso da tecnologia da informática e informação; Projetar e coordenar as ações de implantação e manutenção do Sistema Estadual; Desenvolver pesquisas, levantamento de dados e a disseminação tecnologias avançadas na área da informática e informação; Prestar pareceres técnicos e demais serviços referentes à tecnologia da informação; Desenvolver e implantar, de maneira subsidiária, os aplicativos que não sejam ofertados pelo mercado.

O Instituto de Tecnologia está comprometido nos seguintes projetos: Fábrica de Sítios; Fábrica de Sistemas; Escritório de Projetos; como também, Infovia Digital; Projeto

Alagoas Digital; Reforma Administrativa; DigitAlagoas; Expresso Livre Alagoas, CONSEGE – Conselho Estadual de Governança Eletrônica e Móvel.

3.2. MÉTODO DE PESQUISA

A presente pesquisa tem como sustentação a classificação metodológica exibida por VERGARA (2007) que propõe os critérios essenciais: quanto aos fins e quanto aos meios. Dada à abordagem do problema de pesquisa, quanto aos fins, foi escolhida à metodologia explicativa.

Um estudo é considerado explicativo quando tem por prática expressar, esclarecer determinado fenômeno. Segundo ACEVEDO e NOHARA (2007, p. 47) encontra-se o mesmo entendimento: "A pesquisa explicativa, por sua vez, tem a finalidade de explicar por que o evento acontece, ou quais os fatores que causam ou contribuem para sua ocorrência".

Quantos aos meios: foi levada em questão uma revisão bibliográfica. Segundo VERGARA (2007) a pesquisa bibliográfica é o trabalho fundamentado em artigos publicado em livros, revistas, e redes eletrônicas que podem ser acessados pelo população em geral. Foram empregados livros e artigos sobre backups, gerenciamento de dados, análise de riscos, as normas de segurança e pesquisa eletrônica; além disso, foi adotada pesquisa de campo, que segundo a autora "é investigação empírica realizada onde ocorre ou ocorreu um fenômeno ou dispõe de elementos para explicá-lo", tendo em vista a afirmação o estudo foi realizado no ITEC, local que dispõe de todas as informações para responder ao problema proposto.

3.3. AMOSTRAGEM

De acordo com VERGARA (2007) "existem dois tipos de amostra: probabilística, baseada em procedimentos estatísticos, e não probabilísticas". Conforme o objeto de estudo não foi baseado em métodos estatísticos, por sua natureza qualitativa, o evento analisado foi não probabilístico. Para compor a amostra, o ITEC foi escolhido considerando sua representatividade no setor da gestão da informação e informática em Alagoas.

3.4. COLETA DE DADOS

MARTINS (2002, p. 54) cita que "os dados e informações coletados em publicações, cadastros e fichários são considerados dados secundários e, contudo, a identificação precisa da fonte. Os dados obtidos diretamente com o informante através de questionário ou entrevista são denominados dados primários e são obtidos por instrumentos cuja cópia deve ser parte do relatório final de pesquisa". A coleta de dados confere maior clareza ao estudo, uma vez que, fornece subsídios para compreensão dos fenômenos investigados.

3.5. FORMULÁRIOS DE PESQUISA

O formulário desse estudo foi elaborado para responder os objetivos específicos, ou seja, conhecer melhor a política de recuperação de dados, backup, do ITEC. Também examinar o procedimento adotado para o monitoramento do armazenamento e a segurança dos dados, além de verificar o risco econômico para a segurança dos dados.

4. ANÁLISE DOS RESULTADOS

A política de segurança dentro de uma empresa não deve ser tratada como um tema de ponta. É importante frisar que é um conjunto de diretrizes gerais destinadas a governar a proteção das informações. O ITEC desenvolve a sua própria cultura interna referente ao gerenciamento e backup de seus dados. São demarcadas quais as metas, fixando nos objetivos que serão atendidos, com os recursos essenciais definidos, com fases e prazos estabelecidos.

A política de segurança da empresa é tratada como uma ação produzida, não somente do porteiro ao presidente, portanto é necessário frisar o setor administrativo. Cada funcionário assimila a segurança como parte da cultura do Instituto, tendo consciência do seu papel dentro da segurança e os procedimentos operacionais.

Esse estudo propõe um plano de segurança que pode ser modificada em função das ações década área. Nesse contexto é necessário expor as etapas: Classificação quanto à preservação e sigilo; Análise econômica da segurança; Inventário de usuários e recursos; Escolha dos instrumentos de segurança e registro dos documentos das ações realizadas.

É importante frisar que todo documento de Política de Segurança é necessário atender os seguintes objetivos: aparelhar a empresa com um conjunto de elementos capaz de garantir inviolabilidade dos dados; ter as ações definidas dos funcionários; tornar seguro a adequada utilização e tratamento das informações, como também responsabilizar-se pelo emprego frequente do ferramental de segurança.

As responsabilidades são classificadas de acordo com a posição hierárquica dos funcionários dentro do Instituto.

- Todos os funcionários são responsáveis pelas informações acessadas referentes aos dados da empresa;

- Os diretores devem gerenciar o cumprimento da gestão de segurança de seus funcionários, além de impedir o acesso de funcionários demissionários as informações e expor os desvios praticados com medidas corretivas apropriadas;

- Cada setor cuida das informações utilizadas em suas atividades;

- Através de identificação de acesso, os usuários farão uso das informações por autenticação e senhas secretas. Essas são sigilosas e intransferíveis. Recomenda-se que não sejam anotadas em papel ou outros meios de registro de fácil acesso.

De acordo com a ISO, Segurança da Informação é a preservação dos dados contra diversos tipos de ameaças para tomar certa a continuidade dos negócios, minimizar os prejuízo aos negócios e tornar máximo o retorno dos investimentos e as oportunidades de negócio.

O objetivo geral dessa pesquisa foi implantar normas e procedimentos, através de um manual, referentes à segurança das informações no Instituto. Essa implantação foi baseada nas normas técnicas da ABNT NBR ISO/IEC 27001:2006 de segurança.

O manual teve como objetivo estabelecer um modelo de gestão para operar, analisar, monitorar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) do Instituto de Tecnologia. A adoção de um SGSI deve ser sempre uma decisão muito importante dentro da empresa. Merece consideração frisar que a implementação da proposta no ITEC será exercida de acordo com as exigências e objetivos solicitados de segurança, processos empregado e tamanho da estrutura do Instituto.

As informações sobre backup alcançado através do questionário dialogado com o gerente de banco de dados do Instituto são destacadas a seguir:

- Os procedimentos referentes à política de backup existem, entretanto não são documentados. Como por exemplo, destaca-se a manutenção de equipamentos, gerenciamentos e segurança do ambiente;

- 85% dos backups são feitos on-line e 15% off-line;

- Os backups são feitos na modalidade full e incrementado, normalmente nos finais de semana;

- O software empregado para gestão do backup é o HP Data Protect;

- Todas as unidades, partições e diretórios fazem parte da rotina de backup;

- É utilizado o software Winclamav contra softwares maliciosos;

- Os bancos de dados existentes no ITEC são: Oracle, SQLServer, Postgree e Mysql;

- Os principais programas utilizados nos bancos de dados são: BI, Financeiro, E-mail e sistemas específicos das Secretariais;

- No momento não é disponibilizado de um site próprio de backup, como o *cold site*, *warm site* ou *hot site*;

- Cada equipe de funcionários controla o acesso à biblioteca-fonte dos programas;

- No momento, não existe processo de auditoria para maximizar a eficácia do processo de auditoria de sistemas;

- Os funcionários de cada equipe mantém um log de suas atividades. Eles tomam uma posição, por exemplo, horários de início e fim do sistema; conformam se ocorre o manuseio certo de arquivos de dados e saídas geradas entre outros;

- Quanto ao log de falhas, as falhas são registradas em logs, todavia não há um modelo para tratar as falhas reportadas;

- Não foram encontrados documentos que trata de revisão de logs de falhas para assegurar que as falhas tenham sido satisfatoriamente resolvidas;

- Existe a revisão de medidas corretivas para assegurar que os controles não foram comprometidos e que as atividades executadas foram totalmente autorizadas, entretanto essas ações não são documentadas;

- Os sistemas e técnicas criptográficas para proteção das informações, ou seja, backups criptografados atualmente não há.

Quanto às ações envolvendo recovery são destacados:

- O Instituto possui uma gestão de recovery bem determinada, entretanto não são documentadas;

- As mídias dos backups são sempre testadas, sem um intervalo de tempo fixado, com o intuito de garantir que eles são confiáveis para uso emergencial sempre quanto necessário;

- As mídias são controladas e fisicamente protegidas em um local seguro (cofre), contra danos, roubos e acessos não autorizados;

- Há procedimentos formais para manuseio de dados, por exemplo, tomar a defesa das informações contra divulgação não autorizada ou utilizações indevidas;

- Foi verificado que ocorrem procedimentos de segurança da documentação dos sistemas contra acessos não autorizados;

- Atualmente não há procedimentos formais para descarte seguro das mídias;

- Os procedimentos formais para a reutilização das mídias ocorrem baseados em software, entretanto não há documentação formal;

- A capacidade de armazenamento das mídias é de 22tb de backup e 35tb de software;

- A substituição das mídias é feita automaticamente pelo software;

- As mídias são fiscalizadas através de software e por códigos na identificação por data, hora, descrição do conteúdo.

Quanto à recuperação das informações caso aconteça algum acidente, no momento não existe nenhuma política. Por exemplo, em casos sinistros como inundação, incêndio, nenhum plano formal é executado. Destaca-se também, que não existe nenhum tempo previsto para o sistema retornar a normalidade.

Quanto ao monitoramento das informações armazenadas e sua segurança no Instituto de Informática do Estado, os métodos, as responsabilidades e as operações dos processos de dados são sempre definidas pelo gerente do setor.

Nesse contexto é importante que essas ações sejam sempre documentadas. Cada ação abrange o processamento e tratamento da informação, backup, instruções para tratamento de qualquer engano que possam surgir durante a execução de uma tarefa.

Quanto às mídias, o seu manuseio é sempre fiscalizado e fisicamente preservado. O ITEC age de acordo com as seguintes diretrizes: na ocasião que não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha ser removido do ambiente, seja requerida a autorização para remoção de qualquer mídia e mantida documentada essa remoção, como trilha de auditoria; todas as mídias são guardadas em ambientes seguros para evitar perda dos dados em virtude a deterioração das mesmas; as mídias são registradas para confinar a chance de perda das informações. Todas essas diretrizes ocorrem, entretanto convém que todos as ações, procedimentos e níveis sejam explicitamente documentados.

As mídias são descartadas de forma segura e protegida minimizando qualquer risco de vazamento de dados para pessoas não autorizadas. São feitas através de trituração, como também de remoção de dados, possibilitando ser utilizada para outra maneira dentro da instituição.

É mais fácil implementar a coleta e descarte baseado na segurança de informações de todas as mídias, do que tentar separar apenas aquelas contendo informações consideradas mais importantes.

Antes de definir a metodologia adotada para avaliar os riscos envolvidos nos processos e sistemas com o objetivo de minimizar a possibilidade de falhas no desenvolvimento, utilização de uma informação, aumentando a confiabilidade e segurança é preciso apontar um procedimento através qual o prestador de serviço pode identificar os riscos e calcular, estimar e controlar os riscos e a eficácia do controle, associados aos serviços pelo grupo fornecido. Merece consideração destacar que os requisitos serão aplicáveis a todos os estágios.

Nesse sentido a probabilidade de que cada evento indesejado ocorra é identificada na etapa de reconhecimento do perigo. Em circunstâncias apropriadas, onde os dados adequados estiverem disponíveis, é mais propícia uma disposição quantitativa. As etapas também podem ser descritivas.

São levados em consideração no ITEC os seguintes questionamentos: O perigo ocorre na ausência de uma falha? O perigo ocorre em um modo de falha? Ou somente em uma condição de falha múltipla? No tocante Á gravidade do prejuízo é preciso questionar: Qual a gravidade? Qual o tamanho do prejuízo? E qual o forte efeito que o Instituo vai suportar devido esse dano?

5. CONCLUSÃO

Quando o tema é modelo de gestão adotado na segurança de dados, percebe-se que não há futuro sem passado. Essa é a regra para as empresas que quiserem viver dia a dia sem nenhum tipo de impedimento relacionado à segurança de seus dados.

Acredita-se que o fator determinante para o bom ou mau êxito da segurança de informações de uma empresa é possuir um plano de segurança que representa todas as sentenças tecnológicas, administrativas e operacionais.

Nesse contexto abordado, o problema que a pesquisa traz é se O ITEC adota uma política adequada de backup de suas informações? Sim, o Instituto de Tecnologia segue os procedimentos exigidos em uma política de segurança, entretanto é sugerido que os mesmos sejam documentados.

No período de 4 a 11 de fevereiro (2011) a diretoria de Infraestrutura e Operações realizou simulações de Disaster Recovery envolvendo o Instituto, a Secretaria da Fazenda e a HP.

O objetivo primordial desse trabalho foi implantar normas e procedimentos referentes à segurança das informações no ITEC. O mesmo foi obtido através de modelo baseado nas normas de segurança existente no mercado. O primeiro objetivo específico baseou-se na análise da política de recuperação de dados do ITEC. Destacou-se que os procedimentos operacionais documentados precisam ser tratados através da formalização de documentos. Um fator positivo a ser destacado é que todas as mudanças são sempre autorizadas pela direção geral.

Outro ponto a ser destacado é que as cópias de seguranças das informações e dos programas são testadas, no entanto não são efetuadas regularmente conforme a política de produção de cópias definidas.

Nesse sentido, observa-se não somente a importância dos registros completos das cópias, como a documentação apropriada sobre os procedimentos de restauração da informação.

O próximo objetivo específico foi monitorar o armazenamento e a segurança de informações. Teve como fator positivo, no tocante aos procedimentos utilizados nos tratamento, processamento, armazenamento e transferência das informações onde foram considerados os seguintes itens: tratamento e identificação dos meios magnéticos; acessos restritos para prevenir o acesso de pessoas sem autorização, em outros termos, por mínima que seja à documentação do sistema será sempre autorizada pelo gerente da área; garantia que a entrada das informações seja completa; identificação eficaz de todas as cópias das mídias para atrair a atenção dos funcionários autorizados.

O terceiro e último objetivo específico resumiu-se em examinar o risco econômico para a segurança. Nessa maneira, destaca-se que a análise da perda de uma maneira geral é a forma estratégica no desenvolvimento dos cuidados dos serviços ou produtos gerados e fornecidos.

É importante frisar que a proposta de gerenciamento de risco deve fazer compor o arquivo do modelo escolhido da política de backup e de monitoramento das informações incluindo o gerenciamento de risco. Sendo assim, os critérios para aceitabilidade de risco merecem atenção na determinação da eficácia do processo de gerenciamento de risco. Outro fator importante a ser mencionado é que caso o empreendimento venha sofrer qualquer alteração, um registro das mudanças deve ser mantido no arquivo de gerenciamento de risco.

Destaca-se de uma maneira geral que o sistema de integração de monitoramento e cópias dos dados, assim como gerenciamento de riscos trás várias vantagens a sociedade e se

utilizado de maneira adequada, pode ser armazenado de forma segura e ser reutilizadas sempre que necessárias

REFERÊNCIAS

ABNT NBR ISO/IEC 24762:2009 – Tecnologia da Informação – Técnicas de Segurança – Diretrizes para os serviços de recuperação após um desastre na tecnologia da informação e de comunicação.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação - Requisitos.

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da segurança de informações.

ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.

ARELLANO, M. A. Preservação de documentos digitais. Ciência da Informação. Brasília, v. 33, n. 2, mai/ago. 2004. Disponível em: <http://www.scielo.br>. Acesso em: 20. Nov. 2010.

BARRETO, A. de A. A questão da informação. Revista São Paulo, v.8, n.4, 1994.

CARUSO, C. A.A; STEFFEN, F. D. Segurança em Informática e Informações. Editora SENAC São Paulo. 2006.

COSTA, M. M. et al. A POLITICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANALISE DA RCA 025/2009 SICOOB CREDIP. 2009. Disponível em <http://www.infobrasil.inf.br>. Acesso em: 25 Nov. 2010.

DIAS, C., Segurança e Auditoria da Tecnologia da Informação. Axel, 2000.

FIALHO, Jr., M. Guia Essencial do Backup**.** Universo dos Livros Editora LTDA. 2007.

GARRIDO, U. S. Tendências das novas tecnologias - Livro de actas – Membro da Comissão Executiva, p.01. Disponível em: <www.bocc.uff.br>. Acesso em: 25. Nov. 2010.

HEDSTROM, M. Digital preservation: a time bomb for digital libraries**.**1996. Disponível em: <http://www.uky.edu>. Acesso em: 25. Nov. 2010.

INNARELLI, H. C. Preservação de Documentos Digitais. 2003. Disponível em: <http://fatec.br>. Acesso em: 25. Nov. 2010.

MARTINS, L. A. Cloud Computing - Windows Azure**.** Revista da Ordem dos Engenheiros, número 118 - Julho/Agosto de 2010.

MONTE, A. C. e LOPES, L F. A Qualidade dos Suportes no Armazenamento de Informações. Visual Books Editora. 2004

RIBEIRO, U. Certificação linux, 2ª Edição, DK Editora, 2009.

SILVA, F. Q. B. S. Segurança de dados – Visão geral. 1999. Disponível em: <http://www.buscalegis.ccj.ufsc.br>. Acesso em: 20. Nov. 2010

SANT'ANNA, M. L. Os desafios da preservação de documentos digitais. 2002.

SOMASUNDARA, A. S. Armazenamento e Gerenciamento de Informações. Porto Alegre: Bookman, 2011.

SOUZA, F R. N; FARIA , N. M; DIAS, T. S; VIANNA, M. B. M. Desenvolvimento de um servidor de backup inteligente utilizando a linguagem shell script em linux, 2009. Disponível em: <http://www3.iesam-pa.edu.br>. Acesso em: 20. Nov. 2010.

VERGARA, S. C. Projetos de pesquisa em administração. 8. Ed. São Paulo: Atlas, 2007.