Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

ANA CAROLINA LEITE DE OLIVEIRA

TECNOLOGIA DA INFORMAÇÃO COMO SUPORTE À SEGURANÇA E À TOMADA DE DECISÃO

Assis - SP
2013

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

ANA CAROLINA LEITE DE OLIVEIRA

TECNOLOGIA DA INFORMAÇÃO COMO SUPORTE À SEGURANÇA E À TOMADA DE DECISÃO

Trabalho de conclusão de curso apresentado ao Instituto Municipal de Ensino Superior de Assis – IMESA - e à Fundação Educacional do Município de Assis – FEMA, como requisito à obtenção do Certificado de Conclusão.

Aluna: Ana Carolina Leite de Oliveira
Orientador: Prof. Dr. Osmar Aparecido Machado

Assis – SP
2013

FICHA CATALOGRÁFICA

OLIVEIRA, Ana Carolina Leite de.

Tecnologia da Informação como suporte à segurança e à tomada de decisão/ Ana Carolina Leite de Oliveira. Fundação Educacional do Município de Assis – FEMA –Assis, 2013.
53 páginas.

Orientador: Professor Doutor Osmar Aparecido Machado
Trabalho de Conclusão de Curso - Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Informação. 2. Segurança. 3. Tomada de Decisão.

CDD: 658
Biblioteca da FEMA

TECNOLOGIA DA INFORMAÇÃO COMO SUPORTE À SEGURANÇA E À TOMADA DE DECISÃO

ANA CAROLINA LEITE DE OLIVEIRA

Trabalho de conclusão de curso apresentado ao Instituto Municipal de Ensino Superior de Assis – IMESA - e à Fundação Educacional do Município de Assis - FEMA, como requisito do Curso de Graduação, analisado pela seguinte comissão examinadora:

Orientador: Prof. Dr. Osmar Aparecido Machado

Examinadora: Profª Ms. Rosemary Rocha Pereira da Silva

Assis - SP
2013

DEDICATÓRIA

Dedico este trabalho a minha mãe, Valdelucia, por todo amor e carinho e por ter-me apoiado na realização de mais um sonho.

E a todos que tiverem interesse na área de tecnologia da informação, com ênfase em segurança da informação e em tomada de decisão.

AGRADECIMENTOS

Primeiramente a Deus por ter-me dado força durante esses quatro anos de curso, em meio a dificuldades. Por ter-me iluminado nas decisões mais difíceis, e por ter-me guiado ao longo do curso para trilhar o caminho mais correto possível.

A minha família, em especial a minha mãe, VALDELUCIA LEITE, pelo amor e dedicação e por ter-me proporcionado essa oportunidade de um futuro promissor. Por tantas vezes que desistiu dos seus sonhos para realizar os meus, e abriu mão das suas vontades para realizar meus caprichos.

A ELIZABETH ESTELA NARDON FELICI e ao JOSÉ APARECIDO FELICI, por terem-me incentivado a ingressar no curso, auxiliando, inclusive, financeiramente, para que eu permanecesse nele durante o primeiro ano.

Ao Programa Escola da Família, por ter subsidiado a realização do meu sonho nos anos seguintes. E a todas as pessoas que frequentam o PEF Clybas, fazendo com que nossos finais de semana, apesar de cansativos, sejam alegres e prazerosos.

Aos professores, em especial ao meu orientador, professor doutor OSMAR APARECIDO MACHADO, por ter-me incentivado a não desistir do TCC, por ter-me dado atenção e orientação para o desenvolvimento do meu trabalho de conclusão de curso e a professora mestre ROSEMARY ROCHA PEREIRA DA SILVA, por fazer parte da banca examinadora, acrescentado qualidade ao meu trabalho.

A ELOIDE SANT'ANA CARNEIRO por ter feito a correção ortográfica e gramatical do meu trabalho. A CLÁUDIA FRAZÃO por ter feito a correção do meu abstract.

E aos meus amigos, que torceram para que eu vencesse mais esta etapa da minha vida.

“A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos.”

John Naisbitt

RESUMO

A segurança da informação nunca foi tão importante quanto é atualmente. Isso porque os computadores estão conectados no mundo inteiro por meio da internet, aumentando, assim, a vulnerabilidade da organização com relação a furto, perda, roubo ou alteração das informações. Nesse sentido, este estudo visa identificar e analisar, de maneira geral, a segurança da informação nas organizações, investigar como as empresas gerenciam e mantêm suas informações, como as informações influenciam na tomada de decisão, e, ao mesmo tempo, pretende disponibilizar conceitos teóricos sobre o assunto para pessoas e organizações interessadas. Espera-se, por fim, que o estudo possa mostrar quão importante é manter segura as informações que as organizações possuem, e como as informações podem auxiliar na tomada de decisão.

Palavras-chave: Informação; segurança; tomada de decisão.

ABSTRACT

The security of information has never been so important as currently. This is because computers are connected one another around the world through the internet, thus increasing the vulnerability of the organization in what is concerned to theft, loss or alteration of information. In this context, this study aims to identify and analyze, in a general way, the security of information in organizations, investigate how businesses manage and maintain your information, such as information which influences in decision-making, and, at the same time, you also want to offer a theoretical support on the subject for the organizations concerned. It is expected, finally, that the study can show how important it is to maintain secure information that organizations have, and how the information can assist in decision making.

Keywords: Information; security and decision-making.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Os primeiros computadores eram tidos como "máquinas gigantes" que tornavam possível a automatização de determinadas tarefas. Com o avanço da tecnologia, especialmente a partir da segunda metade do século XX, tais máquinas tornaram-se gradativamente menores, enquanto sua capacidade de processamento aumentou. Esses gigantescos computadores, chamados de Mainframe, foram sendo substituídos por maquinas cada vez menores e mais potentes em termos de processamento e confiabilidade.

Figura 1 – Mulheres operando o ENIAC (WIKIPEDIA, THE FREE ENCYCLOPEDIA).

Em seguida, a evolução das telecomunicações permitiu que os computadores, aos poucos, passassem a se comunicar, mesmo estando em lugares muito distantes geograficamente.

O elemento que tornou isso possível foi a capacidade de gerar, processar e transmitir informação cada vez mais rápida e de forma mais confiável. Desde as máquinas mais antigas e simples até os computadores mais recentes, a informação sempre foi o objeto das transformações.

Nesse sentido, este estudo visa identificar e analisar, de maneira geral, a segurança da informação nas organizações, especialmente das formas de acesso aos servidores, bancos de dados e dos sistemas de informação. Pretende ainda, investigar como as empresas gerenciam e mantêm suas informações. Ao mesmo tempo, pretende também oferecer um suporte teórico sobre o assunto para as organizações interessadas.

E como objetivo específico tem-se o seguinte:

- Levantar e identificar as principais formas de gestão da informação;
- Levantar, investigar e analisar os processos de segurança da informação;
- Pesquisar como as organizações realizam a segurança de suas informações, por meio de revisão da literatura;
- Disponibilizar os resultados de forma a facilitar o uso da segurança da informação por indivíduos e organizações;
- Contribuir para a área específica de conhecimento.

Embora seja possível, muito dificilmente uma organização de grande porte consegue perder suas informações, principalmente quando se trata de bancos, redes de lojas, companhias aéreas, instituições de pesquisas, etc. Isso porque tais organizações, cientes da importância das informações, buscam alternativas no sentido de garantir a segurança de acesso e de manutenção das mesmas em seus bancos de dados.

Por outro lado, se há uma coisa que ocorre com bastante frequência é o uso inadequado de informações ou, ainda, a sua subutilização. Bancos de dados organizacionais sem chaves de segurança podem permitir que, pessoas mal intencionadas tenham livre acesso e danifiquem dados importantes.

Por exemplo, se um banco perder todas as informações dos clientes, ele terá um prejuízo bem maior do que se houver um assalto a uma agência e os ladrões levarem todo o dinheiro. Pois informações incompletas, ou a falta de informações, podem levar a erros, comprometendo a sobrevivência da empresa.

Outro exemplo é se for retirado da conta bancária de alguém R$0,01 por dia. Talvez essa pessoa nem perceba ou ignore a situação, pelo fato do prejuízo

ser relativamente pequeno. Mas, se, uma terceira pessoa conseguir acessar os dados bancários de outra, devido à ausência ou a pouca segurança que o banco oferece, no momento em que os clientes utilizam o internet *banking*, essa pessoa poderá realizar várias transações financeiras, causando grandes prejuízos ao correntista.

Por isso, a TI é hoje, sem dúvida, um tema importante a ser tratado dentro da organização, principalmente quando se trata de tomada de decisão e de segurança da informação.

Para o desenvolvimento deste trabalho, foram realizadas pesquisas bibliográficas sobre a Administração e a Tecnologia da Informação. As pesquisas foram realizadas em livros, artigos científicos e revistas especializadas. Essas teorias possibilitaram uma compreensão acurada de como se apresenta, atualmente, a segurança da informação nas organizações.

A seguir apresenta-se a estrutura do trabalho:

- **Introdução** - espaço dedicado à apresentação e à contextualização do trabalho.
- **Considerações teóricas básicas** - consistem no levantamento bibliográfico de dados, informação, conhecimento e tecnologia da informação.
- **Segurança da Informação** – proporciona o conceito, as tecnologias existentes, as ameaças e as formas de proteção à segurança das informações organizacionais.
- **Tomada de decisão** – evidência as características e as fases da tomada de decisão.
- **Sistemas de Informação** – demonstra o conceito, os níveis, os tipos e os benefícios que os sistemas de informação trazem para as organizações.
- **Considerações Finais** – apresenta as principais conclusões obtidas na elaboração do trabalho.
- **Referências** - relaciona a bibliografia utilizada para a pesquisa.

2. CONSIDERAÇÕES TEÓRICAS BÁSICAS

Este capítulo expõe teorias a respeito de dados, informação, conhecimento e tecnologia da informação, com o intuito de facilitar o entendimento do leitor nos próximos capítulos, conforme a figura abaixo.

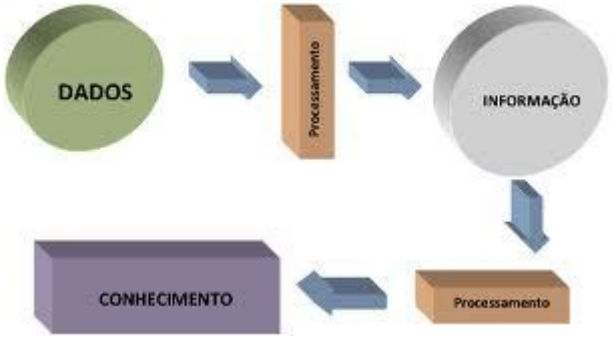

Figura 2 – Dados, informação e conhecimento (REI, 2010).

2.1. DADOS

Os dados podem ser números, palavras ou imagens. O processo de geração de dados dentro das organizações pode ocorrer de diversas maneiras, como, por exemplo, quando se cria um pedido de compra ou quando se contrata um novo funcionário.

“A maioria das organizações não conseguiria sobreviver ou ter sucesso sem dados de qualidade sobre suas operações internas e seu ambiente externo”, (O’ BRIEN, 2004, p.133), pois os dados fazem parte do ativo da organização, e, por isso, devem ser coletados e armazenados de forma segura e com qualidade.

Segundo Oliveira (2007, p.170), “dado é qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação”.

Embora o dado seja um elemento em forma bruta, desde o momento de sua captura já ocorre um processo de filtragem, com o objetivo de extrair somente o que é mais importante para o observador.

Para De Sordi (2008, p. 7), “dados são a coleção de evidências relevantes sobre um fato observado”. Os dados, normalmente, são submetidos a atividades de processamento como cálculo, comparação, separação, classificação e resumo. Essas atividades organizam, analisam e manipulam dados convertendo-os em informação para os usuários finais.

2.2. INFORMAÇÃO

Apesar das pessoas produzirem e transmitirem informação o tempo todo, tem-se bastante dificuldade em definir o que é informação. Muitas vezes, informação é confundida com dados, outras, com conhecimento.

O dicionário Houaiss a define como: “ato ou efeito de informar (-se); informe; notícia, conhecimento, ciência; [...] conjunto de conhecimentos reunidos sobre determinado assunto ou pessoa; fato de interesse geral a que se dá publicidade [...]”.

Para adquirir informação é preciso buscar dados brutos, processá-los e interpretá-los. De Sordi (2008, p. 10) afirma que “informação é a interpretação de um conjunto de dados segundo um propósito relevante e de consenso para o público-alvo (leitor)”. Ou seja, a informação tem que ser válida e ter princípios éticos, além de estar de comum acordo entre os envolvidos, para que haja o entendimento entre as partes.

A informação é um patrimônio, é algo que possui valor. Quando digital, não se trata apenas de bytes juntos, mas sim de um conjunto de dados classificados e organizados de forma que uma pessoa física ou jurídica possa utilizá-la em prol de algum objetivo.

Alecrim (2011) afirma que é preciso utilizar os recursos de tecnologia da informação, como ferramentas, sistemas, de maneira adequada, pois a informação é um patrimônio que agrega valor e dá sentido às atividades que a

utilizam, visando sempre encontrar boas soluções e com o menor custo possível.

Para que as informações sejam um diferencial das organizações, é preciso que elas sejam armazenadas e gerenciadas de forma eficiente, evitando-se, assim as falhas dos sistemas e as perdas inesperadas.

Além disso, para que as informações geradas possuam valor, elas devem ser significativas para as pessoas, como afirma O' Brien (2004, p. 25):

> Informações antiquadas, inexatas ou difíceis de entender não seriam muito significativas, úteis ou valiosas para você ou outros usuários finais. As pessoas desejam informações de alta qualidade, ou seja, produtos de informação cujas características, atributos ou qualidades ajudam a torná-los valiosos para elas.

As pessoas e organizações desejam informações de alta qualidade. Dentre as características que devem ser asseguradas na informação para que ela seja considerada de qualidade elencam-se, segundo De Sordi (2008, p.23):

> Comparabilidade – capacidade de comparar informação sobre o desempenho da organização com períodos anteriores, metas de desempenho, e *benchmarks* externos extraídos de outras organizações, regulamentação obrigatória e normas facultativas;
>
> Confiabilidade – permite à organização e suas partes interessadas dependerem da informação providenciada pela contabilidade, auditoria e relato social e ético para estarem livres de erro e parcialidade;
>
> Relevância – utilidade da informação para a organização e suas partes interessadas como um meio de construção de conhecimento e formação de opiniões, assim como para suporte à tomada de decisão;
>
> Entendimento – compreensão da informação pela organização e suas partes interessadas, incluindo questões de língua, estilo e formato. (Beckett e Jonker, 2002, p. 40, apud De Sordi, 2008, p. 23).

A qualidade da informação nos sistemas de informação será discutida em seção específica para o assunto.

2.2.1. Informação nas Organizações Atuais

Determinar o valor do patrimônio intelectual que uma organização possui não é tarefa fácil, e viver sem informação seria praticamente impossível para uma organização. Mas não basta que uma organização tenha informação. É preciso que ela entenda o quanto é importante armazená-las com segurança, pois essas informações influenciarão na tomada de decisão.

Segundo Alecrim (2011), a informação é tão importante que pode, inclusive, determinar a sobrevivência ou o fim das atividades de um negócio. Dentre os vários problemas que uma instituição financeira teria se perdesse todas as informações de seus clientes estão: não saber quanto cada cliente possui aplicado, quanto cada um lhes deve, ou em quanto tempo os clientes deverão pagar os financiamentos, etc.

Mas não basta ter a informação. É preciso que ela esteja disponível no momento em que for necessário utilizá-la. Pinheiro (2004) afirma que, quando uma informação não é suficientemente precisa ou completa, um profissional pode tomar decisões equivocadas, podendo gerar grandes prejuízos sociais e/ou econômicos.

Por exemplo, se o chefe diz ao funcionário chamado José: “Zé, preciso do número desse pedido” e alguém entende que o Zé está despedido. Começam os boatos dentro da organização. Isso pode levar a problemas de relacionamento, a decisões equivocadas, etc. Por isso, é tão importante que a informação seja precisa, perfeita e completa.

Existe uma área de estudo específica sobre a qualidade da informação, em que a completude, acurácia, pontualidade, objetividade, dentre outras, são dimensões ou características que possibilitam a avaliação da informação. Nesse sentido, informação de qualidade são aquelas que possuem boa avaliação dessas características. Neste estudo, entretanto, não se vislumbram o uso de tais dimensões, por questões de alinhamento com os objetivos aqui traçados.

Em síntese, quando ocorre a coleta dos dados e o processamento dos mesmos, gera-se a informação. Ao interpretar o agrupamento dessas informações, pode-se ou não gerar o conhecimento.

2.3. CONHECIMENTO

Há alguns anos, a grande preocupação das organizações era simplesmente produzir mais produtos e serviços. Atualmente, a gestão dos recursos de conhecimento é uma parte fundamental para o crescimento dos negócios.

O conhecimento baseia-se em dados e informações, mas ao contrário deles, está sempre ligado a pessoas. Ou seja, é possível verificar a veracidade dos dados e das informações, mas do conhecimento não. Porque esse depende da cultura, da história de vida de cada individuo para ser formado.

Para De Sordi (2008, p. 12) o conhecimento é:

> O novo saber, resultante de análises e reflexões de informações segundo valores e modelo mental daquele que o desenvolve, proporcionando a este melhor capacidade adaptativa às circunstâncias do mundo real.

Ou seja, quando se realiza a interpretação dos dados, segundo um propósito relevante e de consenso para um público-alvo específico, gera-se a informação. Esse novo saber, resultante de análises e reflexões das informações, gera o conhecimento, conforme figura 1.

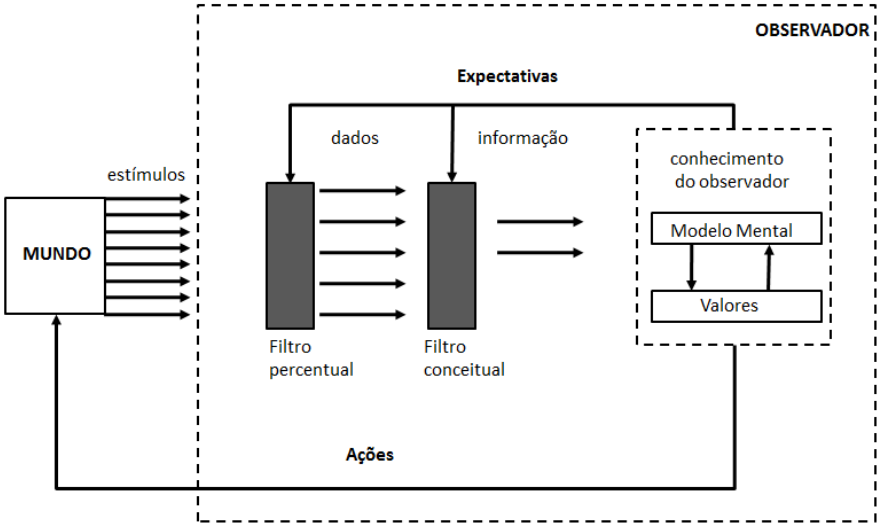

Figura 3 – Conhecimento segundo o agente gerador e beneficiário (DE SORDI, 2008, p.13).

Drucker (1993) apud Nonaka e Takeuchi (1997, p. 5) argumenta [...] que “na nova economia, o conhecimento não é apenas mais um recurso, ao lado dos tradicionais fatores de produção – trabalho, capital e terra – mas sim o único recurso significativo atualmente”.

Sendo o conhecimento o único recurso significativo para a organização, deve-se zelar pela segurança do mesmo. Pois, se o concorrente obtiver conhecimentos a respeito da organização, ele irá adquirir uma vantagem competitiva e conseguir agir antes, captando clientes, lançando produtos melhores, etc.

De acordo com Fegury (2011, p.1) existem dois tipos de conhecimento:

> O Conhecimento Explícito está documentado e pode ser facilmente comunicado e compartilhado. A palavra explícito tem sua origem do latim explicitus, cujo significado é "formal, explicado, declarado".
>
> O Conhecimento Tácito é um conhecimento pessoal e complexo, oriundo da experiência, formado dentro de um contexto social e individual. Este conhecimento é subjetivo, não mensurável e inerente às habilidades de cada indivíduo, por este motivo é difícil de ser explicado e formalizado. A palavra tácito tem sua origem do latim tacitus, que significa "não expresso por palavras".

Ou seja, o conhecimento explícito pode ser expresso por palavras, números e está escrito e documentado. Já o conhecimento tácito, é manifestado dentro do contexto social e individual, por meio das intuições.

Segundo Fegury (2011, p.2) “todo o conhecimento explícito já foi um dia tácito, pois o conhecimento tácito para ser eficazmente comunicado, necessita ser explicitado, e nesse momento, por definição, deixa de ser tácito”. Portanto, ao contrário do que muitas pessoas pensam, esses dois conhecimentos são complementares. E, quando ocorre a conversão do conhecimento tácito em conhecimento explícito, cria-se o conhecimento organizacional.

Nonaka e Takeuchi (1997, p. 11) afirmam que:

> Ter um *insight* ou um palpite altamente pessoal tem pouco valor para a empresa, a não ser que o individuo possa convertê-lo em conhecimento explícito, permitindo assim que ele seja compartilhado com outros indivíduos na empresa.

Ou seja, quando um funcionário tem uma ideia, ele deve criar um projeto que mostre a viabilidade da implantação de sua ideia. Se ela for aprovada pelos demais membros da equipe, ele conseguiu transformar o conhecimento tácito em conhecimento explícito, gerando benefícios para a organização. Portanto, o crescimento do conhecimento organizacional, depende diretamente do conhecimento dos colaboradores. Sendo assim, é imprescindível que a organização valorize o conhecimento de seus colaboradores, para que ambas as partes possam ganhar.

2.4. TECNOLOGIA DA INFORMAÇÃO

Partindo do princípio que tecnologia são as técnicas utilizadas para um determinado fim, pode-se concluir que ao processar, armazenar e distribuir informações no formato digital utiliza-se a tecnologia da informação.

De Sordi e Meireles (2010, p. 20) definem tecnologia da informação como:

> A tecnologia utilizada para processar, armazenar e transportar informações no formato digital, ou seja, é um conjunto de hardware, software e componentes de telecomunicação que provê soluções para a armazenagem, processamento, análise, transferência e pesquisa de informações.

Logo, a tecnologia da informação facilita o uso das informações dentro das organizações, pois permite acessá-las de maneira mais rápida. Alecrim (2011) define tecnologia da informação como o conjunto de todas as atividades e soluções fornecidas por recursos de computação que visam permitir o armazenamento, acesso e o uso das informações.

Nas organizações, as informações geralmente ficam armazenadas dentro de um banco de dados, de forma que é possível acessá-las e consultá-las com exatidão e rapidez. Segundo Korth (1994 apud Rezende, 2006), um banco de dados "é uma coleção de dados inter-relacionados, representando informações sobre um domínio específico".

Para facilitar a troca dessas informações foram criados os sistemas de informação, que podem ser definidos como "o conjunto de softwares que suportam a execução de diversas transações de negócios e a manipulação de dados altamente correlacionados" (De Sordi e Meireles, 2010, p. 21).

Os softwares são programas que desempenham várias movimentações de negócios e manuseiam dados diretamente relacionados, fazendo com que os dados cheguem na hora certa, até a pessoa certa.

Pinheiro (2004) afirma que o valor da informação está relacionado à maneira como os sistemas de informação auxiliam os profissionais responsáveis pela tomada de decisão em alcançar as metas que a organização deseja.

Considerando tais afirmações, é possível afirmar que, quando há gestão da tecnologia da informação aliada à segurança das mesmas, a tomada de decisão torna-se uma atividade mais fácil e ocorre de maneira mais eficiente.

Por isso, De Sordi (2008, p. 1) afirma que:

> [...] os maiores ganhos organizacionais com recursos de TI não residem na sua simples aquisição, disponibilidade e uso eficaz. Espera-se que as atividades de coleta, armazenamento e análise de

> dados gerem informações relevantes que possam, por sua vez, gerar conhecimento estratégico.

Ou seja, não basta comprar um sistema e colocá-lo à disposição dos colaboradores, é preciso que ele atenda às necessidades da organização, possibilitando o acesso às informações em tempo hábil para a tomada de decisão, criando-se assim uma vantagem competitiva em relação aos concorrentes.

3. SEGURANÇA DA INFORMAÇÃO

Para que as informações sejam o diferencial das organizações, é imprescindível que estas ofereçam proteção ao conjunto de dados que compõem as informações e geram o conhecimento, no sentido de preservar o valor que possuem para o indivíduo, para os concorrentes e para a própria organização.

Ao adotar normas de acesso aos sistemas e ao ambiente dos servidores, aplicativos de software especialistas que garantem a segurança dos bancos de dados e dos sistemas, observam-se resultados positivos dentro das organizações como: diferencial competitivo, redução de custos, dentre outros. A segurança de informações visa garantir a integridade, confidencialidade, autenticidade, a disponibilidade e o não repúdio das informações processadas pela organização, como se observa na figura 4.

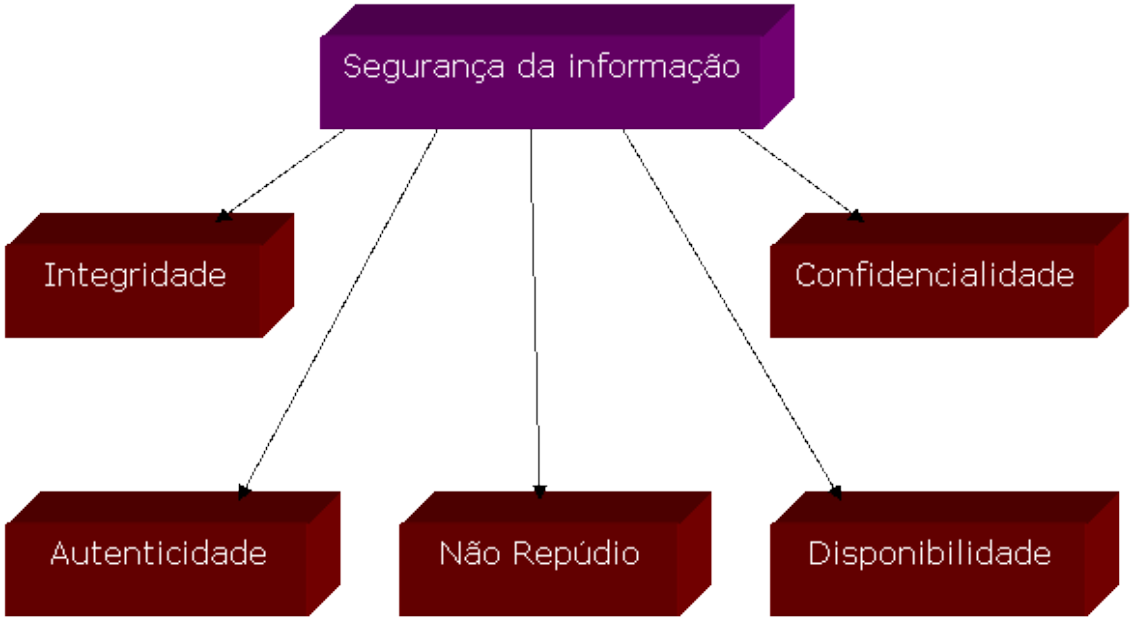

Figura 4: Pilares da Segurança da Informação. In: (Filho, 2004)

Sobre os pilares da segurança da informação, Filho (2004) afirma que:

- A confidencialidade previne a revelação não autorizada de informações, além de impedir o acesso de pessoas não autorizadas.
- A integridade previne a modificação não autorizada de informações.
- A disponibilidade permite um acesso confiável e prontamente disponível a informações.
- E o não repúdio e a autenticidade fazem a verificação da identidade e autenticidade de uma pessoa ou agente externo de um sistema, com o objetivo de assegurar a integridade de origem.

Desta forma, os pilares da segurança da informação garantem que as informações sejam guardadas em segredo, possibilitando o acesso apenas a pessoas autorizadas, de modo que não haja modificações não autorizadas pelo proprietário da informação. E ainda, identifica quem acessou as informações, garantindo, assim, a privacidade da informação.

Turban, Rainer, Potter (2007, p. 54) afirmam que:

> Privacidade é o direito de ficar em paz e de estar livre de invasões pessoais injustificáveis. A privacidade da informação é o direito de determinar quando e até que ponto as informações sobre você podem ser coletadas e/ou comunicadas a outros indivíduos. Os direitos de privacidade se aplicam a pessoas, grupos e instituições.

Para garantir a privacidade da informação as empresas adotam medidas de segurança como, chave de acesso, barreiras que limitam o acesso à informação, assinatura digital, etc.

De acordo com Turban, Rainer, Potter (2007, p. 55), judicialmente, existem basicamente duas regras para a privacidade:

1ª “O direito da privacidade não é absoluto. A privacidade precisa ser contrastada com as necessidades da sociedade”.

2ª “O direito público de saber está acima do direito de privacidade do indivíduo”.

Isso significa que, se a informação for mais importante para a sociedade do que para o indivíduo ou organização, este perde o direito à privacidade, para garantir o direito do coletivo.

Côrtes (2008, p. 485) afirma que as novas tecnologias da informação e o uso intenso de sistemas têm favorecido a execução de fraudes e desvios. Enquanto que o crescente uso de redes de computadores e sistemas *on-line* aumentam a vulnerabilidade da organização em relação a furto, perda ou alteração da informação.

Portanto, apesar das redes de computadores facilitarem a execução das tarefas realizadas nas organizações, elas também facilitam o acesso de invasores. Pois, a internet permite que computadores de diversas partes do mundo se conectem uns com os outros, tornando os dados e as informações muito mais expostos às ameaças.

3.1. AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais, seja perda de confidencialidade, perda de integridade ou perda de disponibilidade.

> Uma ameaça a um recurso de informação é qualquer perigo ao qual um sistema pode estar exposto. A exposição de um recurso de informação diz respeito ao prejuízo, à perda ou ao dano que podem ocorrer se uma ameaça comprometer esse recurso. A vulnerabilidade de um sistema é a possibilidade de ele sofrer algum dano devido ax uma ameaça. Risco é a probabilidade de uma ameaça ocorrer. Os controles de sistemas de informação são os procedimentos, dispositivos ou softwares destinados a evitar o comprometimento do sistema. (TURBAN; RAINER; POTTER, 2007, p. 54).

Ou seja, quanto mais vulnerável for um sistema de informação, mais facilmente ele poderá sofrer ameaças. A quantidade dessas ameaças dependerá do nível de risco do sistema de informação. E o objetivo desse trabalho é apresentar qual a importância da implantação de controles de sistemas de informação.

3.1.1. Ameaças involuntárias aos sistemas de informação

As ameaças involuntárias aos sistemas de informação são aquelas em que não há intenção de prejudicar ninguém. Segundo Turban, Rainer, Potter (2007), elas podem ser divididas em três grandes grupos:

- Os **erros humanos** são responsáveis por mais da metade dos problemas relacionados ao controle e à segurança em muitas organizações, e podem ocorrer no projeto do hardware e/ou do sistema de informação, na programação, no teste, na coleta de dados, na entrada de dados, na autorização e nos procedimentos.
- Os **riscos ambientais** são aqueles relacionados às mudanças do ambiente e incluem terremotos, furacões, inundações, interrupções ou fortes flutuações na energia, incêndios, ar-condicionado defeituoso, explosões, precipitação radioativa e falhas no sistema de resfriamento de água.
- As **falhas no sistema de computação** podem ocorrer como resultado de uma fabricação ruim ou do uso de materiais defeituosos.

As ameaças involuntárias também podem ser causadas por outros motivos, como por exemplo, a falta de experiência do usuário, ou testes malfeitos.

3.1.2. Ameaças intencionais aos sistemas de informação

As ameaças intencionais aos sistemas de informação são aqueles em que há a intenção de prejudicar uma pessoa, grupo de pessoas ou organizações. Normalmente elas possuem natureza criminosa. Segundo Turban, Rainer, Potter (2007), elas podem ser divididas em:

- **Espionagem ou invasões** ocorrem quando um indivíduo não autorizado obtém acesso a informações que uma organização está tentando proteger.
- **Extorsão de informações** ocorre quando um invasor ou empregado que era confiável rouba informações de um sistema de computação e,

depois, exige uma compensação para devolvê-las ou para não revelá-las.

- **Sabotagem ou vandalismo** ocorre quando *hacktivistas* ou *ciberativistas* invadem o *website* de uma organização, com o objetivo de protestar contra operações, políticas ou ações de um indivíduo, uma organização ou um órgão governamental, levando os clientes da organização à perda da confiança da segurança das informações da mesma.
- **Roubo** é a apropriação ilegal de algo que pertence à outra pessoa ou organização. Dentro de uma organização, essa propriedade pode ser física, eletrônica ou intelectual.
- **Roubo de identidade** ocorre quando um criminoso se passa por outra pessoa para cometer fraudes.
- **Ataques de *software*** – ocorrem quando indivíduos ou grupos projetam software para atingir sistemas de computação, sendo que esse software é projetado para danificar, destruir ou negar serviço aos sistemas de computação. Os tipos mais comuns de ataque com software são:
    - **Vírus** - são segmentos de código de computador que realizam ações que variam do mero transtorno até a destruição.
    - **Cavalo de Tróia** - são programas de software que se escondem dentro de outros programas e só revelam seu comportamento quando ativados.
    - ***Back doors*** – são instalados por um vírus ou *worm.* O *back door* normalmente é uma senha, conhecida apenas pelo atacante, que lhe permite acessar o sistema à vontade, sem precisar executar quaisquer procedimentos de segurança.
    - ***Software* invasivo** - os diferentes tipos de *software* invasivo incluem *pestware, adware, spyware, spamware, spam, cookies, web bugs.* Sendo que, *pestware é um software* clandestino que é instalado no computador através de canais não confiáveis. *Adware* é um *software* projetado para ajudar a exibir anúncios *pop-up* no computador. *Spyware* são programas que registram seus toques no teclado, para capturar senhas. *Spamware* é elaborado para usar seu computador para envio de spam. *Spam*

é um e-mail não solicitado, cuja finalidade geralmente é anunciar produtos ou serviços. *Cookies* são pequenas quantidades de informação que os *websites* armazenam em seu computador, temporariamente ou quase sempre permanentemente. E *web bugs* são imagens gráficas pequenas e, normalmente, invisíveis que são adicionadas a uma página da Web ou mensagem de e-mail.

  - ***Phishing*** - usa o logro para adquirir informações pessoais valiosas, como números e senhas de contas, aparentando ser um e-mail verdadeiro.
  - ***Pharming*** – ocorre quando o atacante adquire fraudulentamente o nome de domínio do *website* de uma empresa. Quando as pessoas digitam o endereço do *website*, vão, na verdade para o *website* falso do atacante, que possui a aparência exata do *website* real.
  - ***Worms*** - são programas destrutivos que se duplicam sem a necessidade de qualquer outro programa para garantir um ambiente seguro para a duplicação.
  - **Bombas lógicas** - são segmentos de códigos de computador que são embutidos dentro dos programas existentes em uma organização.
  - **Negação de serviço** – ocorre quando o atacante envia tantas requisições de informação a um sistema alvo, que o sistema não consegue lidar com elas.

- **Transgressões à propriedade intelectual** – é a violação da propriedade criada por indivíduos ou organizações que é protegida por leis de segredo comercial, patente e direito autoral. Logo, violar a propriedade intelectual é quebrar o segredo da informação.

As ameaças são muitas, mas as empresas estão desenvolvendo *softwares* e serviços que ajudam a proteger as informações dentro e fora das organizações.

3.2. PROTEÇÃO ÀS INFORMAÇÕES

A proteção das informações tem o objetivo de preservar o valor que elas possuem, tanto para as pessoas físicas como para as pessoas jurídicas. Mas, antes de implantar algum tipo de proteção, as organizações devem realizar o gerenciamento dos riscos. Segundo Turban, Rainer, Potter (2007, p. 68) “um risco é a probabilidade de uma ameaça causar impacto a um recurso de informação”. Ou seja, um risco é a chance de que possa ocorrer algum problema que danifique ou cause a perda da informação. Turban, Rainer, Potter (2007, p. 68) afirmam que “o objetivo do gerenciamento de riscos é identificar, controlar e minimizar o impacto das ameaças”. Existem três processos no gerenciamento de riscos: a análise de risco, redução de risco e avaliação de controle.

> A análise de risco é o processo pelo qual uma organização avalia o valor de cada recurso ser protegido, estima a probabilidade de cada recurso ser comprometido e compara os custos prováveis do comprometimento de cada um com os custos de protegê-lo. (TURBAN; RAINER; POTTER, 2007, p. 68).

Desta forma, ao realizar a análise de risco, a organização irá mensurar o valor que as informações possuem para ela, a chance da informação sofrer uma ameaça e o custo para fazer a proteção das informações.

> Na redução de risco, a organização executa ações concretas contra os riscos. A redução de risco possui duas funções: (1) implementar controles para prevenir a ocorrência de ameaças identificadas; e (2) desenvolver um meio de recuperação se a ameaça se tornar uma realidade. (TURBAN; RAINER; POTTER, 2007, p. 68).

Assim sendo, ao realizar a redução de riscos, a organização identifica a probabilidade de uma ameaça ocorrer e implanta mecanismos de defesa (controles), para tentar impedir que a ameaça ocorra. E ainda, criam formas de recuperação das informações, para o caso da ameaça se concretizar.

> Na avaliação dos controles, a organização identifica problemas na segurança e calcula os custos da implementação de medidas de controle adequadas. Se os custos de implementar um controle forem mais altos que o valor do recurso a ser protegido, o custo do controle não é viável. (TURBAN; RAINER; POTTER, 2007, p. 69).

Portanto a implantação de mecanismos de defesa irá depender principalmente do custo benefício, pois, se a informação a ser protegida tiver menos valor do que o custo de sua proteção, sua implantação será inviável.

3.3. CONTROLES

Controles são mecanismos de defesa que permitem que um sistema de informação resista a ataques. Turban, Rainer, Potter, (2007, p. 69) afirmam que “os controles se destinam a prevenir danos acidentais, deter ações intencionais, solucionar problemas o mais rapidamente possível, melhorar a recuperação de danos e corrigir problemas”. Logo, a principal função de um controle é a prevenção. Os controles de defesa podem ser divididos em duas categorias: controles gerais e controles de aplicação.

3.3.1. Controles gerais

Os controles gerais são formados para proteger o sistema inteiro. Segundo Turban, Rainer, Potter (2007) eles podem ser divididos em:

- **Controles físicos** - oferecem proteção física das instalações e recursos computacionais.
- **Controles de acesso** – restringem o acesso de usuário não autorizado aos recursos de computador; dedica-se à identificação do usuário.
- **Controles de segurança de dados** – protegem dados contra a exposição acidental ou voluntária a pessoas não autorizadas, ou contra modificação ou destruição não autorizada.
- **Controles administrativos** – publicam e monitoram as diretrizes de segurança.

- **Controles de comunicação (rede)** – lidam com a movimentação de dados através de redes e incluem controles de segurança de fronteira, autenticação e autorização.
    - **Segurança de fronteira** – o principal objetivo é o controle de acesso.
        - Firewalls – sistema que impõe políticas de controle de acesso entre duas redes.
        - Controle de vírus – software antivírus.
        - Detecção de invasão – o principal objetivo é detectar acesso não autorizado à rede.
        - Rede privada virtual – usa a internet para transmitir informações dentro de uma empresa e entre empresas parceiras, mas com maior segurança pelo uso da criptografia, da autenticação e do controle de acesso.
    - **Autenticação** – o principal objetivo é a prova de identidade.
    - **Autorização** – permissão concedida a indivíduos e grupos para realizar certas atividades com recursos de informação, com base na identidade verificada.

Logo, os controles gerais têm como principal objetivo a proteção do hardware e o controle de acesso.

3.3.2. Controles de aplicação

Os controles de aplicação são preservações que protegem aplicações específicas. Segundo Turban, Rainer, Potter (2007), eles podem ser divididos em:

- **Controles de entrada** – impedem alteração ou perda de dados.
- **Controles de processamento** – garantem que os dados estejam completos, válidos e corretos quando forem processados, e que os programas sejam executados corretamente.
- **Controles de saída** – garantem que os resultados do processamento por computadores sejam corretos, válidos, completos e coerentes.

Logo, os controles de aplicação têm como principal objetivo a proteção dos dados que estão sendo processados, visando à garantia da integridade, da confidencialidade, da autenticidade, da disponibilidade e do não repúdio.

3.4. AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Instalar controles de segurança não é o suficiente para garantir a proteção das informações. Turban, Rainer, Potter (2007) afirmam que é preciso saber se os controles estão instalados do modo pretendido, se são eficazes, se ocorreu alguma falha na segurança e que ações são necessárias para evitar futuras falhas. Essas perguntas podem ser respondidas por profissionais que não estão diretamente ligados à organização, profissionais que são denominados auditores. Turban, Rainer, Potter (2007, p. 75) definem auditoria como “uma verificação dos sistemas de informação, suas entradas, saídas e processamento”. Ou seja, uma auditoria tem a função de fiscalizar e corrigir as falhas do sistema de informação e dos usuários desse sistema.

Existem dois tipos de auditores e auditorias: internos e externos. Turban, Rainer, Potter (2007, p. 75) asseguram que:

> A auditoria de SI geralmente é parte da auditoria interna da contabilidade e, frequentemente, é realizada por auditores internos da empresa. Um auditor externo examina tudo o que a auditoria interna descobriu, bem como as entradas, o processamento e as saídas dos sistemas de informação. A auditoria externa dos sistemas normalmente é parte da auditoria externa geral realizada por uma empresa de contabilidade pública certificada.

Portanto, a auditoria é importante para a organização saber se o sistema de informação está funcionando corretamente, se os funcionários estão manipulando adequadamente o sistema, se o sistema de informação está seguro, dentre outros resultados.

3.5. PLANO DE RECUPERAÇÃO DE ACIDENTES

Levando-se em consideração que a perda da maioria ou de todas as informações da organização pode causar danos significativos, chega-se à conclusão que ter um plano de recuperação de acidentes é algo imprescindível. Turban, Rainer, Potter (2007, p. 77) afirmam que a recuperação de acidentes é:

> [...] a cadeia de eventos que abrange desde o planejamento até a proteção e a recuperação. A finalidade de um plano de recuperação é manter a empresa funcionando depois de um acidente, um processo chamado continuidade dos negócios.

Ou seja, a recuperação de acidentes visa permitir que a organização continue realizando suas atividades, mesmo que alguma ameaça venha a atingir o sistema de informação.

Dentro do plano de recuperação de acidentes está a prevenção de acidentes. Turban, Rainer, Potter (2007, p. 77) afirmam que “a prevenção de acidentes tem por objetivo minimizar as chances de acidentes evitáveis, como incêndios premeditados ou outras ameaças humanas”.

Já, a prevenção de acidentes visa à criação de medidas que impeçam que acidentes evitáveis aconteçam com a instalação de sistema antichamas, por exemplo.

Portanto, informações seguras possuem mais credibilidade junto aos tomadores de decisão e permitem que esses as usem com maiores possibilidade de sucesso na escolha.

4. TOMADA DE DECISÃO

Tomar decisões não é tarefa fácil. Algumas pessoas possuem dificuldades nas decisões mais simples, como escolher uma roupa para uma determinada ocasião ou um roteiro para as férias. Isso porque a tomada de decisão envolve um processo de identificação e de resolução de problemas. Sendo que, problema é uma situação que ocorre quando o estado atual das coisas é diferente do estado desejado das coisas.

> As organizações – ou, mais propriamente, as pessoas que tomam decisões importantes – não podem fazer o que querem. Elas enfrentam várias limitações – financeiras, legais, de mercado, humanas e organizacionais – que inibem certas ações. (BATEMAN E SNELL, 2006, p. 86).

Portanto, não basta querer iniciar uma nova atividade de negócio e tomar decisões a esse respeito. É preciso estar de adequado à legislação, ao mercado, a questões humanas e organizacionais.

4.1. CARACTERÍSTICAS DAS DECISÕES ADMINISTRATIVAS

Segundo Bateman e Snell (2006) as características das decisões administrativas são:

- **Ausência de estrutura** – Embora algumas decisões sejam rotineiras e bem definidas, na maioria delas não há um procedimento automático a seguir.
    - **Decisões programadas** – decisões já tomadas em situações anteriores e cujos resultados são objetivamente corretos e alcançáveis por meio de regras, políticas ou cálculos numéricos.
    - **Decisões não programadas** – decisões novas, inovadoras e complexas que não possuem consequências comprovadas.

- **Incerteza** – quer dizer que o gerente não tem informações suficientes para saber as consequências de diferentes ações.
- **Risco** – quando o gerente puder estimar a probabilidade de diversas consequências, mais ainda assim não souber com certeza o que acontecerá, ele estará enfrentando um risco.
- **Conflito** – existe quando os administradores precisam considerar pressões contrárias de diferentes fontes.
    - **Conflito psicológico** – ocorre quando várias opções são atrativas, ou quando nenhuma das opções é atrativa.
    - **Conflito de interesse** – ocorre quando um indivíduo ou grupo quer uma coisa e o outro indivíduo ou grupo quer outra coisa.

Portanto, antes de tomar uma decisão é preciso adquirir o máximo de informações a respeito do problema, tentar prevenir o risco e, quando isso não for possível, ao menos minimizá-lo ou controlá-lo, e tentar entrar em comum acordo com a equipe de trabalho, visando a escolha da opção mais adequada à situação.

4.2. FASES DA TOMADA DE DECISÃO

A tomada de decisão é a tarefa mais difícil que um administrador possui, pois envolve riscos que afetam inclusive a carreira profissional, dependendo das consequências que a decisão tiver. Riech (2001, p. 136) afirma que “tomar decisões é o trabalho mais importante de qualquer executivo. É também o mais difícil e o mais arriscado. Decisões mal tomadas podem arruinar um negócio e uma carreira, algumas vezes de modo irreversível”. Isso pode ocorrer, porque uma decisão foi tomada muito rápido, porque as informações que havia no momento da decisão não eram suficientes, etc. Por isso, para facilitar a tomada de decisão, alguns autores propõem que ela seja dividida em fases.

Simon (1971 apud Haddad; João, 2007, p.3) “propõe uma sequencia de atividades no processo decisório que inclui o levantamento do problema, verificação e análise de possíveis alternativas de solução, escolha de uma

alternativa viável e implantação da solução escolhida". Ou seja, deve-se primeiro identificar qual é o problema, quais são as soluções mais acessíveis, depois escolher a solução mais adequada à situação e, por último, colocá-la em prática.

Bateman e Snell (2006) possuem uma visão mais completa dos estágios da tomada de decisão e afirmam que o processo decisório ideal deve seguir seis estágios:

O primeiro estágio consiste na identificação e diagnóstico do problema. Ou seja, reconhecer que um problema existe, querer fazer algo para solucioná-lo e acreditar que os recursos e as habilidades para resolver existem.

O segundo estágio consiste na geração de soluções alternativas. Ou seja, criar soluções alternativas direcionadas à solução do problema. Essas soluções podem ser prontas, quando os tomadores de decisão utilizam ideias que viram ou tentaram anteriormente, ou seguem orientações de outras pessoas que enfrentaram problemas semelhantes. Ou sob medida, quando os tomadores de decisão projetam soluções para problemas específicos. Essa técnica requer uma combinação de ideias em soluções novas e criativas.

O terceiro estágio envolve a avaliação das alternativas. Ou seja, identificar quais serão as melhores soluções e quais serão as consequências da aplicação de cada solução.

O quarto estágio consiste na escolha. Ou seja, escolher a alternativa que melhor resolva o problema. Esse estágio envolve tomar a melhor decisão possível (maximizar), escolher uma opção aceitável, embora não seja a melhor nem seja perfeita (satisfação + sacrifício), ou alcançar o maior equilíbrio possível entre vários objetivos (otimização).

O quinto estágio consiste na implementação da decisão. Ou seja, pôr a decisão escolhida em prática.

O sexto e último estágio consiste na avaliação da decisão. Ou seja, coletar informações sobre quão bem a decisão está operando. Se a decisão mostra-se inadequada, deve-se voltar ao primeiro estágio, preferivelmente com mais informações, procurando eliminar os erros cometidos na primeira vez.

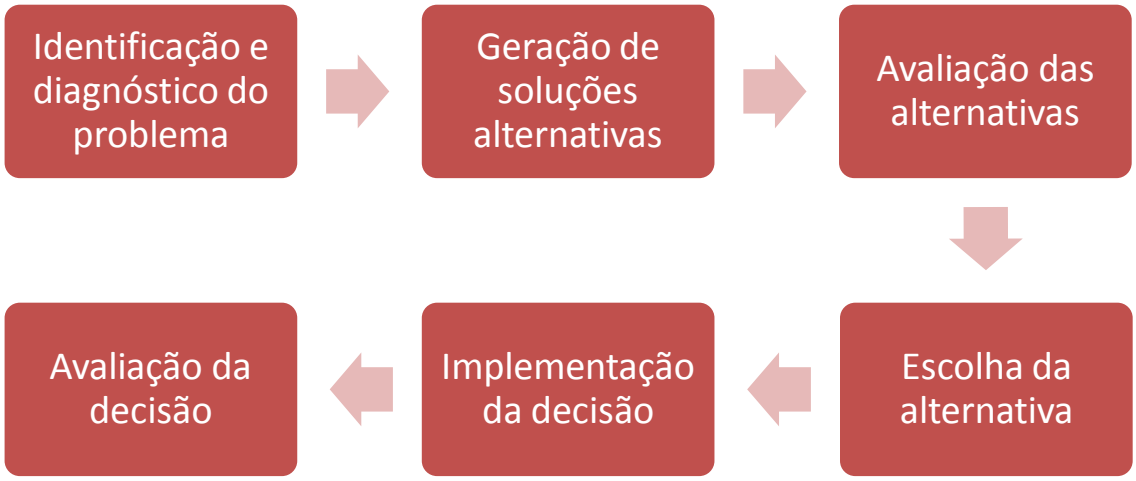

Figura 5 – Estágios da tomada de decisão, segundo Bateman e Snell.

A principal diferença entre as teorias listadas é que, ao contrário de Simon, Bateman e Snell propõem o *feedback* da decisão escolhida.

Logo, para tomar decisões, é preciso fazer a avaliação dos riscos, e aplicar as fases da tomada de decisão, visando à obtenção de maiores benefícios, tanto para as organizações, quanto para os colaboradores.

Para isso, existem alguns sistemas que facilitam esse processo, conceitos que serão explorados no próximo capítulo deste trabalho.

5. SISTEMAS DE INFORMAÇÃO

Antes de definir sistema de informação, é necessário entender o que é sistema. Para isso, deve-se pensar no corpo humano como um sistema, onde cada órgão isolado não consegue fazer o corpo funcionar, mas quando ocorre a união dos mesmos, formando um conjunto, o corpo humano funciona perfeitamente.

O' Brien (2004) define sistema de informação como um conjunto organizado de pessoas, *hardware*, *software*, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização.

Os sistemas de informação são utilizados para facilitar a comunicação dentro das organizações. Côrtes (2008, p. 25) afirma que:

> Sistema de informação é considerado o conjunto de componentes ou módulos inter-relacionados que possibilitam a entrada ou coleta de dados, seu processamento e a geração de informações necessárias à tomada de decisões voltadas ao planejamento, desenvolvimento e acompanhamento de ações.

Assim sendo, o sistema de informação beneficia os três níveis da organização, pois permite planejar, desenvolver e acompanhar as atividades realizadas dentro da organização.

Audy, Andrade e Cidral (2005), afirmam que os sistemas de informação possuem como objetivo geral a disponibilização de informações necessárias para que as organizações atuem em um determinado ambiente. Sendo que esse objetivo geral pode ser dividido em três metas fundamentais, conforme figura 2.

Figura 6 – Objetivos dos sistemas de informação (In: AUDY; ANDRADE; CIDRAL, 2005, p. 110).

Na base da pirâmide dos objetivos do sistema, está o apoio ao controle e a relação dos processos de negócio e funções organizacionais. No centro da pirâmide, está o apoio às decisões dos diversos níveis organizacionais. E, no topo da pirâmide, está o apoio à elaboração de estratégias competitivas e a obtenção de vantagens competitivas.

De acordo com Audy, Andrade e Cidral (2005, p. 111), “as funções de um sistema de informação incluem a coleta, o processamento, o armazenamento e a distribuição dos dados que, ao serem relacionados e contextualizados pelos usuários, proporcionarão as informações necessárias para a organização”.

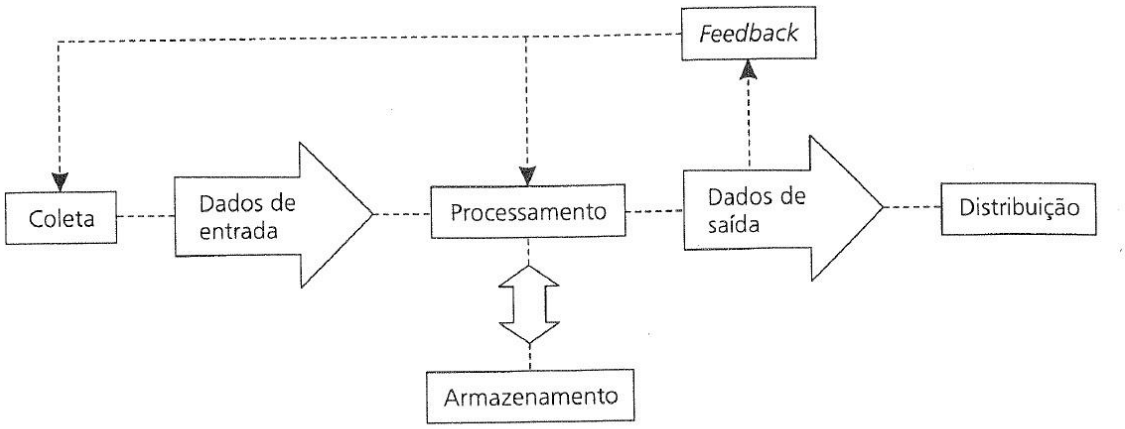

Figura 7 – Funções dos sistemas de informação. (In: AUDY; ANDRADE; CIDRAL, 2005, p. 112)

- A coleta consiste em colher dados brutos.
- O processamento organiza os dados, de acordo com a sequência de instruções codificada num programa.
- O armazenamento estoca (dados) de modo a poder recuperá-los posteriormente.
- A distribuição divide as informações com as demais pessoas interessadas.
- E a retroalimentação ou *feedback* é qualquer processo por intermédio do qual uma ação é controlada pelo conhecimento do efeito de suas respostas

Audy, Andrade e Cidral (2005, p. 114) afirmam que “a efetividade dos sistemas de informação baseados em computador é alcançada a partir de uma visão integrada dos cinco elementos que os compõem: *hardware, software*, dados, procedimentos e pessoas”. Logo, se uma das partes do sistema falhar, podem haver divergências de informação, podendo inclusive levar a erros.

Audy, Andrade e Cidral (2005, p. 114 e 115) asseguram que:

- **Hardware** - são todos os equipamentos usados na coleta, processamento, armazenamento e distribuição dos dados.
- **Software** - são os aplicativos necessários para que o hardware possa realizar a manipulação dos dados.

- **Dados** - podem ser números, palavras ou imagens armazenados no hardware e que permitem seu processamento pelo software.
- **Procedimentos** - distribuem e diferenciam funções, configuram procedimentos operacionais. Esses procedimentos operacionais padrão definem regras formais ou informais de realização de tarefas e correspondem a scripts a serem desempenhados pelos diversos tipos de usuários.
- **Pessoas** – podem ser classificadas em dois grupos: os profissionais de sistema de informação e os usuários. Os profissionais de sistema de informação são responsáveis pelo desenvolvimento, manutenção e suporte do sistema de informação. Os usuários são indivíduos que usufruem as atividades oferecidas pelo sistema, obtendo informações significativas e úteis para a organização.

No entanto, não bastam que as informações contidas nos sistemas de informação estejam integradas com os cinco elementos, é imprescindível que as informações contidas nos sistemas de informação sejam de qualidade, para garantir a credibilidade das mesmas.

Segundo Côrtes (2005, p. 28 – 30), os atributos que qualificam a informação dos sistemas de informação são:

- Nível de utilização – quantidade de vezes que a informação é utilizada
- Facilidade de acesso
- Velocidade
- Qualidade
- Atualidade – atual ou condizente com o momento
- Fidedignidade – informações de confiança
- Veracidade – capacidade de ser verdadeira ou de representar a verdade
- Exatidão – sem erros
- Precisão – capacidade de lidar com valores numéricos
- Reprodutibilidade
- Economia – conter apenas o que for importante
- Integrabilidade – deverá conter tudo o que for necessário para a tomada de decisão

- Inteligibilidade – a que se destina a informação

Portanto, quando os cinco elementos interagem adequadamente, o sistema de informação consegue disponibilizar informações para o planejamento, desenvolvimento e acompanhamento das atividades realizadas dentro da organização, permitindo a análise de problemas e oportunidades e a criação de novos produtos, serviços e formas de operações que propiciem a obtenção de vantagens competitivas.

5.1. NÍVEIS DOS SISTEMAS DE INFORMAÇÃO

Por existir diferentes níveis em uma organização, existem diferentes tipos de sistemas servindo a cada nível organizacional. Os sistemas de informação são classificados em três níveis: operacional, tático e estratégico.

- O nível operacional remete as decisões que devem ser tomadas em curto prazo relativas à avaliação e controle das atividades rotineiras.
- O nível tático está ligado às decisões de médio prazo, controla os processos de negócio, certifica se as metas estão sendo alcançadas e corrige os desvios das metas traçadas.
- Já o nível estratégico refere-se às decisões de longo prazo, relacionado ao ambiente externo e interno, levando em consideração a política, a economia, a sociedade e a tecnologia, além das competências e capacidades da organização, com o objetivo de definir metas e estratégias para que a organização mantenha ou amplie sua participação no mercado.

Portanto, para atender às necessidades de cada nível da organização, foram criados tipos diferentes de sistema.

5.2. TIPOS DE SISTEMAS DE INFORMAÇÃO

Existem vários tipos de sistemas de informação, que atendem aos três níveis organizacionais: o executivo, o tático e o operacional. Levando-se em consideração que o objetivo de um sistema de informação é armazenar, tratar e fornecer informações, de tal modo a apoiar as funções ou processos de uma organização, “há diferentes formas de classificar os sistemas de informação. Entretanto, as classificações mais aceitas agrupam os sistemas pela finalidade principal de uso e pelo nível organizacional”. (AUDY, ANDRADE e CIDRAL, 2005, P. 117).

5.2.1. Sistemas de Processamento de Transações (SPT)

Esse tipo de sistema é utilizado na parte operacional e está relacionado aos eventos básicos da organização. “Uma transação é uma troca de informações que ocorre quando duas partes estão envolvidas em alguma atividade”. (AUDY, ANDRADE e CIDRAL, 2005, P. 117).

Um exemplo disso é quando o departamento de produção envia uma mensagem ao departamento de compras, solicitando a aquisição de uma matéria prima ocorre uma transação, ou seja, a troca de informação. “À medida que as transações se tornam rotineiras, elas tendem a ser normatizadas de acordo com procedimentos operacionais padronizados”. (AUDY, ANDRADE e CIDRAL, 2005, P. 118). Ou seja, cria-se uma sequencia lógica para a execução das transações. De forma que qualquer pessoa seja capaz de realizá-la.

“Essas rotinas são realizadas pelo nível operacional da organização, razão pela qual esses sistemas também são denominados sistemas operativos ou transacionais”. (AUDY, ANDRADE e CIDRAL, 2005, P. 118).

Em síntese, o SPT está relacionado às atividades realizadas na base da organização que, por sua vez, estão diretamente ligadas à produção do bem ou serviço.

5.2.2. Sistemas de Informação Gerencial (SIG)

Esse tipo de sistema é utilizado pelo nível tático da organização. Ele apresenta ferramentas para controle das atividades rotineiras da mesma. Audy, Andrade e Cidral (2005, p. 120) afirmam que “os sistemas de informações gerenciais permitem oferecer suporte a decisões estruturadas. Uma decisão estruturada envolve procedimentos padronizados e se caracteriza como repetitiva e rotineira”. Ou seja, tal sistema admite que se tomem decisões semelhantes para situações semelhantes.

Audy, Andrade e Cidral (2005, p. 119) definem sistema de informação gerencial como “os sistemas de informação que sintetizam, registram, relatam a situação em que se encontram as operações da organização”. Ou seja, esse sistema resume e arquiva as atividades que estão sendo elaboradas no nível operacional, e as expõe ao nível estratégico, com o intuito de facilitar a tomada de decisão deste último.

5.2.3. Sistemas de Apoio à Decisão (SAD)

O sistema de apoio à decisão é usado para auxiliar na tomada de decisão do nível estratégico da empresa. Audy, Andrade e Cidral (2005, p. 121) afirmam que “os sistemas de apoio à decisão disponibilizam dados e técnicas para análise de problemas e oportunidades”. Ou seja, o sistema oferece os dados e as técnicas aos profissionais responsáveis por tomarem as decisões, e estes modelam a situação de forma a torná-la a mais adequada possível à situação em questão.

Audy, Andrade e Cidral (2005, p. 121) definem sistema de apoio à decisão como:

> Os sistemas de informação que auxiliam os gerentes de uma organização a tomar decisões semiestruturadas, com base em dados obtidos dos sistemas de informação gerencial, dos sistemas de processamento de transações e fontes externas. Além disso, esses sistemas disponibilizam ferramentas que permitam ao usuário realizar

> análises e simulações como forma de comparar o impacto de diferentes decisões.

Logo, esse tipo de sistema ajuda a definir qual o melhor caminho a ser seguido pela organização, levando-se em consideração os dados obtidos do SPT, do SIG e de fontes externas, minimizando os riscos e objetivando fazer a melhor escolha possível.

5.2.4. Sistemas de Informação Executiva (SIE)

Esse sistema também é utilizado pelo nível estratégico das organizações. Audy, Andrade e Cidral (2005, p. 122) definem sistema de informação executiva como:

> Os sistemas de informação que auxiliam os executivos do nível estratégico da organização a tomar decisões não estruturadas, a partir da disponibilização de um ambiente computacional e de comunicação que permita fácil acesso a dados internos e externos da organização.

Ao obter dados internos e externos da organização, o tomador de decisão obtém condições de decidir qual o melhor caminho para a empresa seguir, a melhor solução para as ameaças sofridas, ou a melhor oportunidade a ser praticada na empresa.

No entanto, Audy, Andrade e Cidral (2005, p. 122) afirmam que:

> Esses sistemas, a principio, não são projetados para resolver problemas específicos, mas para fornecer ferramentas que permitam aos executivos compreender as situações de negócio, identificar problemas e oportunidades, decidir por alternativas de atuação e planejar e acompanhar ações.

Ou seja, os sistemas não tomam decisões. Quem toma decisões são as pessoas. Os sistemas só auxiliam o processo decisório, dando-lhes informações que ajudam a decidir entre duas ou mais alternativas.

Desta forma, Audy, Andrade e Cidral (2005, p. 123) asseguram que:

> Os sistemas de informação executiva permitem dar subsídios para que os executivos respondam a perguntas estratégicas para a organização. Em geral, esses sistemas são desenvolvidos na forma de um conjunto de recursos que permitem ao executivo extrair informações de acordo com suas necessidades em determinado momento.

Portanto, é possível extrair do sistema somente a informação que se deseja naquele momento, tornando-a uma informação de qualidade, em tempo hábil para utilização. Pois de nada adianta obter uma informação segura, depois que se tomou uma decisão.

5.2.5. Sistemas de Gestão Integrada ou ERP

Existe ainda um tipo de sistema capaz de integrar os três níveis organizacionais. São os chamados sistemas de gestão integrada ou ERP's (Enterprise Resourse Planning).

Audy, Andrade e Cidral (2005, p. 125) afirmam que:

> O ERP promete resolver uma grande gama de desafios empresariais através da integração dos processos de negócio em uma única arquitetura integrada de informação, o que exige mudanças na estrutura da organização, no processo de gerenciamento, na plataforma tecnológica e na capacidade de negócios.

Portanto, quando ocorre a integração das informações em um único sistema, o processo de tomada de decisão fica mais fácil e rápido, pois é possível acessar informações de todos os setores em tempo real.

5.3. BENEFÍCIOS DOS SISTEMAS DE INFORMAÇÃO

Atualmente, ainda existem várias empresas que não possuem um sistema de informação gerencial, por considerarem isso um investimento de alto custo. Oliveira (2007, p, 188) vê como benefícios do SIG para as empresas os seguintes itens:

- Redução de custos das operações;
- Melhoria no acesso às informações, propiciando relatórios mais precisos e rápidos, com menor esforço;
- Melhoria na produtividade, tanto setorial quanto global;
- Melhoria nos serviços realizados e oferecidos;
- Melhoria na tomada de decisões, por meio do fornecimento de informações mais rápidas e precisas;
- Estímulo de maior interação entre os tomadores de decisão;
- Fornecimento de melhores projeções dos efeitos das decisões;
- Melhoria na estrutura organizacional, por facilitar o fluxo de informações;
- Melhoria na estrutura de poder, propiciando maior poder para aqueles que entendem e controlam o sistema;
- Redução do grau de concentração de decisões das empresas;
- Melhoria na adaptação da empresa para enfrentar os acontecimentos não previstos, a partir das constantes mutações nos fatores ambientais;
- Otimização na produção dos serviços aos clientes;
- Melhor interação com seus fornecedores;
- Melhoria nas atitudes e atividades dos funcionários da empresa;
- Aumento do nível de motivação das pessoas envolvidas;
- Redução dos custos operacionais;
- Redução da mão de obra burocrática;
- E redução dos níveis hierárquicos.

Portanto, ao analisar a viabilidade da implantação de um sistema de informação, devem-se observar as vantagens e desvantagens que um sistema trará para a organização. Se as vantagens forem mais atrativas do que as desvantagens e a organização optar pela aquisição de um sistema, ela deverá fazer o levantamento dos requisitos que esse sistema deverá ter, para atender

as suas necessidades sem perder de vista o aspecto financeiro do investimento, ou seja, mensurar as necessidades e o quanto a organização está disposta a investir na aquisição do sistema. Após isso, deve-se fazer uma pesquisa no mercado, para ver quais os sistemas que se encaixam melhor no seu ramo de atividade, se é mais vantajoso adquirir um sistema pronto ou comprar um sistema feito exclusivamente para ela. Por fim, planejar a aquisição e o mais importante, realizar um bom planejamento da implantação do sistema, envolvendo os colaboradores no processo de escolha para que não haja boicotes no processo de implantação. Por fim, resta efetuar a compra do sistema pretendido.

6. CONSIDERAÇÕES FINAIS

Atualmente, a tecnologia da informação é, sem dúvida nenhuma, um tema importante a ser tratado dentro das organizações, principalmente quando envolve a segurança da informação e a tomada de decisão.

A segurança é importante desde a coleta, processamento, armazenamento e distribuição dos dados. É a partir deles que serão geradas as informações e o conhecimento, necessários para a tomada de decisão. Informações inseguras geram insegurança nos tomadores de decisão, que, por sua vez, em alguns casos deixam de tomar decisões ou as tomam por intuição. Se o resultado da decisão tomada intuitivamente for positivo, a organização ficará satisfeita. Mas, se o resultado for negativo, pode inclusive comprometer a carreira profissional do administrador.

Para liberar crédito aos clientes, as instituições financeiras necessitam de informações como valor da renda mensal, se possuem restrições junto ao SPC ou Serasa, etc. Tudo isso, para decidirem pela liberação ou não do crédito e pelo valor da taxa de juros, dependendo do risco que a operação oferecer. Se não houvesse um sistema de segurança que funcionasse corretamente, qualquer pessoa poderia alterar essas informações, levando a instituição a decisões equivocadas que, por sua vez, poderiam, inclusive, comprometer a sobrevivência da instituição.

Nesse sentido, este estudo objetivou identificar e levantar junto à literatura, os conceitos e tecnologias associadas à segurança da informação e desta forma, criar e disponibilizar um material que possa ser consultado por organizações e indivíduos interessados no assunto, além de contribuir para o desenvolvimento do corpo de conhecimento associado à gestão das informações nas organizações.

REFERÊNCIAS

ALECRIM, Emerson. **O que é Tecnologia da Informação (TI)?** 24/fev./2011. Disponível em: <http://www.infowester.com/ti.php>. Acesso em: 07/set./2012

AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller; CIDRAL, Alexandre. **Fundamentos de Sistemas de Informação**. Porto Alegre: Editora Bookman, 2005.

BATEMAN, Thomas S.; SNELL Scott A. **Administração**: Novo Cenário Competitivo. 2 ed. _:Editora Atlas, 2006.

CÔRTES, Pedro Luiz. **Administração de sistemas de informação**. São Paulo: Editora Saraiva, 2008.

DE SORDI, José Osvaldo e MEIRELES, Manuel. **Administração de Sistemas da Informação:** Uma abordagem interativa. São Paulo: Editora Saraiva, 2010.

DE SORDI, José Osvaldo. **Administração da Informação:** Fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: Editora Saraiva, 2008.

FEGURY, Elizabete. **Gestão do Conhecimento**. 17/ago./2011. Disponível em: http://www.ici.curitiba.org.br/Multimidia/Documento/Artigos/ArtigoMBA_Elizabete.pdf. Acesso em: 22/jul./2013

FILHO, Antonio Mendes Da Silva. **Segurança da Informação:** Sobre a Necessidade de Proteção de Sistemas de Informações. Nov./2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm>. Acesso em: 04/abr./2013

HADDAD, Cláudia Maria Salles; JOÃO, Belmiro do Nascimento. **Ti Para A Tomada De Decisão Executiva:** Um Estudo Na Indústria Química Nacional. – Foz do Iguaçu: Associação Brasileira de Engenharia de Produção, 2007.

Harvard Business Review. **Tomada de decisão**. – Tradução de Eduardo Riech. – Rio de Janeiro: Editora Campus, 2001.

Instituto Antônio Houaiss. **Houaiss Eletrônico.** _: Editora Objetiva, 2009.

NONAKA, Ikujiro; TAKEUCHI, Hirotaka (1935). **Criação de conhecimento na empresa**. Tradução: Ana Beatriz Rodrigues, Priscila Martins Celeste. Rio de Janeiro: Editora Campus, 1997.

O' BRIEN, James A. **Sistemas de Informação e as decisões gerenciais na era da internet**. 2 ed. - Tradução Célio Knipel Moreira e Cid Knipel Moreira. – São Paulo: Editora Savaira, 2004.

OLIVEIRA, Jayr Figueiredo de. **Sistemas de Informação:** um Enfoque Gerencial Inserido no Contexto Empresarial e Tecnológico, 5. ed. – São Paulo: Editora Érica, 2007.

PINHEIRO, José Mauricio Santos. **Por que estudar Sistemas de Informação?** 28/set./2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_porque_estudar_sistemas_de_informacao.php>. Acesso em: 18/set./2012

REI, Lucia. **Diferença entre dados e informações**. 09/nov./2010. Disponível em: http://luciareisousatic.blogspot.com.br/2010/11/introducao-aos-sistemas-e-tecnologias.html. Acesso em: 19/ago./2013.

REZENDE, Ricardo. **Conceitos Fundamentais de Banco de Dados**. 16/abr./2006. Disponível em: <http://www.devmedia.com.br/conceitos-fundamentais-de-banco-de-dados/1649>. Acesso em: 26/set./2012

TURBAN, Efraim; RAINER, R. Kelly; POTTER, Richard E. **Introdução a Sistemas de Informação:** Uma Abordagem Gerencial. – Rio de Janeiro: Editora Elsevier, 2007.

Wikipedia, the free encyclopedia. **ENIAC**. Disponível em: http://en.wikipedia.org/wiki/ENIAC. Acesso em: 07/set./2013