



ISSN: 1696-8352 - BRASIL – ENERO 2016

## **UM ESTUDO INTRODUTÓRIO E APLICAÇÃO PRÁTICA DE SEUS BENEFÍCIOS PARA UMA EMPRESA DE RECICLAGEM DE JUNDIAÍ-SP**

Lucas Fernando Stoco

Juliano Schimiguel

### **RESUMO**

Este trabalho tem como objetivo geral estudar os principais benefícios que a segurança em tecnologia da informação (TI) vem a oferecer às organizações, sob o ponto de vista estratégico e empresarial. É um trabalho de abordagem qualitativa, baseado em pesquisa bibliográfica e de estudo de caso de uma empresa que atua no setor de reciclagem de garrafas PET, situada em Jundiaí-SP. Através desse estudo se concluiu que a informação representa um ativo para qualquer empresa hoje, e deve receber segurança diante das vulnerabilidades e dos crimes que envolvem o mundo virtual, justificando assim, o investimento para a mesma.

**Palavras-chave:** Segurança, Informação, Tecnologia, Empresa.

### **ABSTRACT**

This work has as main objective to study the key benefits that security in information technology (TI) is to provide organizations, from a strategic point of view and business. It is a qualitative study, based on literature review and case study of a company engaged in PET bottle recycling sector, located in Jundiaí-SP. Through this study it was concluded that information is an asset for any business today and should be given before the security vulnerabilities and crimes involving the virtual world, thus justifying the investment for the same.

**Keywords:** Security, Information, Technology, Company.

## 1.INTRODUÇÃO

No atual contexto em que as empresas se encontram, isto é, em um ambiente de negócios regido pela globalização e que tudo gira em torno da informação, faz-se de suma relevância discorrer sobre a segurança da informação.

É observável que nem toda informação é crucial ou fundamental a ponto de merecer maiores cuidados, mas, como bem ressalta Laureano (2005), certa informação pode ser tão importante que o custo de sua integridade será justificável.

Portanto, no ponto de vista de uma empresa, o sistema de informação representa uma solução organizacional e administrativa alicerçada na tecnologia de informação com o intuito de enfrentar um desafio constituído pelo ambiente. Desse modo, um sistema de informação pode ser essencial para qualquer organização e, ter o controle sobre este ambiente é elemento-chave para a qualidade dos serviços oferecidos por uma empresa independentemente de qual é o seu ramo de atividades.

A informação tem papel fundamental tanto na definição, como na execução de uma estratégia, a qual é relevante às empresas de diferentes setores, como por exemplo, o de reciclagem, que busca eficiência em suas operações e melhores condições competitivas no mercado. Com vista a esse conceito, propõe-se o presente estudo.

Para os negócios, a informação pode ser considerada como um ativo, que resguarda um valor para a organização, principalmente as de grande porte, muitas vezes se tornando o seu principal patrimônio. Porém, como aponta Dias (2000) esse patrimônio pode se encontrar em constante risco.

Sob esse raciocínio, formulou-se o seguinte problema de pesquisa: A segurança em tecnologia da informação pode proporcionar benefícios também para as

organizações de pequeno porte, sendo considerada um fator de sucesso crítico e de fundamental importância do ponto de vista estratégico e empresarial?

Em hipótese, a segurança em tecnologia de informação pode ser uma boa opção para a empresa, mesmo as de pequeno porte que estima resguardar a veracidade e integridade de suas informações, e assim, utilizá-las de forma a contribuir para suas tomadas de decisão e conseqüentemente em suas ações estratégicas, mesmo que seja necessário de início arcar com um investimento mais elevado para esse processo.

Em grande parte dos países, como no Brasil, é preciso que usuários de computador, quanto e principalmente as empresas estejam em constante alerta sobre os perigos que predominam no mundo digital, cuja segurança para proteger de eventuais danos ou vazamentos de informações importantes se faz relevante se tornando um instrumento que contribui para minimizar os crimes digitais, uma vez que as leis específicas contra esse tipo de delito ainda são muito atenuantes.

O objetivo geral desse trabalho, por sua vez, é estudar os principais benefícios que a segurança em tecnologia da informação possa oferecer às organizações, sob o ponto de vista estratégico e empresarial.

Este trabalho segue uma abordagem qualitativa, de objetivos exploratórios, de natureza aplicada, composto por pesquisa bibliográfica e do estudo de caso de uma empresa de reciclagem, localizada em Jundiaí-SP.

Com este estudo pretende-se contribuir para maior conscientização por parte de profissionais da área de tecnologia, quando de administração sobre a importância da segurança da informação em suas empresas.

## **2.REVISÃO BIBLIOGRÁFICA**

O interesse pela segurança da informação por parte das organizações tem crescido em todo o mundo, tanto em organizações públicas, quanto nas privadas, em que ambas tem buscado meios que contribuam nessa empreitada, e assim, consigam obter benefícios nesse novo contexto regido pela competitividade, visando, portanto, um uso eficiente e ao mesmo tempo, econômico dos inúmeros recursos da Tecnologia de Informação (TI).

À luz desse raciocínio, elabora-se a presente revisão bibliográfica que aborda alguns pontos relevantes ao embasamento desse estudo, como, a relação comunicação e a informação, a conceituação de informação e segurança, principais aspectos sobre a Tecnologia da Informação e uma explanação sobre crimes digitais, riscos e políticas e por fim mencionar alguns mecanismos para o controle de segurança da informação.

### **2.1.Comunicação e Informação**

A sociedade moderna cada vez mais tem dependido das formas de comunicação para se manter e fazer com que os processos fluam adequadamente. A comunicação pode ser definida como: *“O processo de troca de informação.”* (STRAUBHAAR; LAROSE, 2004, p. 5)

O processo de comunicação se divide em oito elementos sendo:

1. A fonte é a originadora da comunicação.
2. A mensagem é o conteúdo da comunicação, a informação a ser trocada.
3. O codificador traduz a mensagem para um formato passível de ser comunicado – geralmente um formato que não pode ser diretamente interpretado pelos sentidos humanos.
4. O canal é o meio ou sistema de transmissão utilizado para transferir a mensagem de um lugar a outro.
5. O decodificador reverte o processo de codificação
6. O receptor é o destino final da comunicação.

7. Um mecanismo de resposta (*feedback*) entre a fonte e o receptor pode ser utilizado para regular o fluxo da comunicação.
8. Ruído é qualquer distorção indesejada ou erro que pode ser introduzido durante a troca de informação. (STRAUBHAAR; LAROSE, 2004, p. 5)

A comunicação pode ser intrapessoal, sendo uma troca de informação do ser humano com si próprio, como com os seus próprios pensamentos, suas anotações, ou ainda, digitando um texto no computador, como forma de comunicação intrapessoal mediada eletronicamente. A comunicação também pode ser interpessoal, a qual abrange todas as trocas de informações e é composta por dois ou mais indivíduos. (STRAUBHAAR; LAROSE, 2004)

A comunicação em massa, no entanto, é o meio por qual se passa a mensagem através de uma única fonte para muitos receptores, como por exemplo, os jornais, tv, entre outros. Porém, em suma existem ainda outras formas de comunicação, e, com o avanço tecnológico as transformações são diversas. (STRAUBHAAR; LAROSE, 2004)

A figura 1 a seguir reúne alguns tipos de comunicação.

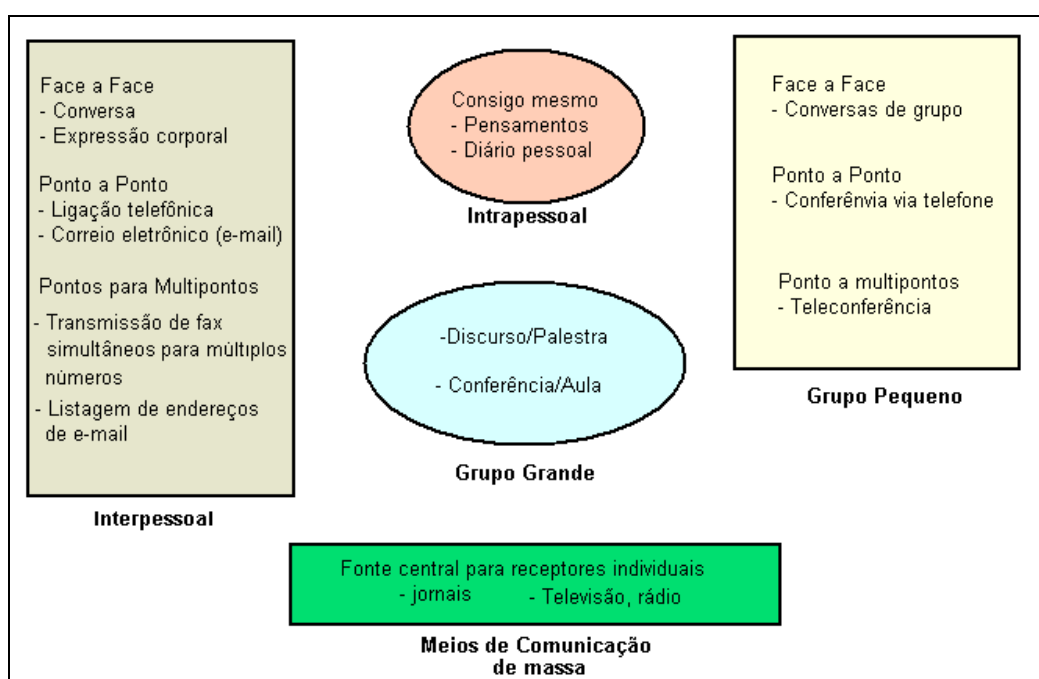


Figura 1- Tipos de Comunicação  
Fonte: Adaptado de (STRAUBHAAR; LAROSE, 2004).

Outra forma de caracterizar a comunicação é através de seu grau de interatividade. Entretanto, definir tal expressão não é tarefa tão fácil, uma vez que, interativo pode ser sinônimo de “duplo sentido”. Jogos de computador, por exemplo, ficam mais difíceis à medida que o usuário atinge uma pontuação, e, sistemas de transação, como o acesso bancário, são bons exemplos de interatividade. (STRAUBHAAR; LAROSE, 2004)

Nos exemplos da Figura 1, o curso da troca de informação é continuamente modificado, dependendo das reações do outro usuário.

Muito provavelmente o modelo ideal de interatividade seria um sistema que passasse no chamado teste de Turing, assim nomeado em homenagem ao inglês Alan Turing, matemático e pioneiro da computação. Para passar nesse teste, um sistema de informação deve ser capaz de convencer usuários que estes estão interagindo com um ser humano não com uma máquina. No outro extremo, o termo “interatividade” é algumas vezes utilizado para descrever qualquer situação na qual o conteúdo de um sistema extensivo de mídia é passível de ser selecionado e individualmente configurado (*customized*, na expressão em inglês) pelo usuário. (STRAUBHAAR; LAROSE, 2004, p. 11)

Outro exemplo de comunicação interativa são os sistemas de computação em rede que possibilitam ao usuário configurar sua própria versão de um jornal diário a partir de uma ampla biblioteca de informação digital.

De uma forma geral, a força da comunicação e a necessidade de informação são elementos da gestão do conhecimento. (CHIAVENATO, 2005)

Sendo que, a distribuição da informação requer um novo modelo de tecnologia de informação e gestão, assim, a empresa inserida na sociedade da informação e do conhecimento deve se encontrar atenta a fim de captar as vantagens da utilização das modernas tecnologias da informação e de sua respectiva segurança, o que resultará em maior competitividade.

A Tecnologia da Informação (TI) oferece, portanto, as ferramentas e o meio que as informações são transmitidas e compartilhadas, ressaltando que nesse contexto, as

distâncias são abolidas, promovendo uma rápida transferência de conhecimento entre os indivíduos e grupos. (LEHMKUHL, 2008)

## **2.2.A Tecnologia da Informação e as Empresas**

Graças ao avanço da Tecnologia da Informação (TI), muitas operações que antes as empresas não conseguiam realizar, hoje estão realizando. As organizações usam a TI buscando a minimização de custos, bem como para conquistar vantagens competitivas, no melhor atendimento ao cliente, e ainda, nas operações entre os membros da equipe de trabalho.

A TI vem demonstrando o quanto é relevante através de sistemas e no avanço dos *hardwares*. O tratamento das informações em um passado não muito distante é explicado:

Antigamente, o fluxo de informações baseava-se principalmente em papel, resultando em uma transferência de informações lenta, pouco confiável e propensa a erros. O custo decrescente da tecnologia, associado a sua maior facilidade de uso, permitem aos executivos poder contar com meios para coletar, armazenar, transferir e processar dados com maior eficiência, eficácia e rapidez. A transferência e o gerenciamento eletrônico de informações proporcionam uma oportunidade de reduzir os custos logísticos através da sua melhor coordenação. Além disso, permite o aperfeiçoamento do serviço baseando-se principalmente na melhoria da oferta de informações aos clientes. (NAZÁRIO, 2013, p. 2)

Os fatores tecnológicos produzem um efeito mais decisivo nos negócios, já que as mudanças são extremamente ágeis no ambiente externo e assim, sentidas pelas empresas. (MONTANA; CHARNOV, 2011)

Entretanto, uma empresa pode estar completamente comprometida com uma forma tecnológica, ter realizados altos investimentos em equipamentos e treinamento de pessoal, mas, de um momento para outro, pode surgir uma nova tecnologia, mais inovadora e menos custosa. A exemplo, menciona-se o ritmo de crescimento da *Internet* nos últimos anos, em que os mercados se transformaram quase de imediato.

A *Internet*, o lançamentos de novos *softwares* e *hardwares* direcionados para a administração e logística das empresas, representam algo um tanto inovador nas últimas décadas. (MONTANA; CHARNOV, 2011)

Parte da evolução da tecnologia data por volta de 1957, quando surgem os satélites de comunicações artificiais postos em órbita e utilizados para fins científicos, militares e de comunicação. E a partir de 1983 são colocados vários satélites em órbita passando a evoluírem e serem utilizados para transmissão de conversação telefônica de longa distância e móvel, imagens de TV e de dados digitais, refletindo ou retransmitindo ondas de radiofrequência. (PINHO, 2000)

Com o tempo, os satélites começaram a ser usados para fins comerciais:

Os satélites comerciais oferecem uma ampla variedade de serviços de comunicação. Programas de televisão retransmitidos internacionalmente deram lugar ao chamado fenômeno da 'aldeia global'. Os satélites também retransmitem programas para os sistemas de TV a cabo bem como para as casas equipadas com antenas parabólicas. Com o crescente uso da transmissão digital, os satélites de comunicação propiciam *links* para o envio de dados e serviços de telefonia internacional mais eficientes e de menor custo. (PINHO, 2000, p. 20)

Os satélites de comunicação estimularam um desenvolvimento tecnológico das telecomunicações com uma infraestrutura que expandiu consideravelmente as condições de implantação de redes de comunicação de alcance regional, nacional e mundial, possibilitando a difusão de dados em tempo real.

Entretanto, as redes de computadores inicialmente surgiu na Guerra Fria, relacionadas a interesses políticos entre os governos como da antiga URSS, em 1957, mas, foi a partir de 1967 que a *Internet* começou a ser formada, com o *Transmission Control Protocol* (TCP) e o *Internet Protocol* (IP), oferecendo 4 bilhões de endereços diferentes e utilizando uma arquitetura de comunicação em camadas, com protocolos distintos e com funções específicas. (PINHO, 2000)



Ao TCP cabia dividir mensagens em pacotes de um lado e recompô-los do outro. Ao IP cabia descobrir o caminho adequado entre o remetente e o destinatário e enviar os pacotes. A ARPAnet adotou progressivamente o TCP/IP, que funcionou em paralelo com o UUCP, até o dia 1º de janeiro de 1983, quando cada máquina conectada com TCP/IP a ARPAnet teve que passar a usar o novo conjunto de protocolos. (PINHO, 2000, p. 26)

Saindo de suas origens militares, a ARPAnet se dividiu, em 1983, na Milnet, para fins militares, e na nova ARPAnet, com objetivos de pesquisa, que portanto começou definitivamente a denominada *Internet*. (PINHO, 2000)

A *Internet* se tornou mundial, e em 1990, passou a contar com o primeiro provedor de acesso comercial do mundo, possibilitando que os usuários comuns tivessem seu acesso através do telefone. Em 1991, a grande novidade da *Internet* se deu na invenção da *World Wide Web (www)*, criada pelo engenheiro Tim Berners-Lee no Laboratório Europeu de Física de Partículas (CERN). A *Web* se posicionou como uma das mais relevantes partes da *Internet* e, que atualmente cada vez mais tem dado “asas” ao comércio eletrônico (*e-commerce*), o qual tem sido praticado por empresas de médio e grande porte, como hipermercados, magazines, e até mesmo atraindo a atenção de pequenos empreendedores. (PINHO, 2000)

Entretanto, os resultados da implementação da TI são os Sistemas de Informação que ocorrem por meio do uso de computadores e telecomunicações. (BALARINE, 2002)

Os Sistemas de Informação são as práticas usadas pelas organizações para aprimorar o seu desempenho, o que também deve incluir um custo operacional adequado, processos logísticos inteligentes, e a integração com fornecedores e clientes. Salientando que, os Sistemas de Informação se mostram fundamentais ao apoio à realização dos negócios de toda organização. (MONTEIRO, 2009)

As empresas precisam dos Sistemas de Informação (SI) porque tem um elevado e crescente volume de informações. Se a empresa possui um bom sistema de

informação a exposição das informações necessárias propicia uma ótica das decisões e a empresa assegura um importante diferencial frente aos concorrentes, já que os gestores têm condições de tomar decisões de forma mais rápida e com o apoio de fontes seguras. (GARCIA, 2009)

Os Sistemas de Informação são de suma relevância em toda a cadeia de valor de uma empresa. Algumas ferramentas atualmente facilitam e fazem a informação mais acurada para certos fins, como na aplicação de cadeias de suprimentos, por exemplo, o código de barras, o *Eletronic Data Interchange (EDI)*, *Efficient Consumer Response (ECR)* e os *ERPs* que integram todos os outros. (MONTEIRO, 2009)

A Tecnologia da Informação, assim, se revela como uma excelente ferramenta de apoio aos processos de tomada de decisão, consideravelmente no atual mercado globalizado em que a cada dia se eleva o nível de competitividade entre as empresas. (CUNHA; NEVES, 2010)

Frente a esse contexto, se faz necessário maior atenção a tudo que a empresa tem a sua volta (ambiente interno e ambiente externo). Nesse sentido podem-se considerar as cinco forças competitivas de Porter, que juntas contribuem para que a organização se posicione com maior vantagem no seu mercado de atuação. As cinco forças de Porter são:

1. Ameaça de novos entrantes;
2. Intensidade de rivalidade entre os concorrentes existentes;
3. Pressão de produtos substitutos;
4. Poder de negociação dos compradores;
5. Poder de negociação dos fornecedores. (PORTER, 2004)

A Tecnologia da Informação contribui para a condição de sobrevivência da empresa em seu mercado, por meio de ferramentas de análise que repercutem na

liderança no custo total (usando Sistemas de Informação gerenciais (SIGs) minimizando os custos de produção e possibilitando que seja lançado no mercado um produto com preço mais competitivo); na diferenciação (a TI apóia o departamento de pesquisa e desenvolvimento na formulação de um novo produto ou serviço); e no enfoque (a TI, por meio de sistemas de *datamining* e sistemas como o *Customer Relationship Management (CRM)*, que pode captar importantes informações a respeito de um nicho específico de compradores ou linha de produtos e serviços que contribuam para se obter novos negócios). (CUNHA; NEVES, 2010)

Desse modo, resume-se que a TI possibilita mudanças substanciais na maneira de como é realizado o trabalho e na integração das funções do negócio, tanto nos níveis internos, quanto entre organizações, havendo também transformações no clima de competitividade e novas oportunidades estratégicas. (ALBERTIN, 2009)

Entretanto, nesse contexto, a segurança é um fator de suma relevância, pois, infelizmente, os riscos existem principalmente no que se refere ao mundo virtual e às informações, em que a todo instante aparecem novas vulnerabilidades e ameaças, levando em algumas situações a crimes digitais.

### **2.3.Mecanismos de controle de segurança em TI**

Atualmente existem vários mecanismos para controles de segurança, como os de autenticação e autorização, os destinados ao combate a invasores, detectores de intrusos, para privacidade das comunicações, para redes virtuais privadas, entre outros.

A autorização se refere ao processo de conceder ou negar direitos aos usuários ou sistemas através das denominadas listas de controle de acessos (*Acess Control Lists – ACL*), determinando as atividades que podem ser realizadas, o que gera os conhecidos “perfis de acesso”. (LAUREANO, 2005)

Os processos de autenticação se classificam em três métodos:

- **Identificação positiva (o que você sabe):** em que o requerente mostra conhecimento sobre uma informação usada no processo de autenticação, como uma senha;
- **Identificação proprietária (o que você tem):** quando o requerente apresente algo usado no processo de autenticação, por exemplo, um cartão magnético;
- **Identificação Biométrica (o que você é):** em que o requerente expõe uma característica própria, como uma impressão digital. (LAUREANO, 2005)

No combate a ataques e invasões, os mecanismos (como dispositivos de *software* e *hardware* de proteção) assumem importante papel na gestão de segurança, uma vez que, as conexões eletrônicas, bem como as tentativas de acesso indevido vêm aumentando consideravelmente. Nessa categoria, podem-se mencionar os dispositivos que realizam filtragem, registros de acessos lógicos, e os direcionados para a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

Um bom exemplo dessa proteção é o *Firewall*, um sistema ou grupo de sistemas que fortalecem a norma de segurança entre uma rede interna segura e uma não confiável, como a *Internet*. Os *Firewalls* podem ser classificados em Filtros de Pacote e Servidores *Proxy*. (LAUREANO, 2005)

Os Filtros de Pacotes se referem a um dos principais mecanismos que permite ou não a passagem de datagramas IP em uma rede. É possível, por exemplo, filtrar pacotes para brechar o acesso a um serviço de Telnet, um *chat* ou até um *site* da *Internet*. O modelo mais simples de *Firewall* é o *dual homed system*, isto é, um sistema que interliga duas redes distintas, que tem um servidor com duas placas de rede permitindo que os usuários se comuniquem entre si. Um modelo clássico é um *Firewall* entre uma *Intranet* e a *Internet* (Figura 2).

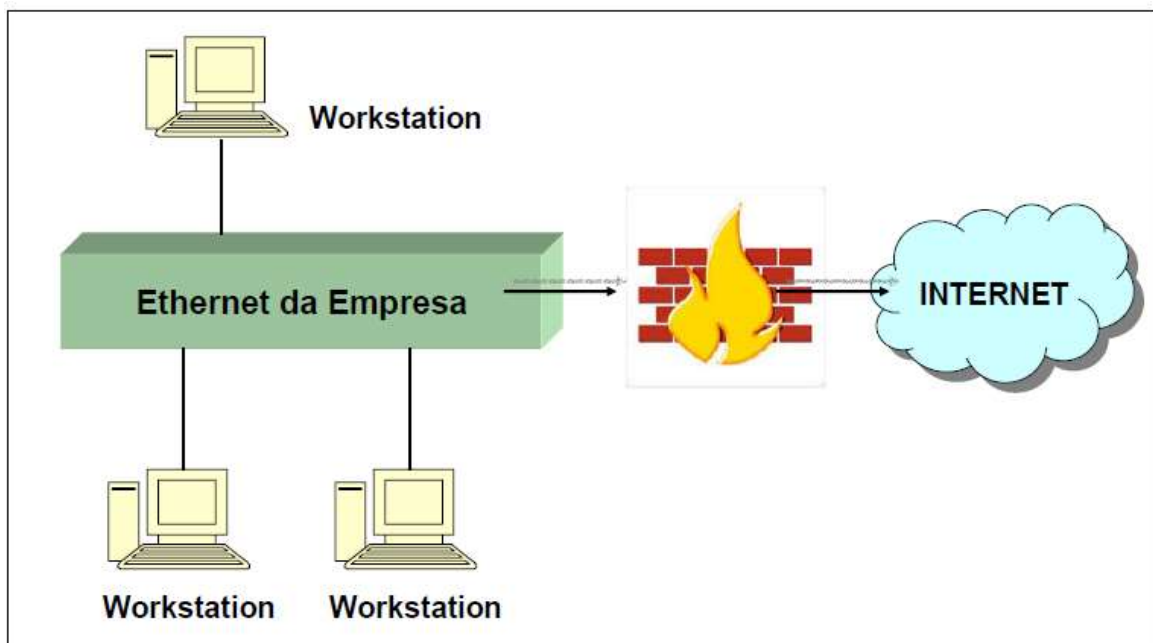


Figura 2 – Firewall Dual Homed Host

Fonte: Laureano (2005, p. 23)

Os Servidores *Proxy* possibilitam realizar a conexão ou não a serviços em uma rede modo indireto. Geralmente os *proxies* são usados como cachês de conexão para serviços *Web*. Um *Proxy* é usado várias vezes como um elemento de aceleração de conexão em *links* lentos (Figura 3).

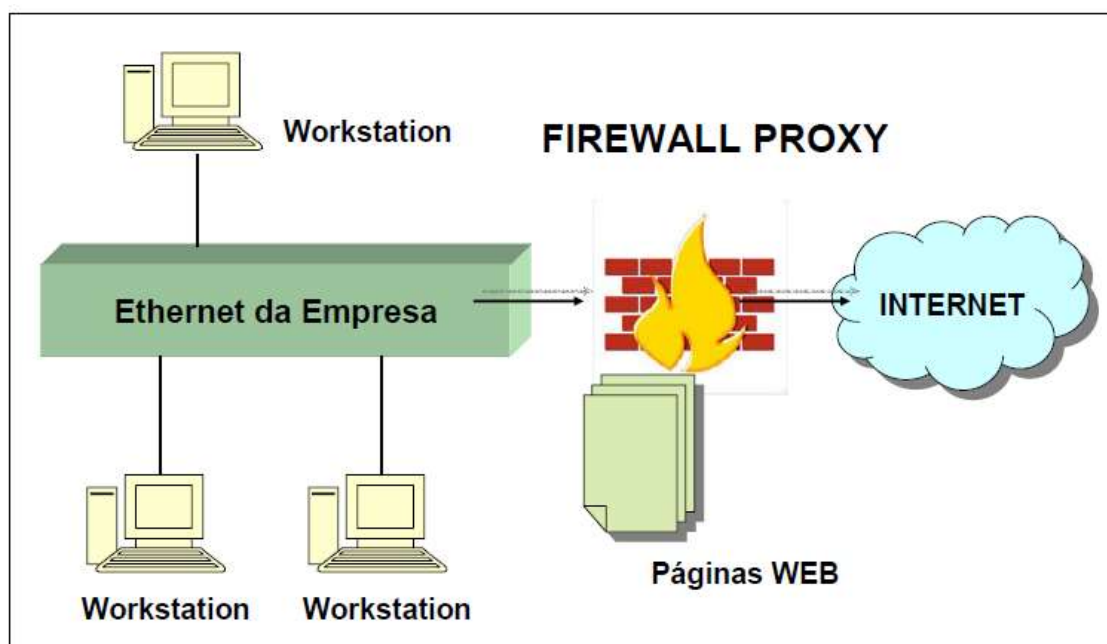


Figura 2 – Intranet

Fonte: Laureano (2005, p. 23)

No que se refere ao detector de intrusos, nos últimos tempos, essa tecnologia – *Intrusion Detection System (IDS)*, tem se apresentado como uma forte aliada dos administradores de segurança. Em uma visão básica, esses sistemas tentam reconhecer um comportamento ou ação intrusiva por meio de análise de informações disponíveis em um sistema de computação ou rede e alerta a ameaça para que se disparem contramedidas.

Para que a detecção ocorra, têm-se diversas tecnologias que vem sendo aplicadas em produtos comerciais ou em projetos de pesquisa, essas tecnologias envolvem análise estatística, inteligência artificial, *datamining*, redes neurais, etc. (LAUREANO, 2005)

O IDS tem por objetivo detectar se algum usuário está querendo invadir o sistema. Esse mecanismo é executado de forma constante em *background* e apresenta uma notificação apenas quando se detecta algo. Os sistemas em uso se classificam de acordo com a sua forma de monitoração – origem dos dados e aos mecanismos – algoritmos de detecção usados.

O Quadro 3 resume o IDS – quanto a origem dos dados e à forma de detecção:

<p><b><u>Quanto à Origem dos Dados</u></b></p> <p>Existem basicamente dois tipos de implementação de ferramentas IDS:</p> <ul style="list-style-type: none"><li>• <b>Host Based IDS</b> (HIDS) – são instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor;</li><li>• <b>Network Based IDS</b> (NIDS) – são instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes de rede e seus detalhes como informações de cabeçalhos e protocolos.</li></ul> <p><b><u>Quanto à Forma de Detecção</u></b></p> <p>As técnicas usadas para detectar intrusões podem ser classificadas em:</p> <ul style="list-style-type: none"><li>• <b>Detecção por assinatura</b> – os dados coletados são comparados com uma base de registros de ataques conhecidos (assinaturas). Por exemplo, o sistema pode vasculhar os pacotes de rede procurando sequências de bytes que caracterizem um ataque de <i>buffer overflow</i> contra o servidor WWW Apache;</li><li>• <b>Detecção por anomalia</b> – os dados coletados são comparados com registros históricos da atividade considerada normal do sistema. Desvios da normalidade são sinalizados como ameaças.</li><li>• <b>Detecção Híbrida</b> – o mecanismo de análise combina as duas abordagens anteriores, buscando detectar ataques conhecidos e comportamentos anormais.</li></ul>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Quadro 1 - IDS – quanto a origem dos dados e à forma de detecção

Fonte: Laureano (2005)

Em relação às Criptografias, a origem da palavra é grega, em que *kriptos* se refere a escondido, oculto e *grifo*, à escrita, que vem a definir assim, a ciência em escrever através de cifras ou de códigos, usando um conjunto de técnicas que faz com a mensagem fique incompreensível, denominando-se assim, “texto cifrado”, possibilitando que somente o destinatário desejado possa decodificar e entender a mensagem claramente. Assim:

A Criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. (...) sem dúvida é a maneira mais segura de se enviar informações através de um canal de comunicação inseguro como, por exemplo, a *Internet*. (LAUREANO, 2005, p. 26)

Cabe ressaltar que hoje, alguns dos mecanismos de busca da *Internet*, por exemplo, apresentam ao usuário uma política de privacidade e garantem que há segurança de suas informações, como o mecanismo de busca mais conhecido – *Google*.

Primeiramente, tal política do *Google* afirma recolher todas as informações básicas do usuário, com a justificativa de prestar melhores serviços aos usuários e do mesmo ter uma experiência diversa ao se utilizar os serviços, uma vez que através das informações pessoais formam um perfil da pessoa e direcionam anúncios de acordo com isso. (POLÍTICA DE PRIVACIDADE GOOGLE, 2015)

Para a coleta de tais informações, o *Google* utiliza duas formas: as informações fornecidas pelo próprio usuário e as informações que são recebidas através do uso dos serviços.

As informações pessoais fornecidas conscientemente consistem no nome, endereço de *e-mail*, número de telefone ou cartão de crédito, criar um Perfil do *Google* publicamente visível, que pode incluir foto. Já as informações que são capturadas através do uso dos serviços do *Google*, incluem também como são utilizados, ou seja, ao visitar um *site* que utiliza os serviços de publicidade do *Google* ou quando visualiza e interage com os anúncios e conteúdo. Incluindo ainda nesta segunda categoria, o *Google* angaria as informações do dispositivo, ou seja, informações específicas do dispositivo (como o modelo de *hardware*, versão do sistema operacional, identificadores de dispositivos exclusivos e informações de rede móvel, incluindo número de telefone). (POLÍTICA DE PRIVACIDADE GOOGLE, 2015)

O *Google* afirma que não compartilha informações pessoais com empresas, organizações e indivíduos externos a *Google*, a não ser que se tenha a autorização do usuário, com administradores de domínios, como dos usuários do *Google Apps* e



revendedores que dão suporte ao usuário e a sua organização, para processamento externo, quando fornecem informações pessoais às suas afiliadas ou empresas confiáveis para processá-las e, por motivos legais. (POLÍTICA DE PRIVACIDADE GOOGLE, 2015)

Em relação à segurança das informações, o *Google* afirma que não medem esforços para protegê-las, em que atuam da seguinte forma:

- Criptografam grande parte de seus serviços utilizando SSL;
- Oferecem verificação em duas etapas quando se acessa a Conta do *Google* e um Recurso de Navegação Segura no *Google Chrome*;
- Analisam a coleta, prática e processamento de informações, para proteger-se contra acessos não autorizados aos sistemas;
- Restringem o acesso a informações pessoais por parte de empregados, contratados e representantes da *Google* que precisam de tais informações são sujeitos a rigorosas obrigações contratuais de confidencialidade. (POLÍTICA DE PRIVACIDADE GOOGLE, 2015)

Em suma, ainda outros mecanismos podem ser usados para a segurança da informação tanto para pessoas físicas, quanto jurídicas, como a Assinatura Digital, entre outros, que no caso de uma organização deverá avaliar qual é o melhor para suas necessidades em seu cotidiano e segundo valor de suas informações.

A seguir, para complementar este estudo será apresentada a metodologia desta pesquisa que abrange a um estudo de caso de uma empresa que atua no segmento de reciclagem sobre o seu sistema de segurança.

### **3. METODOLOGIA**

O presente trabalho é constituído pesquisa de natureza aplicada. Como explica Severino (2000), essa característica visa acentuar maiores conhecimentos em busca de respostas para um problema específico.

A abordagem do problema desse estudo é qualitativa, ou seja, não abrangerá o uso de instrumentos estatísticos.

Esta pesquisa tem objetivos exploratórios. Segundo Gil (2008), esse tipo de pesquisa tem o intuito de estudar os pontos mais relevantes do assunto abordado.

Em relação aos procedimentos para o desenvolvimento desse estudo, abrangeu a pesquisa bibliográfica, documental e de estudo de caso, cuja população/amostra contém um quadro total de 32 funcionários, e que se refere a uma empresa de pequeno porte que atua como reciclagem situada na cidade de Jundiaí-SP.

O estudo foi realizado através da observação direta e individual, em que se fizeram cinco visitas à empresa, nos horários distribuídos entre 13:00hs às 15:00hs e 14:00hs às 16:00hs, nos meses de agosto e setembro antecipadamente agendadas com o responsável da empresa, nas quais foram anotados os principais aspectos do seu sistema de segurança em TI, as ferramentas que atualmente utiliza e diante dessas observações, se analisando a possibilidade de ao final desse estudo realizar algumas sugestões de melhorias à mesma.

#### **4.A EMPRESA E O SISTEMA DE SEGURANÇA (TI)**

##### ***4.1.Radiografia Geral da Empresa***

A empresa, objeto desse estudo será tratada aqui pelo nome ECF Reciclagem, fundada em 1994, deu início às suas atividades com a transformação de garrafas PET em fibras de poliéster.

Segundo documentos da empresa, ela é uma das pioneiras na reciclagem de PET, que a cada ano vem aumentando sua capacidade de transformação de garrafas recicladas.

A empresa tem como Missão, Visão e Valores:

- **Missão:** “Produzir e comercializar fibras sintéticas atendendo às necessidades de nossos clientes, colaboradores, acionistas, fornecedores e da comunidade.”
- **Valores:** “Ser reconhecida no mercado pela qualidade de nossos produtos, sendo referência na reciclagem de embalagens PET.”
- **Valores:**
  - Foco no mercado e nos clientes;
  - Busca constante da excelência operacional;
  - Responsabilidade com a comunidade e o meio ambiente.

Os produtos que a empresa trabalha se referem à transformação das garrafas PET em fibras de Poliéster que se distribuem em:

- Fibras de Poliéster para enchimentos;
- Fibras de Poliéster para não tecidos;
- Fibras de Poliéster para fiações;
- Fibras para concreto e argamassa;
- Fibras de polipropileno;
- Fibras Bi-Componentes.

O processo de fabricação se inicia com o recebimento das garrafas PET e a separação dos produtos contaminantes. Um equipamento separa os rótulos, tampas e demais objetos, os funcionários se certificam de que não passem produtos impróprios pelas esteiras, posteriormente as garrafas são moídas.

Em continuidade, as garrafas seguem para o processo de lavagem, cuja cola dos rótulos e demais impurezas são retiradas. No final da produção se tem a extrusão, quando o plástico recebe um pigmento correto e se transforma em fibra de poliéster, para posteriormente ser cortado em vários comprimentos segundo a necessidade do cliente.

Atualmente em torno de 40% da fibra produzida pela empresa é voltada para atender ao setor automobilístico. A outra parte é voltada para enchimentos de almofadas, travesseiros, pelúcias, máscaras cirúrgicas, forração de calçados, etc.

A Figura 3 ilustra a empresa:



Figura 3 – Empresa ECF Reciclagem  
Fonte: Google Imagens (2015)

Para suprir sua demanda, a ECF Reciclagem vem buscando cooperativas que fazem as coletas de garrafas PET, pois, Jundiaí e região têm uma coleta reduzida. A empresa conta atualmente com mais de 500 fornecedores e com uma estrutura em termos de equipamentos que está em atualização, ou seja, a empresa vem fazendo a compra e a troca por novos equipamentos com melhor tecnologia.

#### **4.2.Sistema de Segurança (TI) da Empresa**

Conforme se observou nas visitas à empresa ECF Reciclagem, que por ainda ser uma empresa de menor porte, não investiu em um sistema de segurança próprio.

Porém, os dados são centralizados, e apenas duas pessoas os gerenciam. Contam com um ambiente de servidores virtuais e poucos físicos.

Seus meios de segurança das informações se dão através:

- *SonicWall* da Dell, que é responsável pelo controle do tráfego, assim como, conexões de fora;
- Antivírus Symantec;
- *Backup* diário, semanal e mensal com *Arcserve Backup*;
- *Nobreak Eaton* com interface *Web* para queda de energia na sala dos servidores;
- Segurança (física) em que se tem a Autenticação de Impressão Digital na sala em que ficam os funcionários que gerenciam os sistemas e na dos servidores.

Até o momento a empresa afirma que não sofreu com invasões ou perdas de informações, mas, como está em crescimento, essa preocupação vem se acentuando.

#### **5.Sugestões de Melhorias a Empresa e Modelos de Laureano**

A segurança da informação, por sua vez, vem se apresentado como um assunto cada vez mais relevante que tem se intensificado em escopo e complexidade, pois, é um campo que lida constantemente com o tratamento de riscos, e de como podem ser evitados.

Como apontou a literatura específica, a segurança da informação é de grande importância em um mundo globalizado que tudo gira em torno da informação. Assim,

na era digital, a proteção é o mínimo que se pode ter para não cair em armadilhas, como da *Internet*. (LISBOA, 2011)

Com o advento da tecnologia da informação as mudanças têm ocorrido profundamente na maneira de como as empresas desenvolvem seus negócios, em que vem acentuando um aumento na produtividade. Assim, a TI, passa a ser um dos principais elementos que possibilita às empresas a se diferenciarem em relação à concorrência, e a garantir maior vantagem competitiva. Porém, nesse contexto, cabe a atenção à segurança. (CUNHA; NEVES, 2010)

Sob essa perspectiva, sugere-se que a empresa ECF Reciclagem que vem demonstrando um crescimento considerável em sua produtividade, construa um Plano de Tecnologia para aumentar a segurança de suas informações.

Abaixo destacamos alguns modelos propostos por Laureano (2005), os quais podem ser seguidos pela empresa ECF Reciclagem:

O modelo de segurança (Figura 4) apresenta os serviços preliminares e os fatores utilizados para suportar e executar a segurança da tecnologia de informação. Este modelo classifica os serviços segundo sua finalidade preliminar:

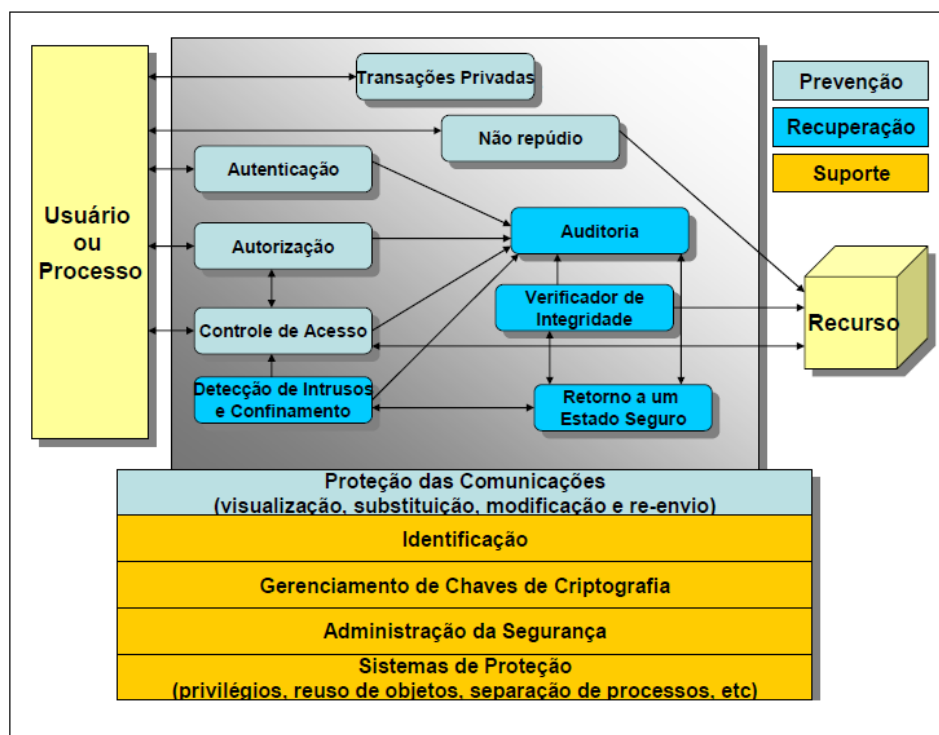


Figura 4 – Modelo para Implantação da Segurança  
Fonte: Adaptado de Laureano (2005)



Os serviços se classificam em suporte, prevenção e detecção e recuperação.

A implementação da disponibilidade e da integridade são tidas por meio do controle e identificação dos indivíduos e alterações não autorizadas, bem como a capacidade do sistema ser recuperado (Figura 5). (LAUREANO, 2005)

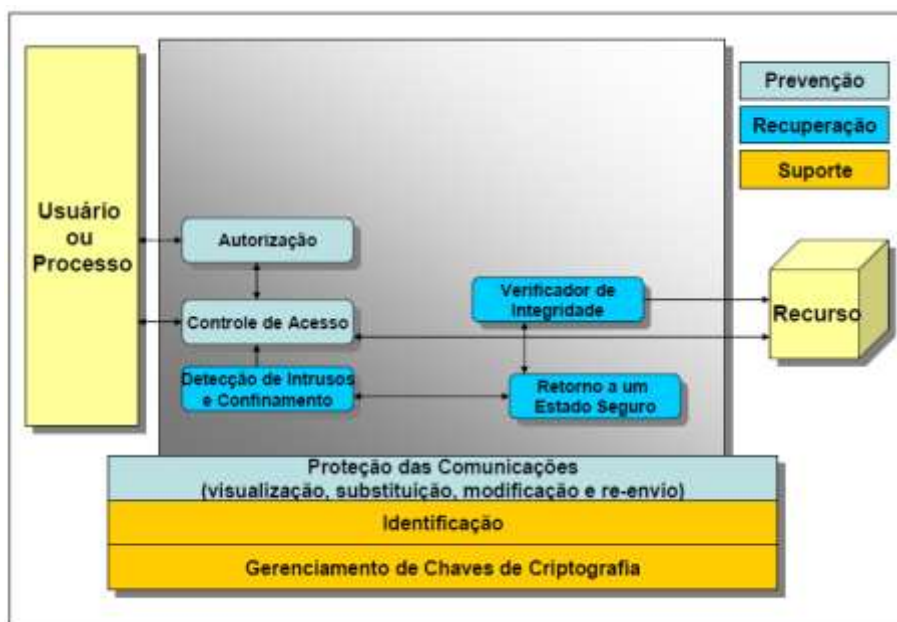


Figura 5 - Modelo conforme Princípios da Segurança  
Fonte: Adaptado de Laureano (2005)

A confidencialidade é tida por meio da proteção das comunicações, do controle de acessos e da utilização eficiente dos mecanismos de privacidade. Também cabe a realização de auditorias do sistema, a fim de manter a rastreabilidade das ações e o não-repúdio das ações realizadas no sistema.

Por fim, se tem a garantia – a qualidade da segurança de um sistema de informação (Figura 6):

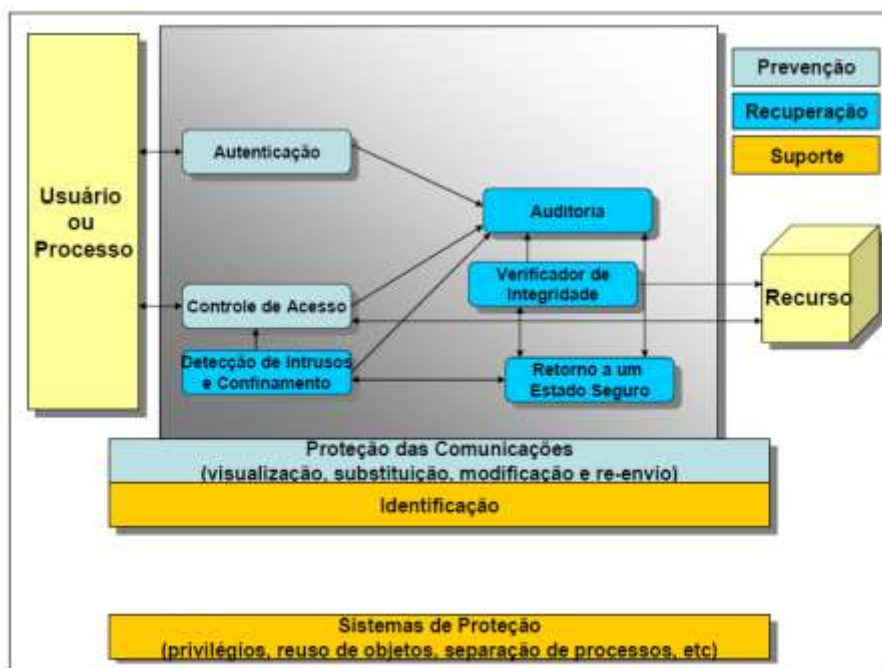


Figura 6 – Garantia de segurança em um sistema de informação  
Fonte: Adaptado de Laureano (2005)

Além dos modelos aqui citados, incluo aqui um modelo originalmente estudado, analisado e sugerido sem referências externas, imaginando um ambiente em risco, o que poderia ser feito/aplicado naquele momento.

Desta vez não existem figuras a serem apresentadas, mas sim uma série de sugestões para que as consequências em questão não afetem o desempenho, ou mesmo a rotina da empresa de modo a prejudicar seus lucros.

Seguimos com estas questões abaixo:

- Confirmar fonte da aquisição do problema;
- Consultar “lições aprendidas” para melhor tratar tal questão;
- Checar

Em suma, pode-se afirmar que a garantia de segurança de um sistema de informação ocorrerá se alguns serviços (como citados na figura) forem implementados, já que a garantia depende da maneira e dos objetivos do sistema.

Desse modo, a empresa em questão deverá analisar e planejar seu Plano de Tecnologia, segundo suas necessidades, para que não se tenha um investimento em programas, dispositivos e demais elementos, além do que é preciso para atender seu cotidiano e manter a integridade de suas informações.

Nos próximos tópicos, saindo um pouco de modelos teóricos, fora incluído uma análise mais prática das sugestões, também seguindo padrões para a segurança da empresa, abaixo serão listados com detalhes cada passo efetuado para garantir um melhor aproveitamento dos recursos adquiridos, e das normas que a empresa segue atualmente.

## **6. SEGURANÇA DA INFORMAÇÃO – APLICAÇÃO PRÁTICA**

### ***6.1 Iniciando o Plano Sugerido***

Com a ideia pré-estabelecida sobre o que seria de fato uma melhoria à empresa, decidiu-se aplicar na prática como um projeto focando e englobando sua segurança.

O projeto portanto, foi motivado pelo ramo de negócio do qual a empresa faz parte e também pelos processos que envolvem toda cadeia de clientes e fornecedores, ficando o departamento de TI responsável por desenvolver e apresentar o escopo do projeto para direção da empresa.

### **6.1.1 *Análise do Ambiente***

Em cada visita realizada pudemos constatar o quanto é diferente a percepção de segurança entre as empresas. Em algumas empresas o acesso à internet é totalmente liberado e não monitorado, em outros é totalmente liberado e monitorado e em alguns casos o acesso é liberado dependendo da autorização do funcionário e, mesmo assim, monitorado.

Chegamos à conclusão que o melhor método para a empresa ECF é de liberar o acesso dependente de autorização e monitoração, esta prática foi adotada pois permite aos responsáveis dos setores acompanhar quais recursos são necessários aos seus funcionários e também possibilita a geração de relatórios que podem servir como base de avaliação das atividades diárias de cada colaborador.

Os relatórios de monitoração permitem a visualização de informações como tempo de acesso, quantidade de downloads por funcionário, entre outras informações.

### **6.1.2 *Desenvolvimento e Treinamento da Política da Segurança da Informação***

Temos nas seções a seguir o conjunto de diretrizes e regras que compõem a política da informação da empresa estudada e elas têm como intuito apresentar os procedimentos para normatizar, melhorar e disciplinar o uso dos recursos da rede.

O documento da política foi originado após intensas discussões entre o departamento de TI e os demais departamentos da empresa. A política apresentada a seguir deve passar por uma reformulação, para adequar por exemplo os tipos de controles existentes aos requisitos da política.

## ITEM 1: AUTONOMIA DO DEPARTAMENTO DE TI

O departamento de TI possui total autonomia para atuar sobre os equipamentos da empresa, sem prévio aviso, no que se refere aos seguintes tópicos:

- Realização de auditoria local ou remota;
- Definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como prejudiciais ao hardware e software ou à rede como um todo;
- A instalação e configuração de softwares de monitoramento;
- A desinstalação de quaisquer softwares considerados prejudiciais à rede;
- O credenciamento e descredenciamento de usuários;

## ITEM 2: DIRETRIZES QUANTO À UTILIZAÇÃO DA INTERNET

- A internet deve ser utilizada para fins corporativos, o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações que venham contribuir para o desenvolvimento de seus trabalhos.
- O uso para fins pessoais, mediante o consentimento do responsável pelo setor, fica restrito à consulta de movimento bancário e ao acesso ao e-mail pessoal, estando vedadas práticas abusivas tais como a circulação de correntes, material fonográfico entre outros.

## ITEM 3: E-MAIL CORPORATIVO

- Desconfiar de todos os e-mails com assuntos estranhos ao ambiente de trabalho.

- Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.
- Evitar enviar anexos acima de 10 Mbytes.

#### ITEM 4: A REALIZAÇÃO DE DOWNLOAD

- A realização de downloads exige banda de navegação do servidor e , se realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários mais demorada.
- A realização de downloads deve ser vista com muito cuidado e feita somente em casos de extrema necessidade. Além disso, estará limitada a arquivos de no máximo 1 Mbyte, pois downloads de arquivos de tamanho superior podem congestionar o fluxo de tráfego e comprometer os sistemas que funcionam on-line.

#### ITEM 5: SENHAS DE ACESSO

- Cada setor deverá, através de comunicado oficial, indicar novos colaboradores e o perfil que devem possuir na rede e nos sistemas da empresa.
- A senha de acesso é pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.
- O compartilhamento de senhas de acesso é absolutamente proibido e o titular que divulgar sua senha a outrem responderá pelas infrações por esse cometidas, estando passível de advertência. Caso o usuário desconfie que sua senha não seja mais segura, poderá solicitar ao departamento de TI a alteração desta.

- As senhas têm validade de 30 dias.

#### ITEM 6: SOFTWARES DE CONVERSÇÃO INSTANTNEA

- É permanentemente proibido aos setores o uso de softwares de conversção instantnea, ou de qualquer mecanismo que venha promover serviço semelhante, existentes ou que venham a existir.
  - Pode haver permissão especial a qualquer setor para utilização de Instant Messengers, desde que seja para fins corporativos e comprovadamente utilizados em assuntos comerciais e/ou para suporte.

#### ITEM 8: A INSTALAÇÃO DE SOFTWARES

- Qualquer software que, por necessidade do serviço, necessitar ser instalado, deverá ser comunicado ao departamento de TI, que procederá a instalação caso constate a necessidade do mesmo. Fica proibida a instalação de qualquer software sem licença de uso.
- O departamento de TI poderá utilizar de sua autonomia citada no Item 2 deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à lei do software (Lei 9.609/98).

#### ITEM 9: PENALIDADES

- O usuário que infringir qualquer uma das diretrizes de segurança expostas este instrumento estará passível das seguintes penalidades (sem prévio aviso):
- Perda da senha de acesso aos sistemas e Internet;

- Cancelamento da caixa de e-mail;
- Advertência formal por intermédio do departamento de RH podendo levar inclusive a demissão do colaborador.

#### ITEM 10: EQUIPE DE SEGURANÇA DA INFORMAÇÃO

- Os servidores relacionados a seguir são diretamente responsáveis pela implantação presente política:
- Gestor de TI;
- Analista de Sistemas;
- Analista de Suporte.

#### ITEM 11: DIVULGAÇÃO E TREINAMENTO

- A política deve ser divulgada por intermédio de treinamento aos colaboradores, clientes e fornecedores, podendo ainda ser divulgada por e-mail, mural ou jornal interno.

#### ITEM 12: VIGÊNCIA E VALIDADE

- A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado podendo ser alterada conforme necessidades previamente detectadas.



### **6.1.3 Inventário de Hardware e Software**

Devemos inventariar todo hardware e software presente na empresa, pois assim podemos ter um panorama das licenças existentes e das características e condições dos equipamentos.

É uma tarefa necessária, porém muitas empresas não dão o devido valor a este quesito. Primeiramente foram realizadas anotações manuais, entretanto após algum estudo, decidiu-se por adotar um software THE DUDE (DUDE, 2007) por ser gratuito e que permitiu o inventário em tempo real e on-line de todos os equipamentos e softwares da rede da empresa.

### **6.1.4 Resultados Obtidos Pós-Análise e Pós-Melhorias**

Após a aplicação de tais conceitos, direitos, deveres e normas de melhores práticas, podemos discutir as melhorias pós tempo de aplicação da Política de Segurança.

Neste projeto buscou-se desenvolver um método que permita as empresas implantarem um sistema para a segurança da informação de modo customizado, de acordo com suas necessidades e percepções. Com a implantação do método conseguimos uma redução no número de ocorrências de ataques, melhor controle de licenças de softwares, também conseguimos racionalizar a utilização dos equipamentos e recursos de rede e maior comprometimento dos colaboradores.

Este trabalho não pretende ser uma solução definitiva para os problemas de segurança da informação, pois se entende que a segurança é realmente algo dinâmico, em vista das novas ameaças que surgem diariamente. Por conta disso, os gestores de TI devem se manter constantemente atualizados com a literatura da área.

A segurança então, se torna um processo que precisa de monitoramento e manutenção.

## **7.CONCLUSÕES**

Há algumas décadas, o investimento em Tecnologia de Informação, e ainda mais, na sua segurança, era visto por muitos como um sinônimo de elevação dos custos ou das despesas. Atualmente muito disso se modificou, e a TI exerce um papel estratégico, em que contribui para o aumento da produtividade e, também, para a redução dos custos operacionais.

Porém, como se pode notar, com o crescimento elevado de usuários acessando à *Internet*, como no Brasil, fica explícito o aumento também de diversos casos de crimes virtuais e das vulnerabilidades frente ao excesso de informações e dos descuidos dos usuários.

Portanto, a segurança da informação, principalmente para as empresas deve ser considerada como um “artigo de primeira necessidade”, sendo essencial investir nesse quesito e buscar constantemente a prevenção das ameaças e armadilhas que o mundo virtual comporta. Essa proteção pode ser conquistada de algumas formas, como realização previamente um Plano de Tecnologia, e contando com sistemas de informação com dispositivos – *softwares*, por exemplo, que ajude a amenizar tais riscos.

Esse trabalho tomou para estudo uma empresa de reciclagem de pequeno porte, cuja pesquisa, proporcionou condições de realizar sugestões de melhoria à mesma, como indicando a necessidade de elaborar um Plano de Tecnologia, e, ajudou a responder afirmativamente a problemática dessa pesquisa, ou seja, a segurança em tecnologia da informação pode proporcionar benefícios também para as organizações

de pequeno porte, sendo considerada um fator de sucesso crítico e de fundamental importância do ponto de vista estratégico e empresarial.

A segurança da informação, quando acentuada na organização, representa valor, isto é, valor da informação adequada que chega de forma precisa e única a gestores, superiores, e que se torna relevante aos processos de decisão da organização, lembrando que, a qualidade e veracidade da informação hoje pode ser considerada um fator de grande importância, e que contribui para a capacidade competitiva da empresa.

Assim, este trabalho, alcançou ao seu objetivo geral que foi estudar os principais benefícios que a segurança em tecnologia da informação pode oferecer às organizações, sob o ponto de vista estratégico e empresarial. Dentre os benefícios, pode-se mencionar que dependendo da forma de implantação e gerenciamento da TI, ocorre melhor definição dos serviços, há um gerenciamento mais adequado da qualidade dos serviços de TI, é possível criar um padrão de comunicação e de escala entre os usuários, os procedimentos de TI são padronizados, divulgados e integrados e as medições de desempenho auditáveis podem ser definidas e acompanhadas, dentre outros benefícios, que também dão suporte às tomadas de decisão da alta administração e de outros departamentos.

O estudo apresentado além de tudo colaborou para um processo de implantação (dificuldades, treinamentos, aceitabilidade dos funcionários, etc.) de um Plano de Tecnologia e Segurança, em uma empresa de pequeno porte.

## 8.REFERÊNCIAS BIBLIOGRÁFICAS

- ALBERTIN, Alberto Luiz. *Administração de Informática: Funções e Fatores Críticos de Sucesso*. 6. ed. São Paulo: Atlas, 2009.
- BALARINE, Oscar Fernando Osorio. Tecnologia da Informação como vantagem competitiva. São Paulo: *Fundação Getúlio Vargas, Revista Eletrônica*, v.1, n.1. jan-jun, 2002. Disponível em: <http://www.rae.com.br/artigos/1059.pdf>, recuperado em 10/08/2015.
- CAPEZ, Fernando. *Curso de Direito Penal*. 13. ed. v. 1. São Paulo: Saraiva, 2009.
- CHIAVENATO Idalberto. *Gerenciando com as Pessoas: Transformando o executivo em um excelente gestor de pessoas*. Rio de Janeiro: Elsevier-Campus, 2005.
- CUNHA, David; NEVES, R. Oliveira. *Tecnologia da Informação como vantagem competitiva*. 2010. Disponível em: [http://www.dido.eti.br/documentos/artigo\\_tecnologia\\_da\\_informacao\\_como\\_vantagem\\_competitiva.pdf](http://www.dido.eti.br/documentos/artigo_tecnologia_da_informacao_como_vantagem_competitiva.pdf), recuperado em 15/06/2015.
- DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação*. Rio de Janeiro: Axcel Books, 2000.
- FONTES, Edison. *Políticas e normas para segurança da informação*. Rio de Janeiro: Brasport, 2012.
- GARCIA, Elias. *A importância do sistema de informação gerencial para tomada de decisões*. 2009. Disponível em: <http://www.unioeste.br/campi/cascavel/ccsa/VISeminarrio/Artigos%20apresentados%20em%20Comunica%E7%F5es/ART%203%20-%20A%20import%E2ncia%20do%20sistema%20de%20informa%E7%E3o%20gerencial%20para%20tomada%20de%20decis%F5es.pdf>, recuperado em 10/08/2015.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. São Paulo: Atlas, 2008.

GOOGLE. *Política de Privacidade*. 2015. Disponível em:

<http://www.Google.com.br/intl/pt-BR/policies/privacy/> recuperado em 19/08/2015.

JESUS, Damásio de. *Direito Penal*. 29. ed. v.1. São Paulo: Saraiva, 2008.

LAUREANO, Marcos A. Pchek. *Gestão de Segurança da Informação*. 2005. Disponível

em: [http://www.mlaureano.org/aulas\\_material/gst/apostila\\_versao\\_20.pdf](http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf)

recuperado em 19/10/2015.

LEHMKUHL, Giuvania Terezinha; VEIGA, Carla Rosana, RADO. O papel da tecnologia da informação como auxílio à engenharia e gestão do conhecimento. *Revista Brasileira de Biblioteconomia e Documentação*, São Paulo, v.4, n.1, p.59-67, jan./jun. 2008.

LISBOA, Gilvânia dos Santos. *Segurança de sistemas de informação: o contexto da segurança dos sistemas de informação*. 2011. Disponível em:

<http://www.atenas.edu.br/faculdade/arquivos/NucleoIniciacaoCiencia/REVISTAS/REVIST2011/6.pdf>, recuperado em 12/07/2015.

MONTANA, Patrick J.; CHARNOV, Bruce H. *Administração*. São Paulo: Saraiva, 2011.

MONTEIRO, Aluisio. *Vantagem Competitiva em Logística Empresarial Baseada em Tecnologia de Informação*. 2009. Disponível em:

<http://www.ead.fea.usp.br/Semead/6semead/PGT/018PGT%20-%20Vantagem%20Competitiva%20em%20Log%EDstica.doc>., recuperado em 06/07/2015.

NAZÁRIO, Paulo. *A importância de sistemas de informação para a competitividade logística*. 2013. Disponível em:

<http://www.faad.icsa.ufpa.br/admead/documentos/submetidos/A%20Importancia%20SI%20Logistica.pdf>, recuperado em 22/09/2015.

- PINHO, José B. *Publicidade e vendas na internet: Técnicas e estratégias*. São Paulo, SP: Summus, 2000.
- PORTER, Michael E. *Estratégia Competitiva: Técnicas para análise de indústrias e da concorrência*. Rio de Janeiro: Elsevier Editora, 2004.
- SANTOS, Antonio R. dos et al. *Gestão do Conhecimento como Modelo Empresarial*. Disponível em: [http://www1.serpro.gov.br/publicacoes/gco\\_site/m\\_capitulo01.htm](http://www1.serpro.gov.br/publicacoes/gco_site/m_capitulo01.htm), recuperado em 12/10/2015.
- STRAUBHAAR, Joseph; LAROSE, Robert. *Comunicação, Mídia e Tecnologia*. São Paulo: Pioneira Thomson Learning, 2004.
- SEVERINO, Antonio. J. *Metodologia do trabalho científico*. 21. ed. São Paulo: Cortez, 2000.
- TEIXEIRA, Tarcisio. *Direito eletrônico*. São Paulo: Editora Juarez de Oliveira, 2007.