ISSN: 1696-8352 - BRASIL – MARZO 2017

ESTUDO SOBRE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO

LEARDINI, Rafael Tafarello.

SCHIMIGUEL, Juliano.

Para citar este artículo puede utilizar el siguiente formato:

LEARDINI, Rafael Tafarello y SCHIMIGUEL, Juliano (2017): “Estudo sobre segurança da informação no ambiente corporativo”, Revista Observatorio de la Economía Latinoamericana, Brasil, (marzo 2017). En línea: http://www.eumed.net/cursecon/ecolat/br/17/antivirus.html

RESUMO

Em função do avanço tecnológico as organizações investem cada vez mais em novas ferramentas para garantir a segurança da informação. Estas ações são necessárias devido a confidencialidade, disponibilidade e integridade - pilares da segurança da informação, para a prevenção e proteção ao sistema de acordo com a política estabelecida no âmbito organizacional, visando à segurança do seu patrimônio. O estudo se apoiou nesses pilares para minimizar riscos, ataques e ameaças, que também podem ocasionar a perda de informações. Para melhor clareza frente a este estudo foram destacadas algumas ferramentas tais como Active Directory, Proxy Squid, antivírus e o recurso do firewall.

Palavras Chaves: Sistemas de Segurança, Firewall, Autenticação de Rede, Antivírus.

*Analista de Suporte, Lan Solver. Rua Jussara, 510, Jardim Santa Cecília, Barueri – SP. rafael.tafarello@lansolver.com.

** Doutor e Mestre em Ciência da Computação pelo Instituto de Computação da Unicamp. Professor dos Cursos de Sistemas de Informação, Analise de Sistemas e Engenharia de Produção no Centro Universitário Padre Anchieta. Campus Prof. Pedro. C. Fornari. jschimiguel@anchieta.br

ABSTRACT

Due to technological advances, organizations are investing in new tools to ensure information security. These actions are necessary to confidentiality, availability and integrity - pillars of information security, for the prevention and protection of the system according to the policy established in the organizational scope. The study is based on these pillars to minimize risks, attacks and threats, which can cause loss of information. For better understanding, this study will highlight some tools such as Active Directory, Squid Proxy, antivirus and the firewall resources.

Key Words: Security Systems, Firewall, Network Authentication, Antivirus.

1. INTRODUÇÃO

A partir do avanço tecnológico nas organizações novas formas de trabalho foram introduzidas beneficiando assim diversas etapas do processo, porém estas trouxeram novas mudanças e comportamentos para empresa, favorecendo assim nas atividades, tanto para planejamento, processo e controles, principalmente com a introdução da internet o qual favoreceu principalmente a comunicação permitindo diversas melhorias entre consultas e busca no acesso de diversos ambientes virtuais em questões de minutos (MORAES, 2003).

No entanto, percebeu-se também um grande risco com relação à própria questão de Segurança da Informação fazendo com que as empresas implantassem procedimentos de trabalhos para adequação de seus sistemas, estabelecendo regras de conduta que resguardem assim seus direitos, além de uma mudança de cultura, em função dos riscos e consequências que estes acabam às vezes gerando para a empresa. Este fato ocorre até mesmo por conta da transmissão de dados e compartilhamento de informações que passam a ser sigilosas, podendo assim interferir também na própria questão de compliace que é um assunto bem discutido atualmente nas organizações (MORAES, 2003).

Bernstein (2000) explica que o conceito de segurança da informação é denominado como um conjunto de dados de valor que determina assim uma organização ou pessoa, sendo um recurso de extremo valor para sociedade atual. Com

a utilização dos sistemas informatizados e conectados através de redes, as empresas passaram a ficar sujeitas de ameaças de diversos fatores, pois o mesmo coloca em risco a integridade dos sistemas e compromete as organizações em função das trocas de informações confidenciais que acabam sendo essenciais para concorrentes.

Diante deste contexto a proposta deste estudo é avaliar por meio da pesquisa bibliográfica os termos e conceitos recentes que tratam sobre o tema, bem como de uma análise histórica sobre a questão da segurança da informação, métodos de trabalho, ferramentas e procedimentos de segurança, visando assim resguardar-se frente à integridade da empresa.

Além disso, tratam-se também das principais formas de prevenção realizada pelas empresas, o papel das pessoas e dos responsáveis, a necessidade do estabelecimento de uma política de segurança confiável para que a mesma se resguarde e atue desde a contratação de um simples funcionário, levando-se assim o entendimento e ao conhecimento de todos.

O próprio termo segurança é definido como uma forma de minimizar a vulnerabilidade dos bens (quaisquer coisas de valor) e seus recursos, pois a segurança da informação não é apenas uma atitude, mas sim um conjunto de ações que visa assim garantir a segurança da própria rede de uma organização (SOARES, 1995).

Neste sentido, observando as palavras de Soares (1995), este explica que as empresas para trabalhar com a segurança da informação devem primeiramente conscientizar seus colaboradores estabelecendo regras e deixando as de forma clara, pois a partir do momento que um computador está conectado em rede, o mesmo já apresenta um risco de segurança, além disso, é muito comum também às empresas disponibilizarem acesso às informações para usuários via remoto. Observa-se, porém que muitos atos ocorrem em função da falta de conhecimento e até mesmo por irresponsabilidade dos usuários, podendo assim colocar em riscos dados confidenciais.

Os sistemas de seguranças nas empresas podem variar de acordo com o segmento da mesma, como é o caso das instituições financeiras os quais precisam operar com sistemas eficientes e eficazes, de modo a garantir a segurança de seus clientes, já em uma organização de menor porte e com menor número de funcionários esta apresenta menor risco, porém recomenda-se o bom uso do sistema, pois prevenir é a melhor forma de utilizar-se dos recursos das empresas (ZWICK et. al. 2000).

É válido destacar que a área de Tecnologia da Informação deve atuar com ações de proteção do ambiente de trabalho, avaliando recursos, analisando ainda possíveis pontos de ataques, ou seja, evitar quaisquer tipos de riscos para as empresas, o que recomenda-se assim que realize adequações dos processos de trabalho, orientação dos colaboradores, melhorias e investimentos em novas tecnologias. Portanto, a proposta deste trabalho é apresentar os principais métodos utilizados com relação às medidas de segurança baseado na prevenção, o qual será utilizado uma empresa de médio porte, porém será utilizado um nome fantasia para demonstração dos resultados.

Neste sentido, Zwick et. al. (2000) explica que a partir do momento que um computador está conectado a rede ou internet, existem três riscos, dados, recursos e reputação, porém eles serão previamente trabalhados e discutidos ao longo deste projeto. Entre outras palavras é válido afirmar que a Segurança da Informação deve atuar na forma de prevenção contra possíveis hackers, cujo propósito é invadir o ambiente de trabalho sendo necessário assim estabelecer regras de segurança (BERNSTEIN, 2000).

1.1.QUESTÃO PROBLEMA

A segurança da informação não é algo novo, pelo contrário, é uma estratégia desenvolvida pela tecnologia da informação implantada nas empresas para preservar a integridade da mesma, oferecendo confidencialidade, disponibilidade e integridade (FONTES, 2006).

Recentemente segundo Grupo New Space, em uma entrevista publicada pela Risk Report (2016) esta afirma que os principais riscos de segurança no ambiente de trabalho para organizações esta no recebimento e envio de mensagens por e-mail e até mesmo na execução de download. Esta questão trouxe grandes consequências para muitas empresas, o qual trabalha com inteligência cibernética, prevenção a fraudes e análise de riscos, que envolve a questão de fidelidade das empresas para diversos segmentos.

Nesta reportagem ainda, a empresa demonstra que os estudos sobre programas de fidelização começaram por volta de 1990 e eram praticamente restritos, porém este mercado ganhou mais força com a entrada de outros setores. As maiorias dos ataques cibernéticos utilizaram-se de uma técnica conhecida como “Phishing Scam” tendo como objetivo capturar dados legítimos para obtenção de vantagens financeiras pelos

criminosos, porém com as novas medidas de segurança adotada pela empresa e com a campanha de conscientização dos clientes e de seus colaboradores, o volume de fraudes conseguiu ser reduzido, o que demonstra assim um ponto favorável (RISK REPORT, 2016).

Isto demonstra uma atitude consciente e de grande interesse para organização. Neste sentido, complementa-se ainda que as organizações demonstram-se plenas preocupações com relações a questão de confidencialidade, os quais encontram-se disponíveis apenas para usuários autorizados, a fim de realizar assim login no ambiente de trabalho. Este método também conhecido como criptografia é bastante eficiente, pois os dados confidenciais referem-se aos que comprometem assim as partes envolvidas no processo, ou seja, a própria organização (FONTES, 2006).

Garantir a confidencialidade é uma forma de manter organizados os termos, os acessos, a sensibilidade, portanto, é de responsabilidade dos usuários a preservação das informações, como forma de preservar a integridade da empresa (FONTES, 2006).

Com relação à disponibilidade este deve estar disponível a partir do momento do acesso a informação, sendo que cada usuário possui diferentes ambientes de trabalhos, os quais passam a ser disponibilizados pelos gestores. Portanto, para que um sistema seja eficaz, esse deve disponibilizar um sistema computacional de controle, mapeado, com segurança, utilizando-se de chaves de seguranças, senhas, bloqueios, e ainda dos canais de comunicação (FONTES, 2006).

Estes sistemas normalmente atuam com possíveis falhas como é o caso das ocorrências por falta de energia, falhas de hardware e atualizações do sistema. Neste caso recomenda-se a reprogramação dos acessos remotos, porém ele deve ser um ambiente seguro como forma de favorecer assim nas ações (FONTES, 2006).

A segurança de informação deve atuar também com foco na integridade, pois é uma forma da empresa garantir que seus dados não sejam adulterados, destruídos ou corrompidos, sendo recomendada assim a instalação de atualizações e de antivírus nos ambientes organizacionais, restringindo os acessos a sites não autorizados entre outros, como é o caso de atualizações automáticas e do trabalhar com pen drives entre outros.

Existem dois pontos essenciais neste processo como destacado anteriormente, o primeiro diz respeito à transmissão o qual este compromete a integridade e outro é com relação à questão de armazenamento de dados ou da própria coleta de dados,

tornando-se assim fator preocupante para as empresas. Diante dos fatos busca-se assim desenvolver ações de melhorias com relação a Segurança de Informações para as empresas.

Qual a influência para organização atuar com métodos e Sistemas de Segurança da Informação no ambiente de trabalho?

1.2.OBJETIVOS

1.2.1.Objetivos Gerais

O objetivo geral deste estudo é conhecer os principais recursos e tecnologias recentes implantadas pelas organizações para garantir assim um Sistema e Controle de Segurança da Informação eficiente para empresas.

1.2.2.Objetivos Específicos

Os objetivos específicos deste estudo destacam-se através dos elementos fundamentais, iniciando-se por uma revisão bibliográfica sobre o tema de Segurança da Informação bem como outros fatores, destacados abaixo:

- Avaliar-se e conhecer principais riscos dos ambientes corporativos;
- Analisar-se a necessidade de implantação de Políticas de Seguranças;
- Reeducar os colaboradores das empresas;
- Destacar-se principais métodos utilizados para preservação das políticas da segurança;
- Conhecer principais tecnologias utilizadas pelas organizações para evitar o risco e invasão bem como a perda do patrimônio;
- Desenvolver sistemas adequados no ambiente de trabalho para garantir a segurança da informação.

2. REVISÃO BIBLIOGRAFICA

Neste tópico iremos abordar o conceito, aspectos e pilares da segurança da informação e as principais funcionalidades das ferramentas utilizadas para o estudo de caso, Antivírus, Proxy Squid, Autenticação de rede (Active Directory).

2.1.Conceito da Segurança da Informação

Em função do avanço tecnologia e da própria internet o conceito de segurança apresentou mudanças significativas para toda uma sociedade, trazendo benefícios e até mesmo risco, causando assim uma verdadeira revolução no mercado e no mundo dos negócios. Além disso, no segundo milênio já na chamada Era Cristã, diversos acontecimentos ocorreram transformando assim o cenário social da vida humana. Esta revolução modificou também a forma de produzir e transmitir seus conceitos e até mesmo de armazenar suas informações (CASTELL, 2007).

Castell (2007) explica que estas mudanças trouxeram também um impacto significativo, para a sociedade, como se destaca:

> *Tal revolução também modificou a forma de produzir, transmitir, acessar e armazenar informações nas organizações. Consequentemente, a segurança das informações e a segurança das comunicações também evoluíram, tornando-se mais complexas e exigentes de novas metodologias, como afirma a Diretoria de Auditoria de Tecnologia da Informação do Tribunal de Contas da União, na segunda edição de sua cartilha sobre boas práticas em segurança da informação (CASTELL, 2007, p. 34).*

Esta mudança também influenciou-se nas empresas que também passaram a apresentar riscos tanto na execução de seus dados e operações realizadas como da própria segurança da informação, mesmo porque antigamente boa parte dos documentos era armazenada em papel, porém com as mudanças estes passaram a ficar guardados com acessos restritos a determinadas pessoas. Porém, com todas estas mudanças, o uso de computadores passou a realizar boa parte da segurança das informações o que atualmente passou a ser armazenado tanto nos computadores como na rede os principais documentos de uma empresa (CASTELL, 2007).

Entretanto, os aspectos de segurança atingiram o desenvolvimento de métodos necessários, sofisticados a fim de resguardar assim estes documentos, bem como assegurar qualquer acesso a internet. O próprio dicionário da Língua Portuguesa define a palavra segurança como “ato definido de segurar” seja ela um Estado ou uma condição (FERREIRA, 1996).

Neste sentido o conceito de segurança da informação visa atender, agarrar, conhecer e entender os riscos e tais situações frente a um cenário atual envolvendo ainda a questão da informação e da comunicação, visto que atualmente com a internet as pessoas passaram também a compartilhar diversos arquivos através do one drive, e-mails e nos próprios diretórios das organizações, porém, seu uso deve ser limitado

respeitando assim limites, critérios e atender as regras estabelecidas pelas empresas, de modo a não comprometer assim a imagem da mesma ou até mesmo a própria conduta de seus usuários (FERREIRA, 1996).

Existem diversos definições para informações a que melhor se adapta a nossa área e a definição do British Standards Institute, o qual é vista como um recurso com importantes negócios, “que possui valor a uma organização, e, portanto, precisa ser protegido de forma adequada” (FERREIRA, 1996, p. 34).

Neste sentindo, a Segurança da Informação deve atuar com a própria “informação” como explica Ferreira (1996, p. 54), pois ela possui uma vasta e extensiva tecnologia, devendo-se adequar de forma adequada evitando-se os riscos e ameaças para que seja dada continuidade evitando-se assim que ocorram os devidos danos empresariais, ou seja, maximizando o retorno em investimentos e oportunidades.

Para melhor compreensão a seguir se destaca os aspectos de segurança da Informação, como segue.

2.2.Aspectos de Segurança da Informação

De acordo com Pelissare (2002) a Segurança da Informação busca a confidencialidade, disponibilidade e a integridade bem como garantir o uso de forma adequada evitando-se assim riscos tanto para empresa como para seus usuários. Nesta linha, pode-se observar as características e aspectos essenciais no que tange a segurança da informação, como se divide:

- Prevenção: tem como propósito evitar que ocorra assim um risco;
- Proteção do hardware: compreende na segurança física considerado de vital importância. Sua função é negar acessos físicos inutilizados diante de uma estrutura de rede, evitando-se assim que ocorram possíveis roubos de dados, desligamento de equipamentos e demais danos possíveis;
- Proteção de arquivos e dados: compreende no controle de acesso antivírus, no processo de autenticação e verificação se o mesmo está pedindo acesso considerado de real importância. Neste processo de autenticação, é verificado também os pedidos, acessos, e quais as transações são controladas e pertinentes. Um exemplo, citado pelo autor, são o compartilhamento de arquivos protegidos como somente disponível para leitura, ou acesso limitado aos

arquivos e ou pastas. Estas são as formas que as empresas buscam restringir a segurança da informação;

- Proteção do perímetro da rede: compreende nas ferramentas firewall, relacionado com os aspectos que mantém a protegida contra invasão de usuários não autorizados.

A própria ISO/IEC 27702 define e controla o gerenciamento de riscos da segurança da informação, estabelecendo assim procedimento, diretrizes, práticas e estruturas organizacionais, devendo ser realizada de natureza administrativa e com técnica de gestão legal. Seu controle deve ser adotado como uma medida de segurança. Portanto, para cada funcionário novo ao ser contratado os procedimentos devem estabelecer o comprometimento quanto às políticas de segurança da empresa.

A informação e seus processos de apoio, sistemas e redes são negócios definidos, estabelecendo metas, realizando melhorias que são atividades essenciais para garantir assim a competitividade das empresas. Além disso, elas devem atuar de formas legais, atendendo os requisitos, imagem das organizações, evitando-se assim qualquer tipo de ameaça para uma organização (ISO IEC 27002).

Com base nas características de segurança apresentada a melhor forma de alcançar e melhorar o sistema de segurança é evitar danos também causados por códigos maliciosos, que também são conhecidos como “hackers” sofisticados, o que deve atender as leis de mercado, sobrevivendo a corrente de seus clientes e fornecedores, mesmo porque eles incluem ações ilegais, desconfiança, fraudes eletrônicas, vandalismo, sabotagem e espionagem, que podem comprometer toda integridade de uma pessoa como a imagem da própria empresa. É com base neste risco que muitas empresas vêm buscando soluções no mercado para evitar-se quaisquer tipos de riscos (PELISSARE, 2002).

2.3 Pilares da Segurança da Informação

Com relação a segurança da informação inicialmente esta refere-se a uma medida adotada pela empresa visando assim preservar bem como proteger as informações e sistemas de informação, pilares da segurança da informação (BUENO, 2008).

Entre esses pilares estão Autenticidade onde é a garantia que a informação que veio da fonte anunciada, a Irretratabilidade (ou não-repúdio) onde é a garantia que a pessoa não negue que tenha assinado a transmissão da mensagem ou arquivo, a

Confidencialidade que é uma propriedade de que a informação esteja disponível somente às pessoas autorizadas, Disponibilidade onde é uma propriedade de estar acessível e utilizável quando necessário, Integridade onde previne a modificação não autorizada de informações.

É necessário destacar que o uso de pilares é realizado em conformidade com as necessidades específicas de cada organização, portanto, ela deve adequado de acordo perfil da empresa, além de fazer parte da política de segurança da empresa (BUENO, 2008).

Neste sentido Bueno (2008) ressalta ainda que os pilares podem ser determinados por suscetibilidade e ou sistemas realizados pelo nível de ameaças que compreende assim na gestão de riscos. É necessário acompanhamento do pessoal da Tecnologia da Informação para que este acompanhe e monitore constantemente este processo.

Atualmente estes pilares tornaram-se essenciais para o desenvolvimento e preservação dos dados da empresa no mundo atual. Ele é composto por uma arquitetura de segurança que visa assim unificar propósito dos cinco pilares, os quais já fazem parte de empresas de primeiro mundo como forte uso de criptografia, incentivo a educação com relação a segurança, disponibilidade de tecnologia da informação, infraestrutura e disponibilidade de mecanismos de monitoramento contra ataques (BARBOSA, 2016).

Ainda sob a visão de Barbosa (2016) estes ataques referem-se a capacidade de alerta, ações coordenadas, pois no mundo atual o conhecimento da informação se torna essencial e indispensável, pois é um pré-requisito para qualquer sistema. Portanto, é fundamental que as empresas trabalhem desta forma, visando assim resguardar-se.

No tópico a seguir será destacado os principais Sistemas de Segurança utilizados nas empresas, a fim de garantir a segurança e os dados da organização. Neste estudo destacam-se o conceito de Antivírus, Proxy, Autenticação da Rede e o Firewall.

2.4 Antivírus

Segundo a Enciclopédia Encarta (ENCARTA, 2003), o vírus é um programa contagioso de computador: um programa de computador que é parte de outro que se insere e replica-se. Um vírus transporta-se com o programa que contém e pode danificar a integridade dos dados armazenados.

O vírus é um programa que tenta se espalhar de computador em computador, causando danos apagando ou corrompendo os dados.

Segundo a Symantec (SYMANTEC, 2003), um vírus de computador é um programa pequeno desenvolvido para alterar a forma como um computador opera, sem a permissão ou conhecimento do seu usuário. Os vírus podem invadir tanto computadores desktops, notebooks como servidores de rede.

O ideal seria jamais ser infectado, mas pode-se afirmar que nenhum computador está imune aos vírus ou spyware e que não existem programas que possam nos dar 100% de proteção para todos os tipos de vírus. Portanto, é preciso ficar atento com as possibilidades do computador ser contaminado.

Para se proteger desses indesejaveis vírus existem algumas ferramentas gratuitas, entre os antivírus gratuitos mais conhecidos estão: AVG, Avast, Avira,

A diferença do antivírus gratuito para o pago é a quantidade de camadas de proteção. O pago tem como proteção contra spyware, anti-spam, firewall próprio e mecanismo de buscas seguras, já o gratuito tem menos barreiras de proteção eles fazem apenas a detecção e remoção de vírus.

2.5 Proxy Squid

Nos últimos nota-se que com avanço da tecnologia houve um grande desafio para as empresas referente a segurança da informação, mesmo porque com o crescente avanço da internet embora apresentou diversos benefícios este também possibilitou novos riscos para as empresas, como já destacado ao longo deste estudo. Estas ações se tornam necessárias a partir das ações de vários usuários em geral. Além disso, em função de um número excessivo de usuários que se conecta também diariamente aumenta de forma favorável principalmente em redes corporativas, o que demonstram-se cada vez mais ineficientes para atender a demanda (BRIAN, 2001).

Outro impacto este no tempo de resposta utilizado para muitos usuários frente à disponibilidade de informações e utilização incorreta de recursos para alta carga nos servidores. Para isto deve-se minimizar também o tempo, para recuperar-se um arquivo, o que se torna ainda mais complexo em redes corporativas (BRIAN, 2001).

Ainda sob a visão de Brian (2001) para se ter segurança às empresas devem precaver-se, resguardando assim seus documentos, caso estes venham ser danificados. No caso da Web este também é complicado, pois o tempo de resposta

ainda é bastante demorado, uma vez que ele depende de uma série de fatores como o tipo de conexão, tamanho do arquivo e localização dos mesmos.

Como consequências deste crescimento deve-se adotar alguns métodos como é o caso da utilização dos servidores que compreende na alteração dos meios físicos (cabos, roteadores e switches) para aumentar assim a taxa de transferência, o que não é economicamente viável, pois envolve uma série de fatores para uma única transação da Web (TANENBAUM, 1997).

Para isto vem sendo desenvolvidos e adotados os servidores Proxy que na verdade passa a ser um espelho dos arquivos. Esta solução bastante inteligente e já implantada em muitas organizações favorece na segurança de dados, além de contribuir também para atender todas as requisições de seus usuários de forma eficiente. Este tipo de servidor direciona ainda as requisições dos usuários para determinado serviço, funcionando como um filtro, pois sua função é analisar a requisição e defini-la de forma adequada podendo ou não ser direcionada para o servidor, como destacado na Figura 1 (TANENBAUM, 1997).

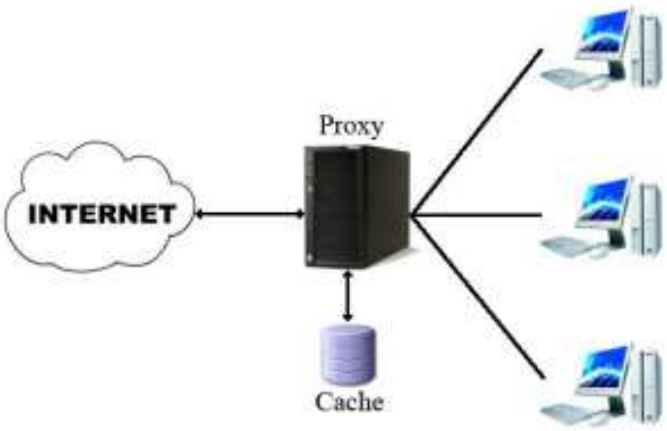

Figura 1: Função do Proxy (Tanenbaum,1997).

Este processo também é conhecido como autenticação de usuários realizado pelo servidor Proxy, tem como papel trabalhar as informações de modo seguro, sendo que qualquer analisador pode interceptar nos dados. Um exemplo ocorre quando um computador é adquirido a um endereço na internet, cadastrando-se assim o nome do usuário e a senha, que são solicitadas pelo servidor Proxy para liberação da sessão e navegação como explica Tanenbaum (1997).

Este código e senha é facilmente identificado, porém nenhum mecanismo de autenticação é mais seguro, realizando ainda processo de login para garantir a

segurança da informação, juntamente com a requisição de dados. Este protocolo realiza um processo de autenticação por meio do mecanismo denominado de “challenge-response”, estabelecendo assim uma comunicação criptografada para atender a validade da senha e por conseguinte a autenticação do usuário (TANENBAUM, 1997).

Este ferramenta é de grande importância para organizações, pois é uma forma de garantir a segurança dos usuários em rede, eliminando também a possibilidade de outro usuário entrar com outra conta para acesso a Internet, pois a autenticação do Proxy utilizará de forma automatica a conta devidamente fornecida para este processo de login no computador, favorecendo de forma eficiente no processo da garantia da informação (TANENBAUM, 1997).

Outra necessidade de adequação frente ao processo de segurança da informação é autenticação da Rede, como se destaca a seguir.

2.6 Autenticação de Rede (AD)

O Active Directory (AD) tem um importante papel central para Tecnologia da Informação tendo como propósito fornecer um local para armazenamento de dados centralizado para contas de usuário, adesões de grupos e configurações de software. Seu papel é disponibilizado por meio da autenticação de usuário, acesso a objetos como as impressoras e arquivos os quais passam a ser disponibilizados em seus diretórios com seus devidos atributos (SAMBA ORG-1, 2013).

O AD é um serviço de diretório desenvolvido pela Microsoft sendo um software proprietário, utilizando-se dos sistemas operacionais de redes, porém ele se faz presente desde a versão Windows Server 2000 até sua versão atual Windows Server para 2012. Este foi criado com objetivo de atender o acesso rápido das informações em diretórios.

As ferramentas da Microsoft AD é um software pago que apresenta um custo para empresas, sendo necessário também que o seu uso seja realizado por meio de um sistema operacional Windows Server, porém ressalta-se que o mesmo depende de licença do sistema operacional, porém outro ponto crítico para empresas é que ele também requer de Licença de Acesso Cliente, para que se tenha assim o direito de acessar computadores na rede, serviços e tecnologias nas máquinas para seus clientes e ou por usuários (SAMBA ORG-1, 2013).

Como recomendações para empresas o AD é um serviço que gerencia de forma eficaz os recursos da rede, armazenando as informações generalizadas sobre todos os recursos disponíveis, facilitando a pesquisa, bem como a autenticação. Um serviço de diretório pode armazenar informações de forma organizada, para que assim facilite a recuperação das mesmas (STANEK, 2009).

Stanek (2009) explica também que os serviços de Diretórios estão disponíveis no mercado através de alguns softwares proprietários a partir de um número de fornecedores. Em sua forma básica este requer de pesquisas de chaves e valores atribuindo assim seus respectivos valores nas informações estruturadas.

Como recomendações toda hierarquia da empresa deve ser realizada de forma organizada, uma vez que ele integra um conjunto de protocolos modernos de autenticação para redes de computadores, mantendo assim protocolos antigos como o NT4 que é um serviço de Diretório NT (STANEK, 2009).

O Serviço de Diretório emprega também vários protocolos para seu funcionamento, sendo que o protocolo principal é o acesso ao Active Directory e o LDAP (Lighweight Directory Acess Protocol) que na verdade é um protocolo padrão do setor para acesso a diretórios administrados pela TCP / IP.

É válido destacar que os protocolos envolvidos se tornam assim regras usadas para que haja comunicação de dados entre computadores que fazem com que dois ou mais computadores possam realizar a troca de mensagens entre si (COMER, 2007).

2.7 Firewall

O Firewall tem como função restringir-se a comunicação para Internet oferecendo um modelo de conectividade sem limites, porém ele não oferece solução aos problemas de segurança, mas sua configuração é realizada por meio da função de ser atingida. Inicialmente este processo foi utilizado e inserido em roteadores na década de 80, por apresentar posição privilegiada (SILVA, 2003).

As regras de filtragem são baseadas nas origens, destinos e tipo de pacote, porém com advento da Web, foi necessário separar também sua funcionalidade do firewall para roteadores, prestando assim atenção para assunto de segurança e da própria dificuldade, aparecendo várias tecnologias e pacotes, tais como, proxies, híbridos e adaptativos (SILVA, 2003).

Com estas mudanças foram necessários também maiores focos e atenção para os filtros de pacotes, como é o caso do gerenciamento da banda, balanceamento de cargas entre outros. Sua funcionalidade envolve um conjunto de sistemas que exerce influência no plano de segurança de dados existentes da organização e principalmente de usuários não pertencente a elas (SILVA, 2003).

Este conjunto de técnicas diferentes visa resolver problemas e soluções que dependem de serviços para empresa, planejando quais são os possíveis riscos que se consideram aceitáveis, porém o mesmo demanda tempo, recursos financeiros e conhecimento técnico disponível na empresa. O objetivo do firewall é formar uma linha fechada de defesa projetada para proteger assim os bens internos da empresa o qual requer de conhecimento e de uma boa administração para se ter bons resultados (NAKAMURA, 2002).

Para tal, deve-se ainda assegurar as condições, as partes integrantes e o estabelecimento de uma política de segurança de informação, pois todo tráfego de dados dentro e fora da rede corporativa deve ser administrado passando a ser obrigatoriamente pelo firewall, o qual realiza assim um tipo de inspeção (NAKAMURA, 2002).

Deve-se ainda permitir a passagem de tráfego de forma específica autorizando assim uma política conservadora bloqueando imediatamente qualquer tipo de acesso e até mesmo por conta dos próprios usuários que apresentam riscos. Portanto, a tecnologia do firewall atualmente se torna indispensável para organizações, pois ela controla o tráfego entre duas redes, bloqueando redes exteriores (NAKAMURA, 2002).

Este processo é necessário para empresas que trabalham com clientes remotos, além de oferecer vantagens deste sistema o mesmo pode assegurar, destacando os facilitadores que devem criar um ponto único de controle bloqueando acessos não autorizados, não permitindo serviços e dados vulneráveis da rede interna e conceber proteção contra diversos tipos de ataques, oferendo possibilidade de monitoração centralizada e criação de alarmes de invasão (NAKAMURA, 2002).

Entre outras palavras este sistema protege também para que não ocorram ataques provenientes do uso de internet, porém as empresas devem investir em tecnologias adequadas para gerar relatórios (SILVA, 2003).

3. METODOLOGIA E ESTUDO DE CASO

Nesta seção será apresentado a metodologia e o estudo de caso da empresa, onde será mostrado a organização antes das instalações dos devidos softwares para obter segurança da informação e demonstrando os resultados obtidos após a implementação.

3.1 Metodologia

Como destacado ao longo deste projeto o trabalho em si apresentará um estudo de caso de uma empresa de médio porte que atua na região de Barueri. Esta empresa por atuar com processos de melhorias de tecnologia da informação passou a implementar e desenvolver melhorias para seus clientes partir da introdução de uma Política de Segurança como recomendação dos Sistemas ISO 9001/2015 que visa garantir qualidade total de seus produtos e processos mantendo a fidelização de seus clientes.

Neste sentido destacam-se algumas ações de Segurança da Informação realizada pela empresa objeto deste estudo que envolve desde a necessidade de aquisição de equipamentos e softwares de controles eficientes, bem como as melhorias realizadas nos sistemas de proteção de e-mails e spam, além-claro, da proteção por senhas e usuários cadastrados no ambiente de usuários definidos por perfil.

Para isto será utilizado das contribuições de Silva e Stein (2007) que tratam da Segurança das Informações nas organizações, iniciando-se uma reflexão sobre atitudes, conhecimento dos colaboradores, a fim de conhecer um pouco da história da Segurança da Informação, para isto será utilizada do conceito da velha engenharia social, bem como das contribuições dos métodos aplicados às empresas no que tange a política de segurança dos autores José C. Gonçalves e de Soares 1995 que tratam sobre o Gerenciamento da Informação.

Para a construção da pesquisa bibliográfica utilizou-se como norte as orientações de Gil (2010) que define a mesma como um método de processo de estudo de caso, iniciado a partir de livros, artigos, revistas e teorias como contribuições. Este conceito visa ampliar o conhecimento, analisando assim diferentes pensadores para que sejam atendidos os objetivos específicos deste estudo.

Segundo Gil (2010) a pesquisa bibliográfica tem como base o material publicado por diferentes autores, resultado de estudos como teses, resenhas e obras de referências que possuem relevância, podendo ser essencial no desenvolvimento deste estudo.

Ainda segundo Gil (2010) a pesquisa em si visa atender o foco proposto, realizando uma análise de dados frente ao comportamento de diferentes organizações, conhecer o resultado obtido por meio de dados e amostras, ou ainda, por meio de uma interrogativa que busca o alinhamento dos processos.

O processo compreende desde um planejamento realizado através das informações bibliográficas, consideradas obras que oferecem maior visão sobre os fatos, contribuindo assim para a elaboração do trabalho de pesquisa científica. O estudo de caso trata-se uma investigação com base na pesquisa empírica, conhecendo fatores que comprometem a segurança da informação nas empresas contribuindo assim para a realização desta pesquisa. O mesmo é obtido por meio de uma formulação para um determinado problema, que possa assim ser comprovado através das hipóteses descritas ao longo do processo (MARCONI e LAKATOS, 2003).

Portanto, os resultados obtidos neste estudo serão previamente analisados, estudados e apresentados como forma de favorecer assim na própria análise de dados e resultados da empresa.

Para melhor clareza serão apresentados alguns exemplos de ferramentas utilizadas pelas grandes organizações, tais como, Proxy Squid que é um sistema de filtragem de conteúdo da internet, baseado nas políticas da empresa adequado de acordo com perfil de usuário, autenticação da rede (AD) para acesso a documentação de rede, acesso a rede wireless entre outros. Também será apresentado os benefícios do Firewall para bloqueio e permissão de acesso a redes de servidores, rede de usuário entre outros, principalmente para empresas que trabalham com sistemas via remoto.

3.2 Estudo de caso

Este estudo foi levado em conta, uma empresa antes de ser feita a instalação dos devidos sistemas de segurança. Antigamente só havia uma rede “caseira”, onde qualquer pessoa desconhecida poderia ter acesso, levando assim a perda de informações.

Como a empresa era nova, não existência uma estrutura de políticas, normas e procedimentos, além dos softwares não serem originais, podendo assim ter problemas futuros.

Na empresa havia somente um servidor de arquivos, onde não tinha nenhum tipo de estrutura e segurança, dessa forma, qualquer setor, acessava os documentos do financeiro, ocorrendo um grande risco de roubo de informação.

Além da empresa não ter nenhum tipo de segurança, não dependemos somente da segurança em si, e sim dos próprios usuários, pois, isso é um fator determinante para o sucesso ou fracasso do processo de segurança da informação em uma organização.

3.3 ANÁLISE DOS RESULTADOS

A empresa objeto deste estudo é uma empresa que busca a segurança da informação em seus clientes, para garantir a execução de processos eficientes, armazenamento de banco de dados, transferências de dados, implantação de softwares de controle e gerenciamento.

Como a empresa deste estudo trabalho com pequenos clientes, estas mudanças foram necessárias para garantir a preservação de dados dos seus clientes bem como a própria imagem da empresa. Estas mudanças foram introduzidas pela própria exigência da ISO/IEC 27702 o qual define-a e controla o gerenciamento de riscos da segurança da segurança da informação nas organizações. Outra mudança realizada na empresa foi à implantação de sistemas de antivírus para seus computadores sendo um processo o qual acaba bloqueando qualquer tipo de mensagem que apresente risco para organização.

A figura 2 demonstra um exemplo da tecnologia implantada pela empresa

Figura 2: Modelo de Tela de Bloqueio de Antivírus (RT IT, 2016).

O sistema de antivírus é uma necessidade para as empresas, pois ele bloqueia site de jogos, bebidas e redes sociais. Caso o antivírus não bloqueie tem outra opção também que a empresa passou a utilizar-se que foi a implantação do servidor Proxy Squid que realiza também o bloqueio de sites.

Entre as principais diferenças apresentadas por cada um pode-se destacar segundo a visão de Silva (2003) como no caso do firewall (bloqueia a saída de dados do seu computador), e do antivírus a entrada de antimaware (impede a entrada de arquivos que danificam assim sua máquina), antispyware (bloqueia pop-up), antiphishing (tem como função detecta e-mails falsos) e antispam (bloqueia o acesso a determinados conteúdos).

Todas estas ações contribuem para a segurança da informação da empresa, estas melhorias resultam conforme demonstrado nas figuras abaixo onde é inserido um site para bloqueio no Proxy Squid e logo em seguida o site é bloqueado

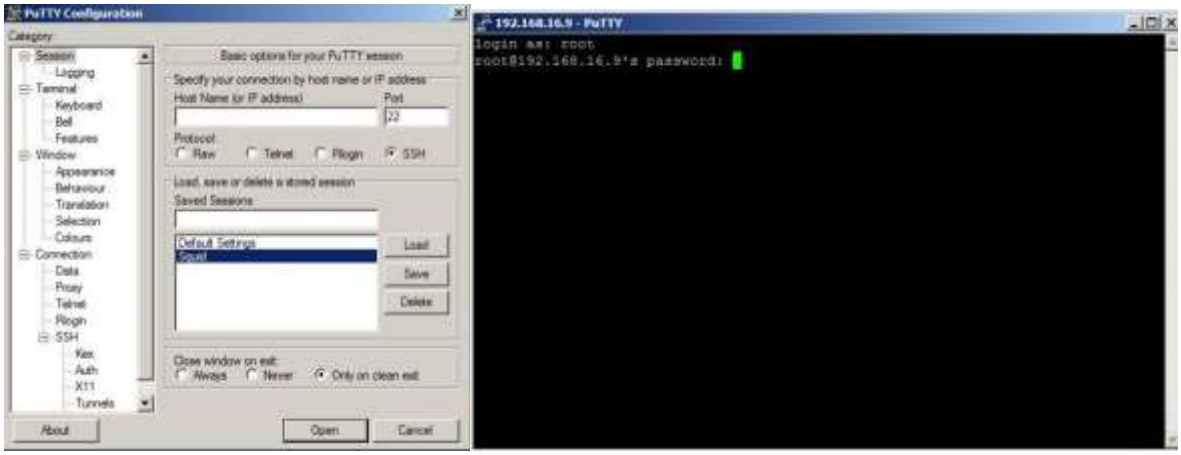

Figura 3: Acesso ao Proxy Squid e inserção de usuário e senha (RT IT, 2016).

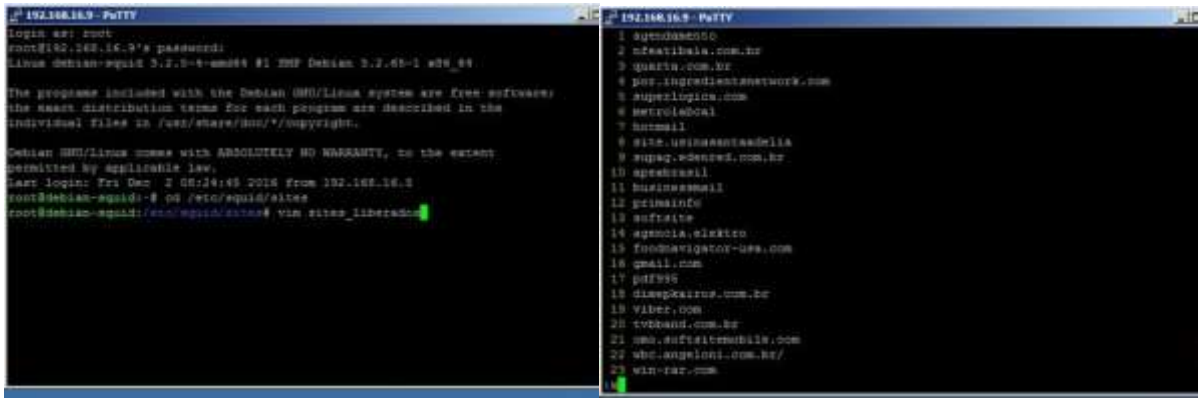

Figura 4: Inserção do site a ser bloqueado (RT IT, 2016).

Figura 5: Exemplo de Bloqueio de Tela (RT IT, 2016).

Este sistema atua como se fosse uma spam, que visa garantir o acesso a sites restritos que oferecem riscos para empresa. Este trabalho é recomendado desde que seja instalado por mio de sistemas de antivírus, podendo ser comprado com as devidas licenças ou ainda através do uso do tipo Avast que é totalmente gratuito.

O antivírus demonstra-se eficaz detectando todo tipo de código malicioso presenciado nas transações eletrônicas, como no caso cavalo de tróia e outros capazes de modificar-se de vírus. Este antivírus reduz muito a probabilidade de entrada das ameaças para navegar na internet (COMER, 2007).

Seu objetivo é reduzir a probabilidade de entrada de ameaças para navegar na internet reduzindo assim a possibilidade de perda das informações, evitando-se danos que podem causar o sistema operacional, ou a necessidade de reinstalar e operar com seus programas. O Antivírus Trend, que foi utilizado para esse estudo, é um antivírus pago, portanto, seu recurso é de fácil acesso devendo ser instalado em todos os computadores.

Outra medida adotada pela empresa foi introduzir o sistema de cadastro para cada usuário estabelecido de acordo com a política de segurança da empresa, que automaticamente o usuário não utiliza-se do computador ou notebook, automaticamente o mesmo realiza o bloqueio de tela por meio de assinaturas digitais, atendendo ao critério que é definido por tempo durante a sua configuração.

Estas ações se tornam formas seguras de trabalhos, porém para esta ferramenta ser funcional, foi necessário realizar a criação do usuário no Active Directory (AD), como segue abaixo:

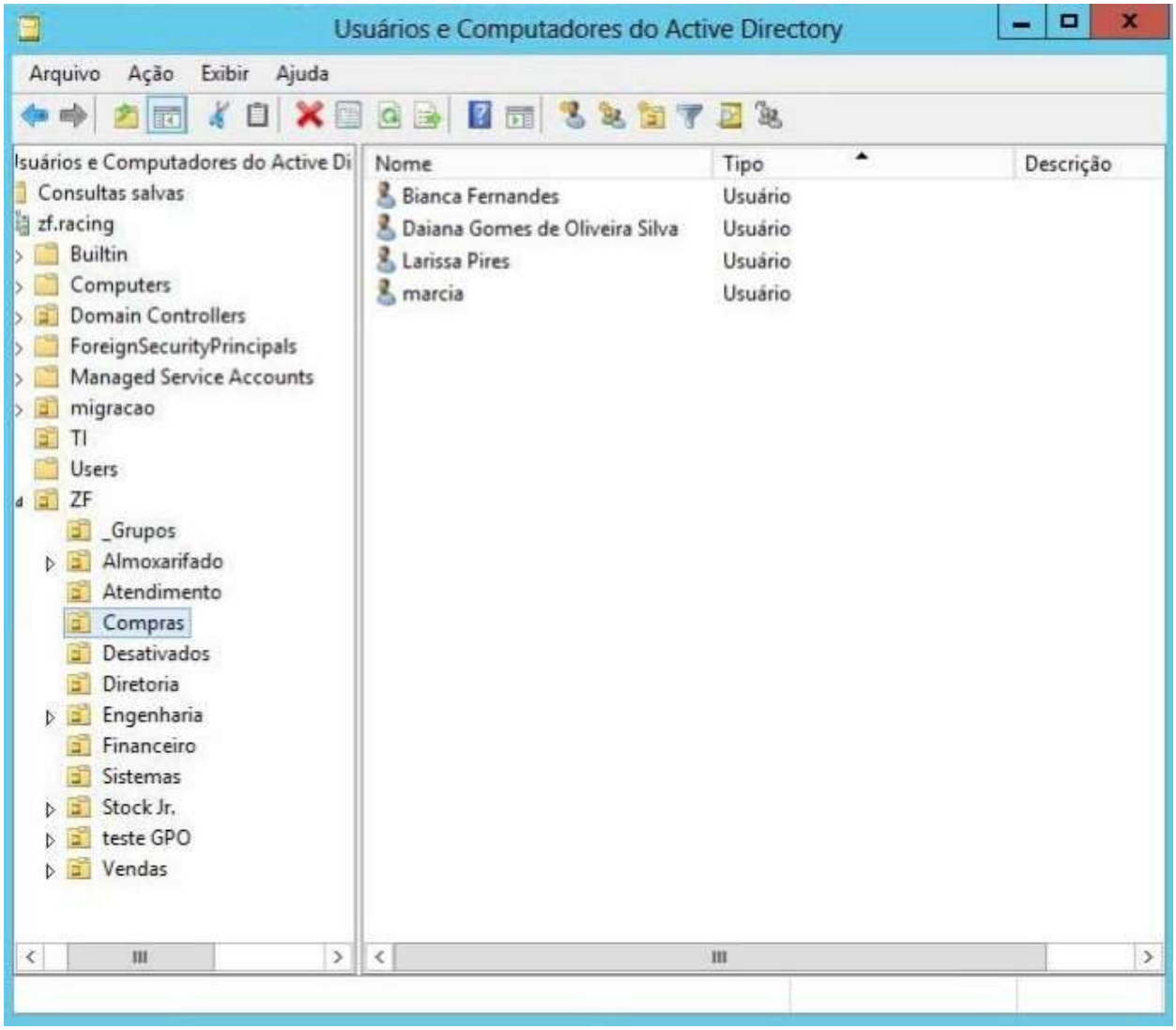

Figura 6: Local onde é criado o usuário de rede (RT IT, 2016).

Figura 7: Exemplo de Bloqueio de Tela Automático (RT IT, 2016).

É muito comum ocorrer o ataque de senhas podendo ser realizado com certa facilidade principalmente quando a pessoa passa a ser especialista nesta área, portanto, se houver uma diretiva de bloqueio de conta de usuário após um determinado tempo e número de tentativas de logon, o sistema é automaticamente bloqueado e poderá ser evitado. Esta diretiva pode levar também ao bloqueio de vários usuários da rede durante uma tentativa de invasão, portanto, nestes casos recomenda-se a instalação do firewall (SCAMBRAY et. al., 2001).

A empresa também adotou o bloqueio de qualquer download ou transferência de programas sendo que este somente pode ser executado por funcionários autorizados evitando-se download inadequado e impróprio para uso. Este requisito se faz necessário, pois a blindagem utilizada para proteger é um bem intangível que neste caso é a informação dentro das organizações, como demonstrado na Figura 8.

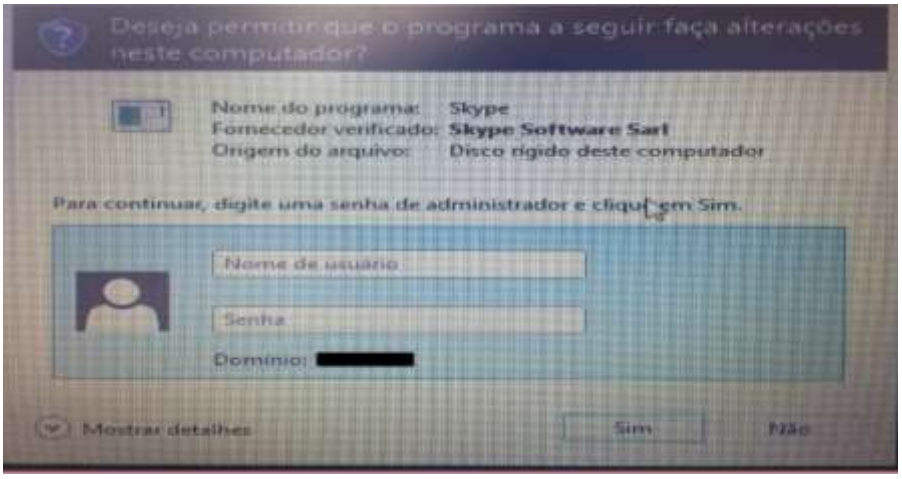

Figura 8: Criptografia para Execução de Download (RT IT, 2016).

Com base neste conceito, embora seja inevitável correr-se o risco é necessário adotar medidas de seguranças necessárias para organizações, porém é inevitável estar sujeitos a riscos, pois a todo momento surgem novas vulnerabilidades e ameaças, os riscos estão realacionados com diversos componentes básicos de segurança, ameaças e riscos. Porém como recomendação a empresa deve sempre realizar uma análise de riscos.

Carvalho (2003) explica que a criptografia e descriptografia é um conceito chave que contém informações relevantes que o destinatário possui, a criptografia deve ser objetiva e corresponder as informações de forma sigilosa para qualquer pessoa sem autorização.

Infelizmente é inevitável não estar sujeito a riscos, pois a todo o momento surgem novas vulnerabilidades e ameaças, pois os riscos se relacionam com diversos componentes básicos de segurança. A análise e avaliação de riscos é uma importante maneira de realizar o levantamento de ameaças, vulnerabilidades e impactos onde os ativos de informação encontram-se dispostos e sujeitos o que cabe também a própria consciência e conhecimento dos usuários, portanto, eles devem ser treinados pelos próprios responsáveis da área de suporte em tecnologia da informação, pois de nada adiantaria um sistema eficiente se as pessoas não se utilizam de forma adequada (TERADA, 2000).

Enfim, conclui-se que todas estas medidas contribuíram para que a empresa tivesse uma nova posição no mercado obtendo um crescimento de 5% nos últimos meses.

4. CONSIDERAÇÕES FINAIS

Como observado ao longo deste estudo, este favoreceu diversas ações e mudanças na vida cotidiana tanto das pessoas como das organizações. Porém no ambiente corporativo cada dia surge uma nova forma de conectividade e comunicação entre os mais variados elementos, requerendo assim sistemas de segurança adequados por meio de assinaturas, logon, criptografias e protocolos que são ferramentas e aplicativos operacionais que devem ser adequados dentro da estrutura física.

Além disso, é muito comum ocorrer também ataque de hackers, portanto, é por conta deste que as empresas vêm buscando investir cada vez mais na segurança da informação estabelecendo ações e melhorias, pois é uma forma de se cobrir diversas áreas de riscos, sejam através da própria estrutura física, infraestrutura da tecnológica bem como das aplicações e conscientizações organizacionais, porém cada uma apresenta um risco e ameaça que podem minimizar o nível de exposição exposta, visto que seu principal foco esta na própria segurança da informação que é seu maior patrimônio.

É muito comum as empresas se protegerem com sistemas de antivírus e de firewall como destacado ao longo deste estudo, que são questões importantes que oferecem meios seguros no ambiente de trabalho, porém muitas vezes a segurança da informação depende também do próprio uso adequado de seus colaboradores, principalmente na execução de download, no compartilhamento e recebimento de

dados e ou ainda nos acessos realizados por meio de comunicação, como é o caso do e-mail, então por causa desses motivos a empresa realizou algumas reuniões com cada departamento, para que fossem orientados a seguir os novas normas e procedimentos.

Outros fatores que também podem comprometer a segurança da informação é que este deve ser limitada, atendendo aos requisitos do ambiente corporativo, da tecnologia, dos processos e das pessoas. Para isto, as empresas devem estabelecer Políticas de Segurança adequadas, normas e procedimentos.

Estas mudanças envolve uma própria mudança de cultura da empresa como de seus colaboradores, porém é válido destacar também que é necessário implantar a adequação de rede, de modo a obter-se também um armazenamento adequado de informações, realizando backups diários, trabalhando com informações generalizadas de forma organizada facilitando a recuperação das mesmas.

Estas ações demonstram eficiências para empresa, embora sejam recursos com custo elevado, atualmente existem diversas formas de se proteger como sistemas de antivírus que hoje já são disponibilizados de forma gratuita, porém alguns métodos devem ser adquiridos para que a segurança da informação deva ser resguardada, pois trata-se do patrimônio empresarial.

Os sistemas de spam também demonstram-se eficientes, podendo ser adequado de acordo com perfil de cada colaborador. Entre as principais operações realizadas pela empresa foi o estabelecimento de procedimentos de trabalho para seus colaboradores, a conscientização dos mesmos, o qual implantou sistemas de bloqueio de telas de antivírus, bloqueio de sites que oferecem riscos para empresa, como acesso as redes sociais, jogos e outros sites de riscos, adequação de perfis e a criptografia.

Para obter maior segurança a empresa também implantou um Proxy Squid que bloqueia sites e firewall, bloqueando a saída e entrada de dados da rede.

Com isto, é válido destacar que a segurança da informação não depende somente das ações de hackers, mas sim das próprias ações das pessoas que a executam, sendo necessário assim realizar ações com confidencialidade, integridade e disponibilidade, ou seja, apenas para as entidades autorizadas. Estas ações também devem ser aplicadas pelos funcionários durante a execução de trabalhos em terceiros,

como no caso da realização de trabalhos em cliente, a fim de proteger também e garantir a execução dos trabalhos de forma eficiente.

Entre outras palavras a segurança da informação é um método de trabalho que deve ser implantando em todas as empresas, pois seu maior patrimônio encontra-se no conhecimento ali aplicado, portanto, como recomendações sugere-se adoção da implantação dos antivírus e das ferramentas do firewall, da autenticação de rede e principalmente do proxy. Portanto, conclui-se que estas ações se tornam favoráveis para garantir assim a segurança da informação.

Como recomendações sugere-se um estudo mais aprofundado sobre os principais tipos de servidores e backup, quais são suas funções e como elas agem dentro do ambiente corporativo.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BERNSTEIN,T; BHIMANI, A; SHUTZ, E. *Segurança na Internet*. Rio de Janeiro. Campus, 1997.

BERNSTEIN, B. *Pedagogy, Symbolic Control and Identity*. Oxford, England: Rowman & Littlefield Publishers, Inc, 2000.

BRASIL. *Norma ABNT ISO 9001/15*. Sistemas de Segurança da Qualidade. Publicado em: 30/09/15. Disponível em: < https://www.abntcatalogo.com.br/norma.aspx?ID=345041> Acesso em: 17 Set. 2016.

BRASIL. *Norma ABNT ISO IEC-27002/13*. Segurança da Informação. Disponível em: <https://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1> Acesso em: 14 Set. 2016.

BRIAN, P. *Proxy – Recursos Tecnológicos*. Estudo de Caso. FGV, 2001.

CASTELLS, Manuel. *A Galáxia da Internet: Reflexões sobre a Internet, os negócios e a sociedade*. Rio de Janeiro: Jorge Zahar Editor, 2003.

CASTELLS, Manuel. *A Sociedade em Rede*. Editora Paz e Terra S/A, São Paulo, 2007.

COMER, Douglas E. *Redes de Computadores e Internet*. Porto Alegre, Bookmanm 2007.

DA SILVA, Denise R. P.; STEIN, Lilian M. *Segurança da informação: uma reflexão sobre o componente humano*. Ciências & Cognição, Porto Alegre, RS, v. 10, p. 46-53, mar. 2007.

FERREIRA, Aurélio Buarque de Holanda, Novo Dicionário da Língua Portuguesa, 2ª edição revista e aumentada, Editora Nova Fronteira – Rio de Janeiro, RJ – 1996.

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

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5. ed. São Paulo: Atlas, 2010. 184p.

L.SOLVER. *Histórico da Empresa*. Publicado em: Março, 2016. Disponível em: <http://www.lansolver.com/empresa.html> Acesso em: 18 de Setembro, 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia científica*. 7. ed. São Paulo: Atlas, 2010.

MORAES, F. A; CIRONE.C.*A Redes de Computadores, da Ethernet á Internet***.** Editora Érica. São Paulo-SP. 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. *Segurança De Redes Em Ambientes Cooperativos*. São Paulo: Berkeley, 2002.

PELISSARI, Anderson Soncini; GONZALEZ, Inayara Valéria Defreitas Pedroso; VANALLE, Rosângela Maria. *Gestores de Pequenas Empresas: Estudo do Papel e das Funções Gerenciais*. In: SEGeT. IV Simpósio de Excelência em Gestão e Tecnologia, 2002, Resende/RJ. v. 1. p. 1-16.

PELISSARI, Fernando Antônio Brossi. *Segurança De Redes e Análise Sobre a Conscientização Das Empresas Da Cidade De Bauru (SP) Quanto Ao Problema*, 2002. Monografia - Faculdade de especialização em Informática, UNESP, Bauru.

RISK REPORT. *Fraudes Miram Programas de Fidelização*. Publicado em: Março, 2016. Disponivel em: <http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=23662&sid=42> Acesso em: 14 Ago. 16.

SAMBA ORG-1. *What is Samba*. Disponível em: <www.samba.org/what-is-samba.html> Acesso em: 14 Set. 2016.

SILVA, Lino Sarlo da. *VPN – Virtual Private Network*. São Paulo: Novatec, 2003.

SOARES, Luiz Fernando Gomes Et Al. *Redes de Computadores - das LANS, MANS e WANS às redes ATM*. 2°.Ed. - Rio de Janeiro: Editor Campus, 1995.

STANEK, Willian.*Windows Server 2008: Guia Completo*. Porto Alegre Bookman, 2009.

STEINER, Jenifer. G. NEUMAN, Cliford, SCHILLE, Jeffrey, I. Kerberos: *Na Authentication. Service for Open Network Systens*. Publicado em: março, 1998.

Disponível em: <www.cse.d.ed/dthain/courses/csc40771/fall2004/papers/kerberos.pdf> Acesso em: 14 Set. 2016.

TANENBAUM, Andrew S. *Redes de computadores*. 3. ed. Tradução nome do tradutor/a. Rio de Janeiro: Campus, 1997.

TAVARES, Mônica. *Governo Investirá R$ 1 Bi Anual em Banda Larga*. O GLOBO. Rio de Janeiro. 02 de abril de 2011. Digital & Mídia.

ZWICKY, CHAPMAN, D.B. *Building Internet Firewalls*. O' Reilly & Associates, 2000.