

CENTRO PAULA SOUZA

GOVERNO DO ESTADO DE
SÃO PAULO

**Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise e Desenvolvimento de
Sistemas**

**SEGURANÇA DA INFORMAÇÃO E A
QUALIDADE DO SISTEMA DE INFORMAÇÃO
DA PREFEITURA DE LUIZIÂNIA – SP: UM
ESTUDO DE CASO**

TALES FRANCISCO ANTONINO GALANTE

**Americana, SP
2014**

CENTRO PAULA SOUZA

GOVERNO DO ESTADO DE
SÃO PAULO

**Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise e Desenvolvimento de
Sistemas**

**SEGURANÇA DA INFORMAÇÃO E A
QUALIDADE DO SISTEMA DE INFORMAÇÃO
DA PREFEITURA DE LUIZIÂNIA – SP: UM
ESTUDO DE CASO**

TALES FRANCISCO ANTONINO GALANTE
tales.galante@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da Fatec-Americana, sob orientação do Prof. Me. Alberto Martins Júnior

**Área: Segurança da Informação/
Sistemas de Informação**

Americana, SP
2014

BANCA EXAMINADORA

Professor Me. Alberto Martins Júnior
(Orientador)

Professora Ms. Luciene M. G. Castello
Branco

Professor Me. Wagner Cavalcanti

Gostaria de compartilhar este projeto com os meus familiares que, juntamente comigo, sofreram, torceram, sonharam e, acima de tudo, incentivaram-me para o bom êxito da conclusão da minha Monografia, pois me fizeram acreditar que é possível vencer desafios quando realizados com gosto e prazer.

AGRADECIMENTOS

Acredito que a vida é como um “campeonato” com várias etapas. Ora perdemos, ora ganhamos. Porém, tenho certeza de que nas vitórias nunca estamos sozinhos.

Logo na “largada” dessa minha corrida quero agradecer a Deus pelo dom da vida, vida que é o grande momento de todos nós. Com o meu nascimento ganhei uma família: pais, irmã (sou o caçula), avós, tios, primos,..., muitos parentes. Já nesse começo fui privilegiado: nasci num berço esplendido. Não em riqueza material, mas em riqueza divina: senti o que é o amor, maior riqueza de qualquer criatura humana, um calor tão gostoso que aprendi chamar de felicidade.

Na “reta” da vida fui acelerando com o apoio da família, colegas, amigos e professores. Dessa maneira venci a educação básica. Esses anos da educação infantil, ensino fundamental e ensino médio foram maravilhosos: muita determinação, muito estudo e o início das festas. Esse tempo parecia que não chegaria ao fim, mas chegou.

O término do ensino médio, para mim, foi como o início de uma “curva fechada”, tive que reduzir a velocidade e ficar mais atento. Era um momento de tomada de decisões. As incertezas e sonhos, dobradinhas difíceis de controlar, angustiaram-me causando muita ansiedade quanto ao meu futuro. Ingressar numa faculdade pública seria um grande desejo. Com a colaboração de amigos e professores, no cursinho, a família em casa e o meu esforço pessoal, consegui realizar a minha grande meta: ingressar na FATEC Americana.

Nessa nova “reta” na minha vida pude acelerar novamente. Com a companhia e ajuda da Mariana Bertelini, Camila Peracini e Jonatas Cruz, estive sempre seguro. Esse grupo foi responsável por vários ajustes e acertos no “motor do meu carro da vida”. Nos bastidores (boxe) contei também com a colaboração dos amigos de sala de aula: Eduardo, Adalto, Carlos, Junior Botelho. O incentivo e a torcida do Guilherme Orange e da Rúbia Pirovani também preciso destacar.

Com o término do meu TCC já estou avistando a chegada e o fim dessa corrida. Fizem-me vencedor. Obrigado, Professor Me. Alberto Martins Júnior – “Chefe de equipe”. Sua orientação segura e competente, seu estímulo constante e testemunho de seriedade permitiram-me concretizar este estudo. Agradeço-lhe também pela paciência e compreensão com as minhas limitações. Sua sabedoria foi imprescindível para a elaboração deste trabalho.

Agradeço novamente a toda a minha família, que sempre me apoiou em todas as minhas decisões, aos meus pais Claudemir Pedro Galante e Odila Pedrina Leite Antonino Galante por sua capacidade de acreditar e investir em mim. A minha irmã Natalia Antonino Galante por sua solidariedade e conforto nos meus momentos de impaciência.

Agradeço as minhas avós Hortência e Izaura, pelo carinho incondicional durante todo esse tempo e minha tia, Maria Aparecida Leite Antonino, pelo apoio prestado a mim durante toda a minha vida e principalmente durante minha graduação.

Agradeço ao Prefeito Rogélio, à sua esposa Maria Tereza e aos funcionários da Prefeitura de Luiziânia-SP, por permitirem que meu projeto se desenvolvesse.

Gostaria de registrar que os frutos que hoje os colho, na FATEC – Americana, foram plantados e cultivados por vocês – funcionários, professores e colegas de sala. Eu jamais os esquecerei. Vocês foram pessoas marcantes nesta etapa da minha vida.

Nesta hora de encerramento de uma etapa muito especial, em que a alegria por estar terminando junta-se à saudade, torna-se difícil lembrar-me de todos os amigos e pessoas que participaram da jornada, mas de uma maneira muito sincera, agradeço a todos, que de uma forma ou de outra colaboraram para a realização desta Monografia.

Meus sinceros agradecimentos!

“Eu sou parte de uma equipe.

*Então, quando venço, não sou eu apenas quem vence. De certa forma
termino o trabalho de um grupo enorme de pessoas”*

Ayrton Senna

RESUMO

Nos tempos atuais, a tecnologia está presente em todos os lugares. E nas organizações, esse cenário não é diferente, pois ela é de suma importância para se manter conectado no mundo moderno. Devido a isto, este projeto apresenta um estudo de caso de Segurança da Informação para uma organização, com o intuito de aprimorar o desempenho organizacional e, conseqüentemente, oferecer mais sustentabilidade ao negócio. Foram entrevistados alguns funcionários da organização, coletando informações quanto à situação de trabalho no momento atual e, posteriormente, foi proposta a adoção de alguns modelos funcionais de Segurança da Informação para solucionar os problemas relatados pelos colaboradores da organização com o intuito de evitar perda de informação, possibilitando assim, que os gestores possam realizar suas atividades de um modo mais eficiente.

Palavras Chave: Tecnologia da Informação, Segurança da Informação, Sistema de Informação.

ABSTRACT

Nowadays, technology is present everywhere. And when it comes to organizations, the scenario does not change, because the supreme importance is to keep it connected in the modern world. Because of that, this project presents a study of the practicability of Information Security for the organization, with the intention of enhancing its performance, and by that consequently offering more sustainability to the business. Some employees were interviewed, who gave information about the work situation at the moment, and afterwards, it was proposed the adoption of some of the Information Security models. In order to solve reported problems by the organization employees with the intention of avoiding the information loss, allowing the managers perform their activities in a more effective way.

Keywords: Information Technology, Information Security, Information System.

LISTA DE FIGURAS

Figura 1. Atividades dos Sistemas de Informação	23
Figura 2. Componentes de um Sistema de Informação	24
Figura 3. Organização da Segurança da Informação	31
Figura 4. Organização Interna.....	32
Figura 5. Dispositivos Móveis e Trabalhos Remotos.....	32
Figura 6. Diagrama.....	35
Figura 7. Fatores Motivadores da Governança de TI	37
Figura 8. Os Domínios e Componentes da Governança de TI.....	39

SUMÁRIO

1. INTRODUÇÃO.....	18
2. REVISÃO DE LITERATURA	22
2.1. Sistema de Informações (SI).....	22
2.2. Tecnologia da Informação	26
3. SEGURANÇA DA INFORMAÇÃO	29
3.1. Histórico	29
3.2. Organização da Segurança da Informação	30
3.3. Segurança Organizacional	33
3.3.1 Importância da Infraestrutura.....	33
3.3.2. Coordenação da Segurança da Informação.....	34
3.4. Políticas de Segurança	34
4. GESTÃO E GOVERNANÇA DE TI	37
4.1. Componentes da Governança de TI	39
4.2. Governança Corporativa.....	41
5. ISO 17799.....	43
5.1. Abordagens	44
5.2. Estrutura da Norma	45
6. ANÁLISE E DISCUSSÃO DOS DADOS	46
6.1. Aspectos do estudo de caso realizado na Prefeitura de Luiziana-SP	46
6.2. A Segurança da Informação na Prefeitura de Luiziana-SP	47
6.3. Considerações acerca da gestão Segurança da Informação na Prefeitura de Luiziana-SP	49
7. CONSIDERAÇÕES FINAIS.....	52
8. REFERÊNCIAS	54

1. INTRODUÇÃO

Atualmente, os principais agentes de transformação nas empresas têm sido a globalização e a tecnologia, responsável também pela maioria das inovações. A globalização aumenta a concorrência, dando mais opções para o cliente e oferecendo várias oportunidades. A tecnologia faz da velocidade a base da competição, obrigando as instituições a repensarem processos que um dia já foram eficientes. De acordo com Rezende e Abreu (2000, p.59): “A ação da Tecnologia da Informação e seus recursos, sem organização antecipada, não atinge seu principal objetivo de auxiliar a empresa em todos os seus processos e níveis de ação”.

Outro fator levado em grande consideração são as tomadas de decisões, em que se faz presente a Tecnologia de Informação. O auxílio da tecnologia no processo decisório das empresas é usado hoje em larga escala. Sistema de Informação, segundo Laudon & Laudon (2010, p.12):

Pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.

Observa-se que, nas últimas décadas, há uma mudança considerável nas atividades econômicas, bem como nas organizações em nível mundial. O mundo competitivo leva as empresas a buscarem uma redução de custo, desenvolvimento e organização de seu sistema e satisfação do usuário.

Nesse contexto, alguns pontos merecem uma ênfase especial, como a quantidade, a qualidade e o valor da informação. Segundo Gates (1999, p.21),

O modo como você reúne, administra e usa a informação determina se vencerá ou perderá. Há mais concorrentes. Há mais informação disponível sobre eles e sobre o mercado, que agora é global.

O autor aponta que as organizações que souberem utilizar e administrar as informações disponíveis de forma correta terão maiores chances de sair vencedoras no cenário globalizado da atualidade. Com esse grande desempenho da tecnologia da informação, resultando um mundo cada vez mais industrializado, é necessário obter a segurança da informação, bem como determinar as responsabilidades

relativas à segurança dentro da empresa. De acordo com Laudon & Laudon (2010, p.215):

Se você opera uma empresa hoje, precisa ter a segurança e o controle como prioridade. O termo Segurança abarca as políticas, os procedimentos e as medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação.

A Segurança da Informação é considerada um valor extremamente significativo, podendo representar vantagens estratégicas para quem a possui e sabe como aplicá-la. Atualmente a Segurança da Informação é utilizada fortemente como recurso estratégico, estando presente em todas as atividades que envolvem pessoas, processos, sistemas, custos, tecnologia etc.

O desafio das organizações é a utilização da TI para projetar e realizar a gestão de forma competitiva e efetiva, considerando-se que a Segurança da Informação é vital para gestão, organização e operação das instituições, e que:

A Segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negocio pode ter perdas que compromete, o seu funcionamento (FONTES, 2006, p.11).

Nesse ambiente econômico empresarial, as organizações reconhecem a necessidade de obter mais seguranças de suas informações, para preservar a confidencialidade, integridade e disponibilidade das informações. Devido a essa necessidade, o projeto visa ao estudo para garantir a qualidade do sistema da Prefeitura de Luiziânia tendo como prioridade a Segurança da Informação.

O estudo JUSTIFICA-SE pela importância da Segurança da Informação em um ambiente empresarial. Segundo Fontes (2008, p.6):

A informação sempre foi um dos bens mais importantes da organização. A diferença é que há alguns anos a informação mais crítica para a empresa poderia ser guardada e trancada dentro de uma gaveta.

Para que a gestão da Prefeitura de Luiziânia seja aprimorada e preparada para garantir a confiabilidade dos dados em tempo real, evitando perda ou roubo de informações, faz-se necessária o estudo e posteriormente uma implantação de um

sistema de segurança, para que haja melhor desempenho da empresa sem houver preocupação com as informações abordadas.

O PROBLEMA encontrado foi: A compreensão da sistemática dos departamentos da Prefeitura de Luiziânia é a questão fundamental a ser estudada, pois pela falta de acesso à informação de forma confiável é que se pode observar a viabilidade do estudo para encontrar a melhor maneira de corrigir o problema com a falta de segurança das informações dos departamentos. O estudo permite encontrar a melhor maneira de corrigir a perda ou roubo de informações.

A Prefeitura de Luiziânia neste momento enfrenta problemas referentes a documentos, formulários e controle das informações. Com o estudo, buscamos descrever a conduta adequada para a sua proteção.

A PERGUNTA que se buscou responder foi: O estudo é a possibilidade de implantação de um software diminuiriam os riscos de uma suposta invasão ao sistema?

As HIPÓTESES foram: a) A Segurança da Informação é utilizada para proteger o recurso informação contra os vários tipos de ameaças, minimizando os riscos relacionados com o negócio. b) Serão observados todos os trâmites da Prefeitura para analisar como será possível a integração dos departamentos para manter as informações seguras. c) Será feita uma análise detalhada da empresa e das funcionalidades do sistema usado por ela, para propor a melhor solução dos problemas que a empresa está enfrentando.

O OBJETIVO GERAL constitui em verificar o estudo do atual sistema e possivelmente a busca de um sistema mais eficaz, visando à Segurança da Informação da Prefeitura de Luiziânia.

Os OBJETIVOS ESPECÍFICOS foram: a) Levantar dados bibliográficos sobre a importância da implantação de um sistema de Segurança da Informação, visando conhecer os recursos existentes para evitar a perda ou roubo das informações em uma empresa. b) Verificar como as informações estão distribuídas nos

departamentos contidos na Prefeitura de Luiziânia no presente momento, buscando diminuir a taxa de erros. c) Analisar os benefícios que a implantação de um sistema de segurança trará para a Prefeitura, objetivando aumentar a qualidade e confidencialidade da empresa.

O MÉTODO CIENTÍFICO: do ponto de vista da sua natureza, a pesquisa é aplicada, pois procura solucionar problemas relacionados à segurança da informação e propor algumas soluções. Do ponto de vista da forma de abordagem, a pesquisa é qualitativa, pois procura a melhor solução para diminuir os riscos da empresa. Do ponto de vista dos objetivos, a pesquisa é exploratória e descritiva, pois busca demonstrar os benefícios da Segurança da Informação em um ambiente empresarial, em um estudo de caso. Há ainda o levantamento das informações que serão disponibilizadas pela empresa em destaque. Do ponto de vista dos procedimentos técnicos, a pesquisa é bibliográfica e experimental, pois a pesquisa foi realizada através de livros, teses e demais materiais acadêmicos disponibilizados na internet e biblioteca. Além da pesquisa acadêmica foi necessário realizar um acompanhamento para verificar o êxito do estudo e do sistema.

O trabalho foi estruturado em sete capítulos: o PRIMEIRO é a introdução, o SEGUNDO conceitua Sistema de Informação e Tecnologia da Informação, o TERCEIRO capítulo conceitua Segurança da Informação, o capítulo QUATRO conceitua Gestão e Governança de TI. O QUINTO versa sobre a ISO 17799, o SEXTO capítulo é o estudo de caso – Prefeitura Municipal de Luiziânia.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo SETE se reserva às considerações finais.

2. REVISÃO DE LITERATURA

2.1. Sistema de Informações (SI)

No cenário econômico-empresarial, devido à globalização e à competitividade as organizações precisam organizar de forma mais eficiente suas informações, para gerar excelentes resultados e diminuir os custos. Para isso, é necessário Sistema de Informação, que auxilie no processo de transformação dos dados em informação, possibilitando que essas informações sejam utilizadas pelos gestores para tomar decisões rápidas e corretas.

De acordo com Albertão (2001, p.75), a importância de um Sistema de Informação nas empresas está relacionada aos tomadores de decisão, sendo de fundamental importância para as organizações e seus gestores.

Rezende e Abreu (2000, p.62) conceituam Sistema de Informação como sendo “o processo de transformação de dados em informação que serão utilizadas na estrutura decisória da empresa e que proporciona a sustentação administrativa, visando à otimização dos resultados esperados”. Já Laudon e Laudon (2007, p.9) definem Sistema de Informação da seguinte maneira:

[...] um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.

Laudon e Laudon (2007, p.9) afirmam que um Sistema de Informação é constituído por três atividades essenciais que geram as informações que as empresas precisam para tomar as decisões, analisar os problemas, controlar operações e criar novos produtos ou serviços. São elas: entrada, processamento e saída.

A Figura 1 apresenta o esquema básico de um sistema baseado em computador ilustrando as três atividades básica descritas pelos autores Laudon e Laudon (2010).

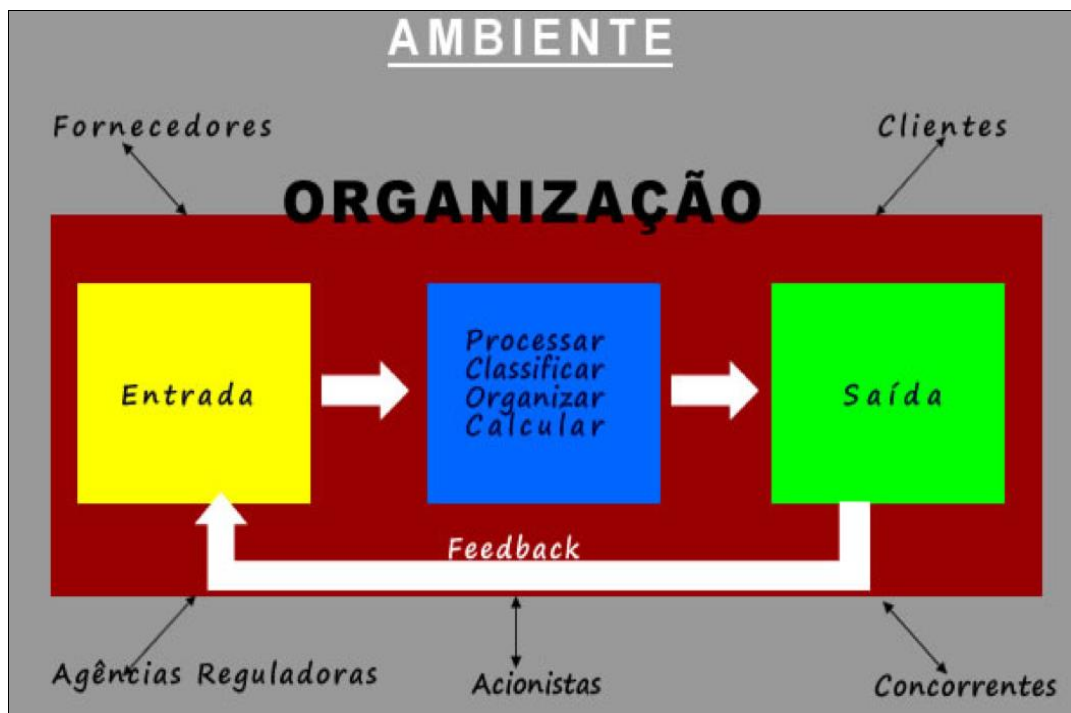


Figura 1. Atividades dos Sistemas de Informação

(Fonte: Laudon e Laudon 2010, p.13)

A entrada coleta ou captura os dados; o processamento converte ou transforma os dados em saídas úteis, e a saída transfere a informação útil às pessoas ou atividades em que ela será usada. Os Sistemas de Informação requerem ainda um feedback (avaliação), que é a saída devolvida aos membros das organizações para ajudá-los na avaliação ou na correção da fase de saída.

Desta forma, é possível afirmar que um Sistema de Informação é definido a partir da identificação de suas partes e a constatação de que as mesmas atuam em um mesmo sentido e direção, resultando em algo que pode ser definido como sendo seu objetivo.

O'Brien (2004, p.9) afirma ainda que os Sistemas de Informação são compostos por um conjunto de cinco componentes: recursos humanos, hardware, software, dados e redes, que executam atividades de entrada, processamento, produção, armazenamento e controle, com a finalidade de converter recursos de dados em produtos de informação. A Figura 2 apresenta, de forma ilustrativa, esse conceito.

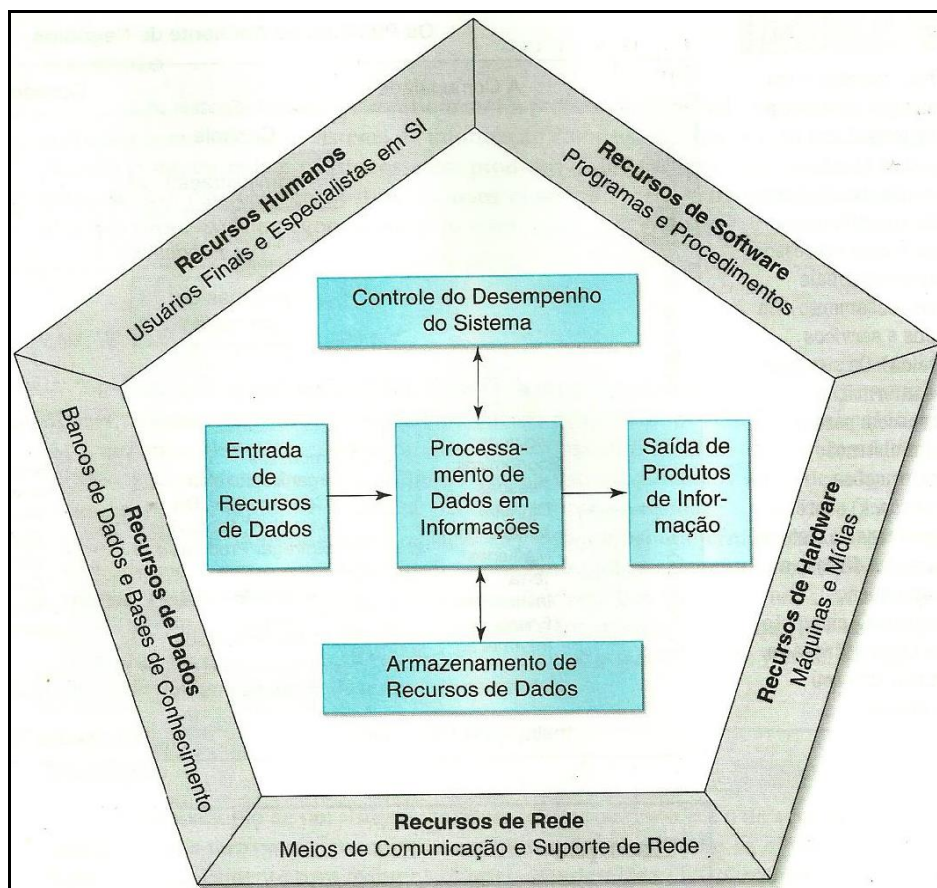


Figura 2. Componentes de um Sistema de Informação

(Fonte: O'Brien 2004, p.10)

A Figura 2 apresenta os componentes de um Sistema de Informação relacionados às atividades de entrada, processamento, saída, controle de desempenho e armazenamento de dados. Dentre esses, destaca-se o componente de recurso de dados, que tem como função armazenar todas as informações geradas pelo Sistema de Informação, sendo necessário planejar com muito cuidado a base de dados que dará suporte aos Sistemas de Informação.

Oliveira e Stair (1998) apud Rezende e Abreu (2000, p.63) relatam que:

Um Sistema de Informação eficiente pode ter um grande impacto na estratégia corporativa e no sucesso da empresa. Esse impacto pode beneficiar a empresa, os clientes/ou usuários e qualquer indivíduo ou grupo que interagir com os Sistemas de Informação.

Esses benefícios que as empresas procuram adquirir por meio dos Sistemas de Informação, segundo os mesmos autores, são:

- Suporte à tomada de decisão profícua;
- Valor agregado ao produto (bens e serviço);
- Melhor serviço e vantagens competitivas;
- Produtos de melhor qualidade;
- Oportunidade de negócios e aumento da rentabilidade;
- Mais segurança nas informações, menos erros, mais precisão;
- Carga de trabalho reduzida;
- Redução de custo e desperdícios;
- Controle das operações etc.

Os Sistemas de Informação têm como finalidade beneficiar seus usuários, procurando auxiliar na melhoria do conhecimento do mercado, aumentando sua capacidade de resposta, aperfeiçoando as comunicações e aprimorando as suas estratégias, além de converter os dados em informações. Segundo Laudon e Laudon (2007, p.9):

Dados são sequências de fatos brutos que representam eventos que ocorrem nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los. Informação quer dizer dados apresentados em uma forma significativa e útil para os seres humanos.

A informação só é importante para as organizações se existir alguém que a utilize. É inútil efetuar gastos com planejamento e implementação de Sistema de Informação se não forem utilizados pelo gestor e/ou as informações disponíveis não possibilitarem tomadas de decisões. É importante ressaltar que, para um Sistema de Informação ser implantado nas organizações, tem que respeitar a cultura organizacional adotada pelas empresas.

Deve-se levar em conta que a implantação de Sistema de Informação nas organizações apresenta características próprias, sendo necessário realizar estudos e planejamentos de acordo com os padrões de gerenciamento utilizados pela empresa, ou seja, a implantação de Sistema de Informação em uma empresa não é o mesmo realizado para outra. Outro ponto relevante é que as organizações tenham bem delineado o que necessitam, onde querem chegar e como será feita a implantações, determinando-se, dessa forma, prioridades e prazos, no contexto em que “Toda empresa, independentemente de seu negócio e meio de atuação, possui

cultura, filosofia e políticas, podendo ser definidas formal ou praticadas informalmente” (Rezende e Abreu, 2000, p.38).

Deve-se ressaltar que o Sistema de Informação adotado desempenha um papel extremamente importante para os negócios da organização, porém para atingir os resultados esperados o Sistema de Informação deve estar alinhado à Tecnologia de Informação, porque sendo ambos mal administrados, mal aplicados podem levar a empresa ao fracasso.

2.2. Tecnologia da Informação

Atualmente, estamos vivendo na era da informação, na qual as organizações têm como objetivo obter vantagem competitiva, inovação tecnológica e manter seus recursos centrados em dados e sua transformação em informação relevante.

Rezende e Abreu (2000, p.76) definem Tecnologia da Informação “como recursos tecnológicos e computacionais para geração e uso da informação” e ainda diz que “pode ser todo e qualquer dispositivo que tenha capacidade para tratar dados e ou informações, tanto de forma sistêmica como esporádica, quer esteja aplicado no produto, quer esteja aplicado no processo”.

Dentre os recursos de Tecnologia da Informação, são importantes:

- a) O Hardware, que compreende todos os equipamentos computacionais, de computadores e equipamentos de segurança ou mesmo de conexão de rede;
- b) O Software, que são todos os programas e que vão desde o Sistema Operacional até as ferramentas de produtividades, ou mesmo ferramentas de Banco de Dados;
- c) A Rede, que compreende toda estrutura de interligação entre computadores e equipamentos, como gerenciadores e concentradores de rede, bem como sua própria arquitetura;
- d) E o Dado, que Côrtes (2008, p.26) define como sendo:

[...] sucessões de fatos brutos, que não foram organizados, processados, relacionados, avaliados ou interpretados, representando apenas partes isoladas de eventos, situações ou ocorrências.

Atualmente as organizações precisam realizar investimentos na área de Tecnologia da Informação para tornar o ambiente complexo, garantir melhoria na qualidade dos serviços prestados, e, assim, aumentar sua produtividade e lucro.

Os avanços tecnológicos desafiam tanto os profissionais de TI, como os gerentes que participam da tomada de decisão de suas organizações. As organizações necessitam de gestores que, independentemente de serem bons usuários da área de informática, ou não, sejam conhecedores de tecnologia de computação que possa ser implementada profissionalmente nas empresas, sejam elas de pequena, médio ou grande porte, do setor público ou privado. Rezende e Abreu (2000, p.101) afirmam que “As empresas esperam que gestores não somente usem sistemas”, mas que também saibam utilizar a Tecnologia da Informação com intuito de transformá-las em organizações competitivas, participem no desenvolvimento de projetos, saibam administrar os recursos de informação da empresa, tenham conhecimento tanto em *Hardware* como *Software*, gerenciem a locação de recursos para projetos e possuam competência para sugerir novas utilizações para os Sistemas de Informação em suas organizações.

Hoje não se pode pensar em Tecnologia da Informação de forma isolada. É necessário analisar a cultura organizacional, as necessidades reais da organização, investimentos a serem feitos, e a realidade econômica da organização. E, caso não tenham o conhecimento em Tecnologia da Informação e de seus recursos, as empresas terão muitos problemas e dificuldades, principalmente nas atividades envolvendo Sistemas de Informação e Gestão da Tecnologia da Informação. Segundo Albertin (2001, p.36):

A TI tem grande influência na administração porque pode afetar:

- a produção, tanto física como intelectual, de qualquer produto ou serviço que a organização vende;
- a coordenação da organização, por seu poder de encurtar distâncias e diminuir tempo;

- a memória das organizações, por meio de seus bancos de dados.

Como este trabalho tem a finalidade de propor subsídios para o estudo da viabilidade de Segurança da Informação para um ambiente organizacional, julga-se necessário compreender sobre Tecnologia da Informação voltada para o mesmo ambiente, visto que em um Sistema de Informação faz-se necessário o uso de Tecnologia da Informação.

Acrescenta-se que através das Redes de Computadores, Internet, Intranet, Extranet, as pessoas e organizações mantenham-se conectadas o tempo todo, permitindo dessa forma que as trocas de informações sejam realizadas de maneira mais rápida e que, no caso da organização em estudo, essas informações possam ser trocadas entre os seus vários departamentos e entre ela e outras organizações.

É evidente a importância da Tecnologia da Informação para as organizações nos dias atuais, pois é através desses recursos que as empresas conseguem obter vantagens competitivas e conseguem desenvolver seus serviços de forma dinâmica e eficiente, independentemente do ramo de atuação, ou mercados com os quais se relacionam, além de oferecer condições para que a troca de informações e comunicação seja realizada de forma rápida e com maior frequência.

3. SEGURANÇA DA INFORMAÇÃO

3.1. Histórico

No passado questões como Segurança da Informação eram tratadas com maior simplicidade, pois os arquivos com informações de valores para as organizações eram trancados fisicamente, com a chegada da Tecnologia da Informação a questão ficou um pouco mais complexa.

Talvez não tivéssemos dado conta do quão importante é a informação nos dias de hoje. Podemos dizer que ela é um recurso que move o mundo, além de proporcionar o conhecimento de como o universo está caminhando. Segundo Fontes (2006, p.03), “Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional”.

Nos últimos anos as tecnologias de informação têm evoluído de forma significativa, proporcionando maior rapidez e eficiência para as organizações nas tomadas de decisões. Com isso podemos dizer que em uma organização a necessidade de usar sistemas de informação tornou-se de total importância, e as chances de não utilizá-los seria praticamente nula. Neste contexto a importância de se utilizarem mecanismos de Segurança da Informação é extremamente importante para a sobrevivência e competitividade das organizações.

Com a globalização influenciando novos processos tecnológicos, dentre eles a facilidade de adquirir informações, e considerando que hoje o meio de adquirir essas informações está cada vez mais fácil, é necessário que a informação seja protegida e gerenciada.

Segundo a ISO/IEC 17799 (p.VI), Segurança de Informação: “protege as informações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais”.

O termo **Segurança**, segundo Laudon e Laudon (2010, p. 215), “abarca as políticas, os procedimentos e as medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação”.

Informação seria todo conteúdo ou dado valioso para uma organização ou indivíduo, podendo ser qualquer conteúdo com capacidade de transferência ou armazenamento, que possui um propósito, sendo também de utilidade do ser humano.

A Segurança da Informação é um ponto crítico para a sobrevivência das organizações na era da informação, portanto fez-se necessário assegurar que a informação seja protegida adequadamente. Conforme a ISO/IEC 17799 (p.VI):

A segurança da informação é aqui caracterizada como a preservação de:

Confidencialidade: garantir que as informações sejam acessíveis apenas àqueles autorizados a terem acesso;

Integridade: salvaguardar a exatidão e inteireza das informações e métodos de processamento;

Disponibilidade: garantir que os usuários autorizados tenham acesso às informações e ativos associados quando necessário.

A informação existe em diversos formatos: impressa ou escrita, armazenada eletronicamente, falada em conversas etc. De qualquer forma, ela deve ser protegida adequadamente. Sendo assim, é de responsabilidade da Segurança da Informação protegê-la de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar riscos e maximizar o retorno dos investimentos.

3.2. Organização da Segurança da Informação

Como em qualquer ambiente onde se busca o melhoramento de qualquer recurso, o normal é entender o que está se passando para tomar as medidas necessárias, para corrigir, se for necessário.

No ambiente de Segurança da Informação segue-se o mesmo caminho; identificar os erros e a melhor maneira para corrigi-los. Organização da Segurança da Informação objetiva apresentar controles estruturados para gerenciar a

segurança da informação dentro do ambiente organizacional. Também objetiva controlar a segurança dos recursos de processamento da informação, quando disponíveis em trabalhos remotos e dispositivos móveis. A Figura 3 a seguir demonstra esse primeiro momento da organização da segurança da informação.

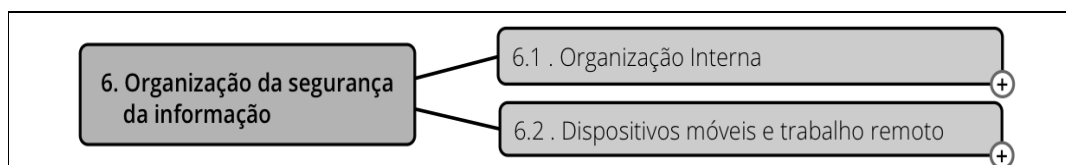


Figura 3. Organização da Segurança da Informação

(Fonte: Coelho, Araújo e Bezerra 2014, p.21)

Observa-se que a organização da segurança da informação é nesse primeiro momento dividida em duas categorias de organização: a primeira, Organização Interna, estabelece um suporte de gerenciamento para começar e inspecionar a inserção e operação da Segurança da Informação na instituição. A segunda, Dispositivos Móveis e Trabalho Remoto, busca garantias de segurança da informação no uso de dispositivos móveis e no trabalho remoto.

De acordo com as Figuras 4 e 5, analisam-se os principais controles de ambas as categorias apresentadas anteriormente. Verificam-se na Figura 4, os principais controles a serem elaborados para o melhoramento da organização em função da segurança da informação.

Esses controles buscam uma estruturação melhorada para o gerenciamento da segurança da informação no ambiente organizacional, atendendo seus processos de autorização, privacidade e contatos com outros grupos.

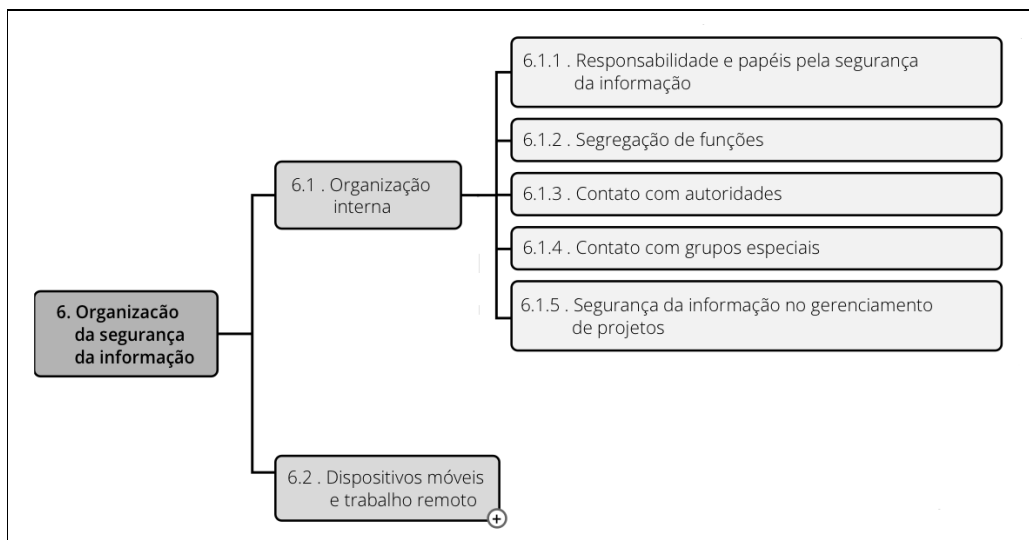


Figura 4. Organização Interna

(Fonte: Coelho, Araújo e Bezerra 2014, p.22)

Apresentam-se na Figura 5 controles fundamentais para que a organização obtenha o controle e o gerenciamento da segurança da informação no ambiente de trabalho remoto e na utilização de dispositivos móveis.

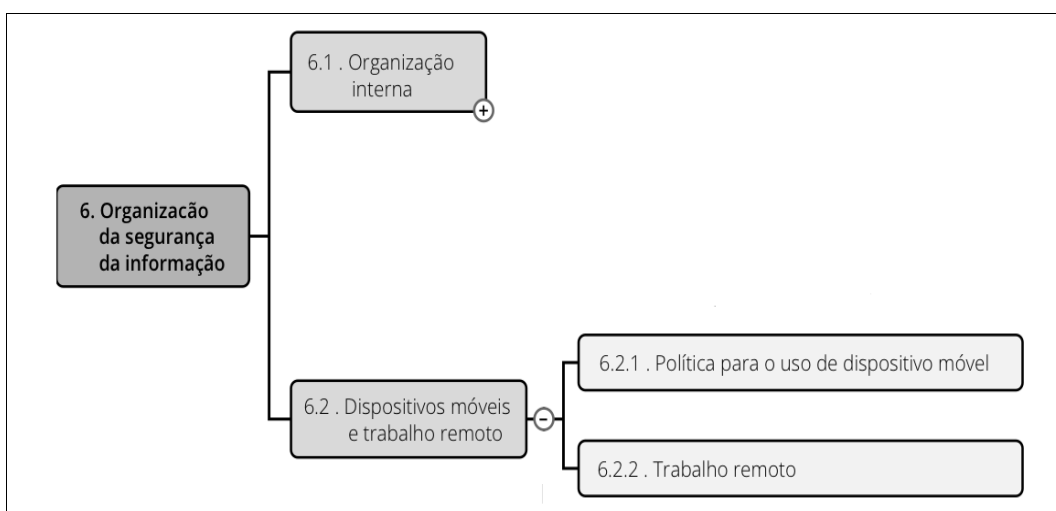


Figura 5. Dispositivos Móveis e Trabalhos Remotos

(Fonte: Coelho, Araújo e Bezerra 2014, p.21)

3.3. Segurança Organizacional

Como visto anteriormente, hoje a maioria dos arquivos de uma organização é digitalizada, portanto é portátil. Este fato fez que estes ativos se tornassem atrativos para ladrões. Outro fato a ser levado em consideração, os computadores conectando-se à internet e conseqüentemente a internet conectando-se a eles, possibilitando acessar locais com conteúdos de extrema importância para uma organização. Isso se tornou um grande problema no ambiente organizacional, fazendo com que muitas empresas estabelecessem uma estrutura organizacional para a segurança da informação.

Segundo a ISO/IEC 17799(p.03), Segurança Organizacional tem como objetivo: “Gerenciar a segurança das informações dentro da organização”.

É fundamental sentir-se seguro no seu próprio ambiente de trabalho, não possuir preocupações com qualquer informação que seja fundamental para sua organização. Cada vez mais interconectadas, as empresas têm necessidade de garantir e proteger as informações de ameaças e vulnerabilidade. Nesse contexto de segurança organizacional, é necessário analisar dois itens de extrema importância para obter uma infraestrutura organizacional para a Segurança da Informação, o primeiro seria a *Importância da Infraestrutura* e o segundo item, seria *Coordenação da Segurança da Informação*.

3.3.1 Importância da Infraestrutura

Objetivando fornecer todas as condições necessárias para a gestão da segurança da informação no ambiente organizacional, é aconselhável definir uma estrutura de gerenciamento para controlar a elaboração e implementação da Segurança da Informação.

Para garantir totalmente a segurança das informações em um ambiente de negócios, é necessário ainda, estabelecer uma infraestrutura que propicie o seu gerenciamento. Define-se primeiramente uma estrutura de gerenciamento próprio para o controle da implantação da Segurança da Informação.

3.3.2. Coordenação da Segurança da Informação

Busca a compreensão e colaboração entre os envolvidos (funcionários, dirigentes, consultores, auditores etc). É necessário um fórum interfuncional, envolvendo todos os setores a fim de implementar controles de segurança da informação. Segundo a ISO/IEC 17799 (p.03), esse fórum:

- a) Concorda sobre papéis e responsabilidades específicos para segurança da informação em toda a organização;
- b) Concorda sobre metodologias e processos específicos para segurança de informação, por exemplo avaliação de riscos e sistema de classificação de segurança;
- c) Concorda com e apoia iniciativas de segurança da informação que abrangem toda a organização; por exemplo, programas de conscientização sobre segurança;
- d) Assegura que a segurança seja parte do processo de planejamento de informação;
- e) Avalia a adequação e coordena a implementação de controles específicos para segurança de informação em novos sistemas ou serviços;
- f) Revisa os incidentes relacionados com a segurança de informação;
- g) Promove a visibilidade do suporte corporativo para a segurança de informação em toda a organização.

3.4. Políticas de Segurança

Voltada para estabelecer diretrizes e padrões que possibilitem garantir a integridade, confidencialidade e a disponibilidade de dados e informações corporativas, as políticas de segurança objetivam também fornecer direção e apoio gerenciais para a Segurança da Informação. De acordo com Coelho, Segadas de Araújo e Bezerra (2014, p.71), Políticas de Segurança podem ser definidas como:

- Conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos.
- Devem ser seguidas por toda a organização, orientando a segurança da informação, conforme o ramo de negócio, legislação e normas vigentes.
- A política de segurança deve ser clara e objetiva.

- E pode ser considerada um documento jurídico.

Com intenção de aumentar a segurança da infraestrutura, a política de segurança determina as regras e práticas a serem seguidas para garantir a segurança da informação. É constituída pela diretriz (serve de base para as normas), normas, procedimentos e instruções (referentes à Segurança da Informação). Abaixo, um diagrama que mostra a seqüência e a relação da política de segurança com fases do planejamento.

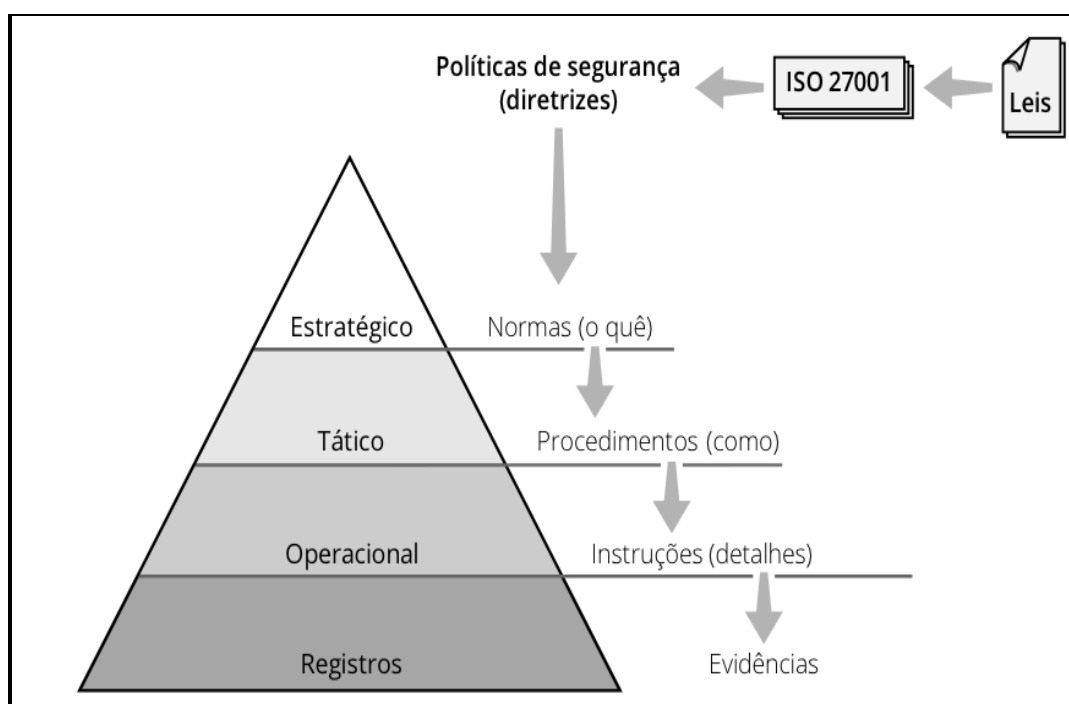


Figura 6. Diagrama

(Fonte: Coelho; Araújo e Bezerra 2014, p.72)

As **Políticas de Segurança** respondem ao “porquê” de realizar a Segurança da Informação, buscando definir as diretrizes necessárias para melhorar a segurança da informação dentro da organização. As **Normas** responde “o quê” fazer para alcançar as diretrizes que foram definidas na Política de Segurança, baseadas nas regras básicas de como devem ser implementadas, de acordo com as definição da política.

Procedimento responde “como” deve ser implementado o controle ou seu conjunto de controles. **Instruções**, explicam as operações para a execução da

implementação de controles de Segurança da Informação. Encerrando, temos **Evidências**, que permitem a coleta e comprovação da aplicação dos controles de Segurança da Informação.

4. GESTÃO E GOVERNANÇA DE TI

Governança de TI liga-se diretamente ao desenvolvimento estruturado de competência e habilidades estratégicas para profissionais de TI responsáveis pelo planejamento, implantação, controle e monitoramento de programas e projetos de governança. Buscando atender às necessidades organizacionais de aperfeiçoar, reduzir custos e alinhar o setor de TI às estratégias de negócio. Segundo Fernandes e Abreu (2012, p.14):

O principal objetivo da Governança de TI é alinhar TI aos requisitos do negócio, considerando solução de apoio ao negócio, assim como a garantia da continuidade dos serviços e a minimização da exposição do negócio aos riscos de TI.

Com a crescente dependência de TI nas operações do dia-a-dia, e também nas ações estratégicas, as corporações vêm aumentando sua atenção sobre a forma como a TI é governada. Na Figura 7 apresentam-se motivações para a implantação de programas de Governança de TI na visão de Fernandes e Abreu (2012, p.01).

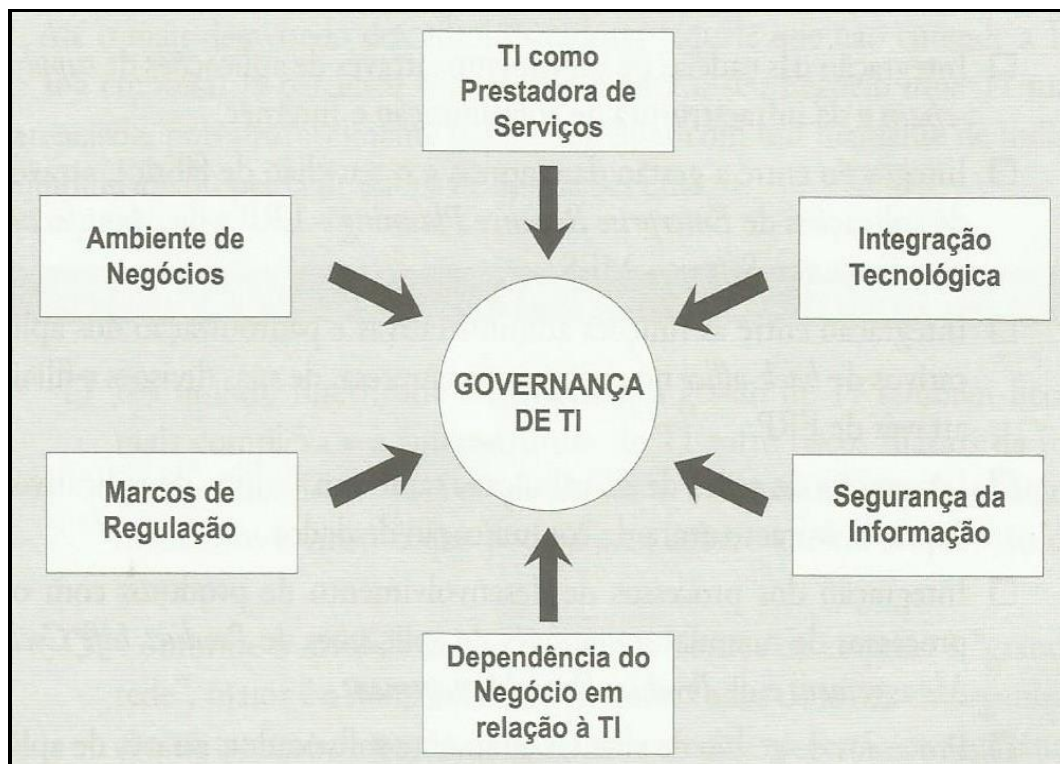


Figura 7. Fatores Motivadores da Governança de TI

(Fonte: Fernandes e Abreu 2012, p.01)

Como se observa na figura, a Governança de TI é motivada por alguns fatores:

- **Ambiente de Negócio** - que possui intensa competição, pois investidores exigem mais transparência na gestão.
- **Marcos de Regulação** - representam restrições ao negócio, mas devem ser seguidos, pois são ancorados em lei.
- **Integração Tecnológica** - integração de redes de distribuição, como componentes dos ambientes de Tecnologia da Informação (redes, servidores, aplicativos), buscando nesse fator de motivação maior entendimento.
- **Segurança da Informação** - com o mundo interligado da Internet, a gestão de TI também ficou mais aberta a tentativas diárias de roubo, fazendo com que a infraestrutura de TI mais vulnerável aos ataques a funcionalidade de seu sistema. Fernandes e Abreu (2012, p.9) dizem: “Conforme o nível de acesso dos vários pontos da empresa à “grande rede”, maior é a necessidade de envolver todos os níveis da organização na questão da gestão da TI e, em especial, na gestão da Segurança da Informação.”.
- **Dependência do Negócio** - as operações do dia-a-dia e as estratégias corporativas do negócio tornam-se cada vez mais dependentes da TI.
- **TI como Prestadora de Serviço** - segundo Fernandes e Abreu (2012, p.11):

Projetos dentro do prazo e orçamento, atendimento aos requisitos do negócio, disponibilidade das aplicações, disponibilidade da infraestrutura, capacidade para expandir o negócio, rápida resolução de incidentes e de serviços. Tudo isto requer postura e organização orientada à prestação de serviços.

Como qualquer organização do mundo globalizado almeja atender à crescente demanda por aumento de qualidade de produtos e processos, a alta

competitividade do mercado e a busca em minimizar custos e maximizar lucros buscam na Governança de TI o melhor caminho para atingir o sucesso.

4.1. Componentes da Governança de TI

Governança de TI envolve componente e mecanismo que possibilitam o desenrolar da estratégia de TI, até as operações dos produtos e serviços, quando esses componentes estiverem organizados para o seu funcionamento.

A figura 8 apresenta os componentes da Governança de TI dentro de cada domínio (ou etapa).

Figura 8 - Os Domínios e Componentes da Governança de TI

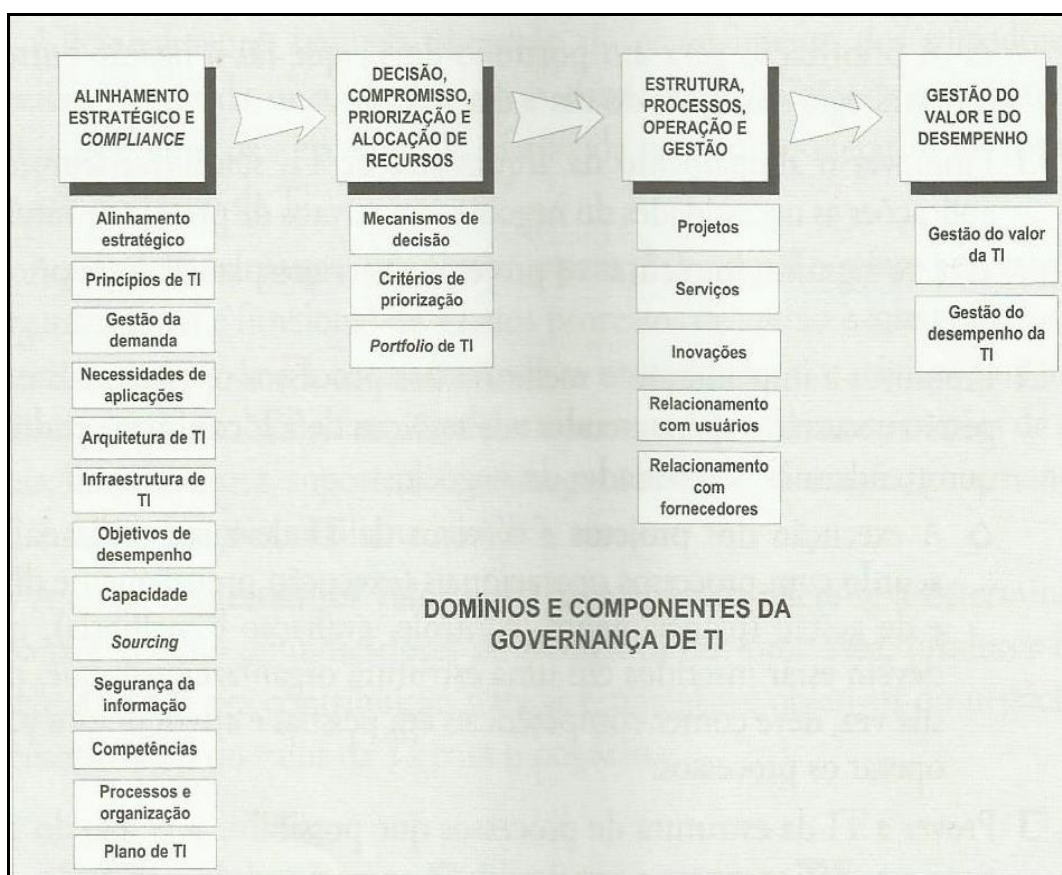


Figura 8. Os Domínios e Componentes da Governança de TI

(Fonte: Fernandes e Abreu 2012, p.16)

O processo de Alinhamento Estratégico e Compliance busca o melhor alinhamento da TI em termos de arquitetura, infraestrutura, aplicações, organizações e processo, analisando um planejamento estratégico da TI, que leva em conta as estratégias da organização para seus vários produtos e segmentos de atuação. Weill e Ross listam cinco decisões de TI (2006, p.11):

Princípios de TI – esclarece o papel de negócio da TI.

Arquitetura de TI – definindo os requisitos de integração e padronização.

Infra-estrutura de TI – determinando serviços compartilhados e de suporte.

Necessidade de aplicações de negócio – especificando a necessidade comercial de aplicações de TI compradas ou desenvolvidas internamente.

Investimentos e priorização de TI – escolhendo quais iniciativas financiar e quanto gastar.

Decisão, Compromisso, Priorização e Alocação de Recursos possuem grande responsabilidade pelas decisões, definem “quem decide o quê”, envolvendo a TI. Estrutura, Processo, Operações e Gestão buscam os locais onde acontece o atendimento, a interação dos usuários com a área de TI e interação dos fornecedores com a área de TI.

Gestão do Valor e do Desempenho pode ser dividido em dois conceitos: Gestão do valor da TI e Gestão do Desempenho da TI. Segundo Fernandes e Abreu (2012, p23), Gestão do Valor da TI “refere-se às atividades conduzidas para que a TI demonstre o seu valor para o negócio em termos de custos relativos, transformação do negócio e apoio à estratégia do negócio e as medições decorrentes.” Fernandes e Abreu (2012, p23) ainda diz em que Gestão do Desempenho:

[...] refere-se ao monitoramento dos objetivos de desempenho das operações de serviços em termos de desenvolvimento de aplicações, suporte e serviços, entrega de serviço, segurança da informação e o seu monitoramento, assim como dos acordos de níveis de serviço, acordos de níveis operacionais e níveis de serviços dos contratos de apoio.

Mas ambos buscam determinação, coleta e geração de indicadores de resultados dos processos, serviços e produtos de TI, e contribuem para estratégias e objetivos das organizações.

4.2. Governança Corporativa

“A Governança de TI está relacionada à Governança Corporativa e preocupa-se com o controle e a transparência das decisões em Tecnologia da Informação, sem desconsiderar mecanismos e processos para incrementar a eficácia da TI” Peterson (2004) apud Assis (2011, p.43). Governança de TI e Governança Corporativa não estão apenas sincronizadas, mas a primeira compõe em alguns fundamentos a segunda.

De acordo com o Instituto Brasileiro de Governança Corporativa – IBGC (2014), a Governança Corporativa consiste:

[...] sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para sua longevidade.

De acordo com (BEDICKS, 2012), a Governança Corporativa possui quatro princípios básicos:

Transparência – mais do que obrigação, é desejo de informar para gerar um clima de confiança interna e externamente à organização.

Equidade – não só entre sócios de capital, mas também entre todas as partes interessadas.

Prestação de Contas – quem recebe um mandato tem o dever de prestar contas de seus atos.

Responsabilidade Corporativa – visão de longo prazo, considerações de ordem social e ambiental.

Sendo um pilar muito importante para a economia global, a Governança Corporativa é considerada hoje como um instrumento determinante da

sustentabilidade das empresas. Com objetivo de examinar as questões centrais de governança e compreender os processos que a envolvem.

5. ISO 17799

Em 1987 o DTI (Departamento de Comércio e Indústria) do Reino Unido criou um centro de segurança da informação, o CCSC (Commercial Computer Security Centre), que objetivava criar uma norma de segurança das informações para o Reino Unido. Diversos documentos foram publicados, até que, em 1995, surge a British Standard 7799 (BS7799). Em 01 de Dezembro, a BS7799 ganha algumas alterações e sugestões, tornando-se a ISO/IEC 17799:2000 conhecida internacionalmente. Mas somente em Setembro de 2001 a ABNT homologou uma versão brasileira da norma, a NBR ISO/IEC 17799.

Reiterando o que se afirmou, sobre o quão importante é a informação em um ambiente de negócio, faz-se necessário protegê-la, pois organizações estão cada vez mais interligadas e competitivas no mercado, o que torna a informação um fator essencial para a manutenção e abertura de negócios. A Segurança da Informação seria um meio encontrado pelas organizações para proteger seus dados, com regras e controles rígidos, monitorados, implementados e estabelecidos diariamente.

De acordo com a ABNT NBR ISO/IEC 17799:2005 (2005, p.1), o objetivo dessa norma:

Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêm diretrizes gerais sobre as metas geralmente aceita para a gestão da segurança da informação.

ABNT NBR ISO/IEC 17799:2005 (2005, p.1) afirma ainda:

Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais.

A norma ISO/IEC 17799 sempre objetiva a Segurança da Informação, que é utilizada para prognosticar, prevenir e proteger qualquer tipo de advertência e vulnerabilidades nas informações encontradas em diversas formas (escritas, digitalizadas, gravações, imagens, etc.), que possuem valores para uma organização, pois sua violação traz prejuízos ou perda para o ambiente de negócio. Nesse ambiente de competitividade, de certa forma, no qual o grande conhecimento em Segurança da Informação pode ser um diferencial, a ISO/IEC 17799 busca facilitar seu domínio por meio de certificações.

Essa norma só pode ser adquirida com uma certificação, que consiste em um processo longo e muito trabalhoso devido à norma possuir um grande número de controles e requerimentos. Possuir o certificado ISO/IEC 17799 seria o diferencial buscado pelas organizações. Com a certificação, a organização mostra estar adaptada para tratar de dados de forma sigilosa. Sigilo e intangibilidade das informações são objetivados por todo mercado consumidor, que por sua vez está cada vez mais preocupado com a segurança das suas informações.

5.1. Abordagens

Buscando facilitar sua compreensão são disponibilizados alguns itens abordados pela norma:

- a) Estudo das exigências de Segurança da Informação em uma organização, e das necessidades de estipular uma política e objetivos para a Segurança da Informação. O primeiro passo a ser dado para a implantação da norma é o conhecimento dos motivos que estabelecem os padrões de Segurança da Informação adotados pela organização, para então definir os objetivos que a empresa deseja almejar com a aplicação da Segurança da Informação.
- b) Acompanhar e observar as críticas do desempenho e eficácia do Sistema de Gestão de Segurança da Informação (SGSI), resultados adquiridos pelo SGSI, que informa se o sistema atende aos objetivos propostos;

Sempre buscando as melhorias necessárias para a segurança das informações, baseando-se no modo como a organização se encontra no presente momento, mas almejando os objetivos que ela deseja alcançar.

5.2. Estrutura da Norma

A estrutura da ISO/IEC 17799 possui 11 seções de controle de Segurança da Informação. Cada seção contém um número de categoria de Segurança da Informação que, juntas, totalizam 39. Segundo a ABNT NBR ISO/IEC 17799:2005 (2005, p.4), as categorias são:

Política de Segurança da Informação (1);

Organizando a Segurança da Informação (2);

Gestão de Ativos (2);

Segurança em Recursos Humanos (3);

Segurança Física e do Ambiente (2);

Gestão das Operações e Comunicações (10);

Controle de Acesso (7);

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6);

Gestão de Incidentes de Segurança da Informação (2);

Gestão da Continuidade do Negócio (1);

Conformidade (3).

6. ANÁLISE E DISCUSSÃO DOS DADOS

Este capítulo apresenta o estudo de caso efetuado na Prefeitura de Luiziânia, demonstrando as técnicas e métodos utilizados, as características da organização em estudo e o cenário de Segurança da Informação observado nessa organização.

6.1. Aspectos do estudo de caso realizado na Prefeitura de Luiziânia-SP

Este estudo de caso objetiva descrever e observar a questão da gestão da Segurança da Informação na Prefeitura de Luiziânia. Para tal estudo, fixou-se o foco em dois tópicos relacionados à segurança da informação: políticas de segurança da informação e sistemas de informação.

O estudo de caso desta pesquisa foi de natureza exploratória e descritiva, como falado no início deste trabalho, sempre buscando identificar a real situação atual da Segurança da Informação na Prefeitura de Luiziânia, tema até então nunca abordado nessa organização. Sua abordagem, qualitativa, possibilitou o uso de técnicas e métodos de pesquisas.

- a) Observação Direta – Consiste em observar os controles de segurança presentes na organização, suas funcionalidades, a conduta dos colaboradores.
- b) Análise Documental – Foram considerados (o regimento interno) e a prévia da política de Segurança da Informação, que está sendo aperfeiçoada e será estabelecida em breve.
- c) Entrevistas – buscando a melhor solução e satisfazendo a todos na mesma organização, a entrevista foi feita por meio de questionários com questões relacionadas à TI e à Segurança da Informação, com usuários membros do ambiente de negócio que utilizam essas informações organizacionais. Tal questionário objetiva adquirir dados sobre a Segurança da Informação na Prefeitura de Luiziânia, observando os elementos destacados durante este trabalho e que se relacionam entre si, como políticas de segurança da informação, sistemas de informação e infraestrutura de segurança da

informação. As questões, motivadoras desta pesquisa, realizadas com funcionários e colaboradores da Prefeitura de Luiziana, foram:

01- Qual a importância de uma Política de Segurança da Informação para a Prefeitura de Luiziana?

02- Há estímulo por parte da Prefeitura de Luiziana para procedimentos de Segurança da Informação?

03- Os funcionários da Prefeitura de Luiziana possuem o conhecimento necessário sobre Segurança da Informação?

04- Qual o cenário atual da Prefeitura de Luiziana no que diz respeito à Segurança da Informação?

6.2. A Segurança da Informação na Prefeitura de Luiziana-SP

A segurança da informação na Prefeitura de Luiziana caracteriza-se como inicial, pois não houve anteriormente grande preocupação nesse sentido. A Política de Segurança da Informação da Prefeitura ainda está sendo produzida, mas já se tem decisões e ações importantes e algumas críticas à Segurança da Informação. Durante todo o tempo de estudo para o desenvolvimento deste trabalho, ficou bem claro que a participação de todas as áreas da Prefeitura é fundamental para o bom desempenho da empresa como um todo.

Este trabalho objetiva o melhoramento da segurança da informação na Prefeitura de Luiziana, a qual não possuía conhecimentos suficientes que esclarecessem a organização como um todo, as diretrizes, os princípios, necessidades e benefícios relacionados a Segurança da Informação para a Prefeitura.

Agora, medidas e procedimentos que garantem a segurança da informação de forma eficaz farão parte de um procedimento, que possibilitará a preservação das informações em sua confidencialidade, disponibilidade e integridade.

Anteriormente, preocupações com segurança da informação eram exclusivas para profissionais da área de TI, que buscavam estabelecer a segurança nos ativos tecnológicos. Essas medidas sem uma política explicando e fundamentando suas finalidades e estabelecendo as responsabilidades e regras envolvidas, em muitos casos, tornaram-se ineficazes. Observa-se essa dificuldade na implementação da Segurança da Informação isoladamente da TI, na resposta do tesoureiro da Prefeitura, quando questionado sobre a importância de uma Política de Segurança da Informação para a Prefeitura:

“... muitos dos controles de segurança da informação são entendidos como modismo da área de TI e a existência de uma política de segurança ajudaria a mudar esse entendimento.”

Outra dificuldade encontrada no ambiente de trabalho da Prefeitura de Luiziana é a conscientização e capacitação de alguns funcionários quanto à Segurança da Informação. Quando indagado, se os procedimentos de Segurança da Informação são estimulados pela Prefeitura, um funcionário do Administrativo respondeu:

“Estimula pouco. Penso que o estímulo está ligado a mostrar a importância de tais procedimentos e capacitar os seus executores para efetuar-los.”

Quando perguntamos para outro funcionário sobre o conhecimento que todos possuem sobre Segurança da Informação na Prefeitura:

“Ainda não há análise nesse sentido. No entanto, medidas pontuais para aumentar a segurança das informações já foram combatidas pelos usuários, pela ausência da política de segurança.”

Com essa preocupação dos membros da Prefeitura a respeito da segurança das suas informações, podemos dizer que seria um grande passo a elaboração de uma segurança da informação, podendo mostrar a importância da segurança organizacional não apenas como algo imposto pela TI. Quando se fala de Segurança da Informação, muitos a relacionam com segurança de ativos tecnológicos, quando

na verdade a Segurança da Informação é também um fator humano, de processos etc.

É importante, para obter-se o sucesso esperado, que a Prefeitura gerencie os riscos de segurança da informação aos quais está exposta, pela ausência de uma eficaz política de segurança da informação. E outro grande problema importante a ser tratado é o acesso de funcionários terceirizados às informações organizacionais. Quando um funcionário da Prefeitura foi questionado acerca da existência de requisitos de Segurança da Informação em contratos com terceiros, respondeu:

“Existem, mas os terceiros ainda possuem acesso a mais informações que o necessário para executarem suas funções.”

Um dos analistas da Prefeitura ilustrou o cenário no presente momento da Prefeitura de Luiziânia a respeito do de Segurança da Informação tanto para desenvolvimento e manutenção de SI, quanto para outros departamentos:

“Quando falamos em requisitos de segurança e segurança da informação, ainda estamos muito longe de um cenário ideal, ainda estamos dando os primeiros passos nessas questões. O contexto de segurança é bastante amplo. Acredito que faltam definições no que diz respeito à política de segurança, à organização de segurança da informação, à disseminação da cultura de segurança da informação, à implantação de métodos de desenvolvimento de aplicações seguras durante todo o ciclo de desenvolvimento. Como falei, estamos dando os primeiros passos.”

6.3. Considerações acerca da gestão Segurança da Informação na Prefeitura de Luiziânia-SP

Com o estudo de caso deste trabalho, foi identificada a real situação da Segurança da Informação da Prefeitura de Luiziânia. Observa-se o interesse da Prefeitura em estabelecer a gestão da segurança das suas informações buscando dados, referências para atender de forma satisfatória a todos os requisitos de segurança da informação.

Abaixo, são expostas algumas considerações sobre alguns fatores críticos para se obter o sucesso na implantação da Segurança da Informação, apontadas em ABNT NBR ISO/IEC 17799:2005 (2005), e a estruturação da Segurança da Informação na Prefeitura.

- a) **Política de Segurança da Informação:** como já citado anteriormente, a Prefeitura não possui ainda uma política de segurança da informação definida, necessária para determinar as regras e práticas a serem seguidas.
- b) **Participação de todas as áreas da Prefeitura:** é necessário o entendimento de quão importante é a Segurança da Informação para uma organização de todo o corpo trabalhador da Prefeitura, já para facilitar o seu tratamento em todo o ambiente organizacional, não somente da TI.

De acordo com o estudo de caso já explicado anteriormente, observa-se que a gestão da Segurança da Informação na Prefeitura é um processo em desenvolvimento, Então é necessário que, nessa etapa de implantação, assim como nas posteriores, a Segurança da Informação seja tratada com muita atenção, direcionando-se a gestão da segurança da informação de acordo com as necessidades da Prefeitura. Com uma boa aplicação de seus requisitos e recursos necessários (resultados alcançados e investimentos financeiros), a Segurança da Informação será reconhecida na Prefeitura e maximizará a qualidade de trabalho da organização.

Outro ponto importante a ser observado é que a Prefeitura teria que gerenciar mais os riscos de segurança da informação a que ela está sujeita. Assim os ativos de TI e de negócios são protegidos das ameaças que exploram suas vulnerabilidades acarretando danos a esses ativos e conseqüentemente à Prefeitura de Luiziana.

Com uma política de segurança da informação adequada, o reconhecimento dos membros da Prefeitura de Luiziana sobre a importância dessa segurança para a organização, o gerenciamento dos riscos e o seu entendimento (ISO 17799) são os primeiros passos para minimizar os riscos com a perda de informação na Prefeitura.

Com esse estudo, espera-se que haja melhora no ambiente de trabalho, que a Prefeitura possa ter a continuidade de seus negócios.

7. CONSIDERAÇÕES FINAIS

Como já se afirmou durante todo este trabalho, o processo da globalização trouxe algumas facilidades no ambiente tecnológico, mas também algumas complicações. Uma delas seria o quão a informação ficou vulnerável em alguns ambientes organizacionais nos quais a Segurança da Informação não se faz presente.

Nesse contexto, e tomando como exemplo a Prefeitura de Luiziânia, a qual permitiu a realização do estudo de caso, mostrou-se como uma organização desprotegida pode ter o seu ambiente de trabalho afetado, consequentemente afetando a qualidade de seu funcionamento.

O estudo de caso realizado buscou a melhor saída para o problema encontrado na Prefeitura de Luiziânia, baseada em questionários com perguntas de fácil entendimento por parte de todos os membros da organização.

Por meio deste trabalho e do estudo de caso que ele abrangeu, foi possível entender um pouco mais da estrutura da gestão da Segurança da Informação da Prefeitura de Luiziânia. Durante todo o processo, observou-se que a segurança da informação na Prefeitura está em um estágio inicial, com ausência de uma política de segurança da informação para o embasamento de uma estrutura e ações a serem tomadas a respeito desse assunto.

Outro destaque se dá à importância de alguns fatores, sem os quais não se atinge o sucesso esperado: participação de todas as áreas e a compreensão da segurança da informação como uma questão sistemática. O trabalho demonstra alguns benefícios da ISO 17799, que facilitará o melhoramento da segurança da informação, pois é voltada para esse assunto.

Após a finalização do projeto, fica claro que hoje a Segurança da Informação é indispensável para qualquer organização. Se esta tiver como foco principal um ambiente de trabalho satisfatório e priorizar a segurança de suas informações para

minimizar os riscos de perda ou roubo e maximizar sua qualidade, então um ambiente de Segurança da Informação se faz necessário.

8. REFERÊNCIAS

ALBERTÃO, Sebastião Edmar. **ERP Sistemas de gestão empresarial**: metodologia para avaliação, seleção e implantação. São Paulo: Iglu, 2001.

ALBERTIN, Alberto Luiz. **Administração de informática**: funções e fatores críticos de sucesso. 3ªed. São Paulo: Atlas, 2001.

ASSIS, Célia Barbosa. **Governança e Gestão da Tecnologia da Informação**: Diferenças na Aplicação em Empresas Brasileiras. São Paulo, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago-2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago-2002. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 17799**: Tecnologia da Informação – Código de Prática para Gestão da Segurança de Informações.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**: ABNT NBR ISO/IEC 17799:2005. 2ªed. Rio de Janeiro, 2005.

BEDICKS, Heloisa B. **Princípios de Governança Corporativa**. São Paulo, 2012. Disponível em: http://www.bmaiscompet.com.br/arquivos/Principios_Governanca_IBGC.pdf < Acesso em: 14 Maio 2014 às 17h31min.

COELHO, Flávia Estévia S., ARAÚJO, Luiz Geraldo S., BEZERRA, Edson K. **Gestão da Segurança da Informação**: NBR 27001 e NBR 27002. Rio de Janeiro: RNP/ESP, 2014.

CÔRTEZ, Pedro Luiz. **Administração de Sistemas de Informação**. São Paulo: Saraiva, 2008.

FERNANDES, Aguinaldo A., ABREU, Vladimir F. **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços**. 3ªed. Rio de Janeiro: Brasport, 2012.

FONTES, Edison. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

_____. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GATES, Bill. **A Empresa na Velocidade do Pensamento**: com um sistema nervoso digital. São Paulo: Companhia das Letras, 1999.

IBGC - Instituto Brasileiro de Governança Corporativa
<<http://www.ibgc.org.br/inter.php?id=18161>> Acesso em: 06 Junho 2014 às 15h54min.

LAUDON, Kenneth, LAUDON, Jane. **Sistemas de Informação Gerenciais**. 7ª ed. São Paulo: Pearson Prentice Hall, 2010.

_____. **Sistemas de Informação Gerenciais**. 7ª ed. São Paulo: Pearson Prentice Hall, 2007.

O' BRIEN, James A. **Sistemas de Informação e as Decisões Gerenciais na era da Internet**. 2ªed. São Paulo: Saraiva, 2004.

REZENDE, Denis Alcides, ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000.

WEILL, Peter, ROSS, Jeanne w. **Governança de TI**: Tecnologia da Informação. São Paulo: M. Books do Brasil Editora Ltda, 2006.


ANEXO A – Autorização para coleta de informações da Prefeitura de Luiziana**PREFEITURA MUNICIPAL DE LUIZIÂNIA**

Praça Benedito Cláudio, 135 – LUIZIÂNIA – SP – CEP:16.340-000 Fone: (18) 3603 1208
E-mail: prefeitura@luiziania.sp.gov.br

AUTORIZAÇÃO

A Prefeitura Municipal da cidade de Luiziana, Estado de São Paulo, autoriza o recolhimento de informações mediante a aplicação de questionários e realização de entrevistas com os secretários, para fins de trabalho acadêmico. Sendo assim, eu, Rogélio Cervigne Barreto, Prefeito Municipal de Luiziana, portador do RG. 21.957.983, autorizo o estudante Tales Francisco Antonino Galante, portador do RG. 47.937.891-5, estudante do curso de Análise e Desenvolvimento de Sistema, da FATEC Americana, a realizar os procedimentos acima descritos e utilizar os dados obtidos na construção de seu trabalho monográfico. Sem mais.

Luiziana, 02 de Dezembro de 2013.


ROGÉLIO CERVIGNE BARRETO
Prefeito Municipal de Luiziana - SP
RG. 21.957.983