INSTITUTO ENSINAR BRASIL
FACULDADES INTEGRADAS DE CARATINGA

FERNANDO OLIVEIRA DE ALMEIDA

Implantação e análise da ferramenta PFsense como firewall em uma empresa de médio porte baseado na ISO\27001

Caratinga
2017

FERNANDO OLIVEIRA DE ALMEIDA
FACULDADES INTEGRADAS DE CARATINGA

Implantação e análise da ferramenta PFsense como firewall em uma empresa de médio porte baseado na ISO\27001

Monografia apresentada à banca examinadora da Faculdade de Ciências da Computação das Faculdades Integradas de Caratinga, como requisito parcial das exigências para obtenção do título de Bacharel em Ciências da Computação, sob orientação do Prof. MSc. Jonilson Batista Campos.

Caratinga
2017

rede de ensino DOCTUM

FACULDADES INTEGRADAS DE CARATINGA

FOLHA DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado: IMPLANTAÇÃO E ANÁLISE DA FERRAMENTA PFSENSE COMO FIREWALL EM UMA EMPRESA DE MÉDIO PORTE BASEADO NA ISO\27001, elaborado pelo aluno FERNANDO OLIVEIRA DE ALMEIDA, foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de Ciência da Computação das Faculdades Integradas de Caratinga, como requisito parcial da obtenção do título de:

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO

Caratinga, 14 de dezembro 2017

Prof. Jonilson Batista campos (Orientador)

Prof. Wanderson Miranda Nascimento (Debatedor 1)

Prof. Vagner Aquino Zeferino (Debatedor 2)

AGRADECIMENTOS

Primeiramente agradeço a Deus, por ter me guiado, dando forças e por ter abençoado meu caminho nessa etapa da minha vida.

À minha família pelo incentivo e apoio durante todo esse percurso. Em especial a minha Mãe Sebastiana Oliveira de Almeida e meu pai Silvério Teixeira de Almeida, por toda contribuição e conselhos durante este período acadêmico.

Agradeço ao Leandro Xavier Timóteo e a Sheila Valquíria Gomes Timóteo, por permitir a realização deste trabalho em sua empresa.

Agradeço a minha namorada Rafaela Cristina que sempre esteve ao meu lado, me dando força nesta jornada.

Agradeço aos meus amigos e em especial Cesar Bento da Silva, por não ter medido força para me ajudar na execução deste trabalho.

A todos os professores, pela partilha de conhecimentos e ensinamentos que levarei por toda minha vida. Por fim, agradeço ao meu orientador Jonilson Campos, por ter me conduzido desde o início com dedicação e paciência.

A todos a minha mais sincera gratidão!

RESUMO

Atualmente um grande número de informações transitam constantemente via internet, porem parte destes dados são sigilosos, como por exemplo, transações bancárias, dados de clientes, ativos, regras de negócios e tantos outros espécimes de informações. Entretanto, a troca de informações sem uma segurança adequada pode se tornar perigosa e consequentemente atrair Cracker interessados em roubar tais dados e infectar redes acarretando em perdas substanciais. Com a percepção deste problema, as empresas vêm buscando proteção através de ferramentas de *firewalls*. Atualmente o mercado da tecnologia da informação disponibiliza vários tipos de software de proteção, contudo essas ferramentas tem preços expressivamente altos. O presente trabalho expõe a utilização de um *Firewall* em *software* livre chamado *PFSense* em empresas que possuem baixa receita para gastos na área de segurança, mas que mesmo assim, necessita-se de uma proteção, para que seus dados sejam mantidos internamente ou trafeguem de forma segura para o ambiente externo. Este ínterim apresenta o resultado da implementação do *Firewall PFSense* deliberada para o atendimento da demanda de segurança de empresas emprega-se mecanismos de prevenção de ataques e furtos de informações.

Palavra-chave: Segurança, *PFSense, Firewall,* Rede Corporativa.

ABSTRACT

Nowadays a large number of information that constantly travels through the internet, parts of this data are confidential, such as bank transactions, customer data, assets, business rules and so many other specimens of information. However, the exchange of information without proper security can become dangerous and consequently attract hackers interested in stealing such data and infecting networks leading to substantial losses. With the perception of this problem companies are seeking protection through firewalls tools. Nowadays the information technology market offers several types of protection software, however these tools have expressively high prices. The present work exposes the use of a free software firewall called PFSense in companies that have low revenues for security spending, but which nevertheless require protection, so that their data is kept internally or safely traversed to the external environment. This interim presents the result of the implementation of the PFSense Firewall deliberate to meet the security demand of companies employing mechanisms to prevent attacks and thefts of information.

Keyword: Security, PFSense, Firewall, Corporate Network

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FTP	File Transfer Protocol
GB	Gigabyte
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ID	Identification
IP	Internet Protocol
ISSO	International Organization for Standardization
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
MAN	Metropolitan Area network
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PING	Packet Internet Network Grouper
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
SGSI	Sistema de gestão Segurança da informação
SNA	System Network Architecture
SSID	Service Set Identifier
SSL	Secure Socket Layer
TI	Tecnologia da Informação
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WEB	World Wide Web
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Acces II

LISTA DE ILUSTRAÇÕES

SUMÁRIO

.

1 INTRODUÇÃO

Com a evolução nos sistemas de comunicações, o acesso a informação se torna cada dia mais democrático, universal e a internet tem papel fundamental na evolução do mercado corporativo atual. Com amplo acesso a informações, é essencial o desenvolvimento de equipamentos com competência de prover a segurança das informações trafegadas pela rede. Desta forma, estas ferramentas são responsáveis por uma série de funcionalidades, como por exemplo, o controle de entradas, para evitar acessos danosos ou não permitidos as informações.

Com a ampliação da utilização da rede de computadores, se torna impreterível o investimento em segurança, pois pessoas mal intencionadas tentam corromper dados e informações criando mecanismos para furtos de serviços e produtos, dando grande prejuízo financeiro às empresas de pequeno e grande porte chegando até às multinacionais, além do vazamento de vários dados importantes de ONGs, hospitais, países e etc. O número de usuários da internet vem crescendo e cada vez mais colaborando para que o computador fique vulnerável pelo fato desses usuários compartilharem senhas e informações em redes desprotegidas. Pela falta de conhecimento do próprio usuário ou de um mecanismo de segurança que proteja essas informações (PUGLIESE & LOVISI, 2015).

No mercado corporativo atual existem uma variedade de tipos de comunicações, o que tornou a transferência de informações mais instantânea a cada dia. Outro fator em destaque é a extensão da internet e das redes de computadores que trazem vários problemas de segurança, a confiabilidade das informações para estas empresas e instituições que utilizam da tecnologia, através de computadores e dispositivos interconectados em rede, nos seus negócios.

Com o crescimento das comunicações cliente-servidor, faz-se necessário a utilização de mecanismos de prevenção de ataques e furtos de informações. A partir dessa demanda, foi desenvolvido o *firewall*, um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída fazendo com que todos os fluxos de dados passem por ele decidindo permitir ou bloquear tráfegos específicos de

acordo com um conjunto definido de regras de segurança (SEVERINO & ARAÚJO, 2016).

É importante salientar que o *firewall* não faz toda a segurança da rede por si só, ele é somente uma das várias ferramentas necessárias para a segurança de uma rede. Também é importante a distinção das demais soluções de segurança, como por exemplo: conexões VPN, mecanismos antivírus, *anti-spyware*, entre outros.

A segurança da informação é regulamentada pelas normas ISO/IEC 27000 e ISO/IEC 27001 que incidem em definir um desígnio para o desenvolvimento de um Sistema de Gestão e Segurança da Informação (SGSI) nas organizações, algo indispensável tendo em conta a abundância de informações produzidas ultimamente nas grandes corporações (ISO/IEC 27000, 2013).

Desta forma, será apresentada uma solução baseada em software livre, para uma empresa de médio porte, buscando solucionar alguns destes problemas citados. Será feito um estudo no Instituto Alfa LTDA ME, localizada no leste mineiro, onde o ambiente de pesquisa é a própria rede de computadores da organização. Implementou-se um ambiente protegido pelo software *PFSense*, onde foram realizados testes de funcionalidades de disponibilidade e tolerância a falhas do sistema implementado.

O objetivo deste trabalho é a pesquisa e aplicação de conceitos sobre segurança da informação, utilizando como ferramenta de firewall, a *PFSense*. Também serão seguidas algumas das diretrizes da ABNT NBR ISO/IEC 27001, que orientam o processo de acréscimo e divulgação da política de segurança. Todavia, ferramentas livres como o *PFSense* mostram-se muito eficazes quando trata-se de segurança em redes corporativas. Esse software é de código livre, licenciado sob BSD *license*, fundamentado no sistema operacional *FreeBSD* e ajustado para adotar o papel de um firewall e/ou roteador de redes, podendo ser considerado como uma ferramenta completa, pois atende com excelência empresas de qualquer porte, além de controlar toda a rede interna e filtrar todos os dados oriundos de WEB.

Com base nas informações colhidas neste ínterim objetiva-se a implantação de um servidor de *firewall* empregando-se a ferramenta *PFSense* em uma rede corporativa, e analisar os resultados provenientes de relatórios de desempenho visando concluir se essa ferramenta atende as normas presentes na ISO\27001.

2 REFERENCIAL TEÓRICO

2.1 Redes de computadores

De acordo com Gallo (2003, p.12) o conceito de Redes de Computadores pode ser definido como um anexo de computadores independentes conectados por uma única rede. Que pode ser por meio de fibra óptica, fios de cobre, satélites ou ondas de infravermelho. Surgiu com a necessidade de troca de informações possibilitando o acesso a dados que estão fisicamente longínquos. Com o progresso tecnológico passa-se a existir novas padronizações que resultara em uma melhoria na comunicação e uma diminuição em seu custo.

Gallo (2003, p. 13), além disso, cita que em qualquer panorama de redes de computadores, há três presunções subjacentes. Primeiro, uma rede precisa ser composta por membros; segundo, os membros carecem se conectar uns aos outros de alguma maneira; terceiro todos os elementos da rede devem entender visivelmente as comunicações uns dos outros para que a difusão efetiva possa ocorrer. No mundo das redes de computadores a ligação pela qual a comunicação ocorre é designada meio da rede, e as regras que conduzem a maneira pela qual as informações são trocados entre dispositivos são deliberadas por um protocolo comum para a rede.

Contudo, para distingue uma rede deve-se observar o tipo de conexão, sua topologia física e sua categorização referente ao seu tamanho. Outrora, os computadores eram vinculados em distâncias curtas, ficando conhecidas como redes locais. No entanto, com a evolução das redes de computadores, foi imprescindível aumento da distância para a troca de informações entre as pessoas. As redes podem ser rotuladas de acordo com sua disposição (*Arcnet*, *Ethernet*, DSL, *Token ring*, etc.), a expansão geográfica (LAN, PAN, MAN, WLAN, etc.), a topologia (anel, barramento, estrela, ponto-a-ponto, etc.) e o ambiente de transmissão (redes por cabo de fibra óptica, trançado, via rádio, etc.) (PINHEIRO, 2006).

2.1.1 Domain Name System (DNS)

MAFIOLETTI (2013) explanam a essência do DNS: 21 que é a criação de um diagrama hierárquico de imputação de nomes baseado no domínio e de um sistema de banco de dados difundido para implementar esse projeto de nomenclatura. Empregado para mapear nomes de hosts em endereços IP, além disso, pode servir para outros objetivos. No entanto, se não existisse o DNS, isto é, Domain Name System – sistema de nomes de domínio, para o acesso em uma página na Web, seria indispensável memorizar o endereço IP do servidor onde no qual está hospedada a página em questão.

Segundo Mafioletti & Furtado (2013, p. 38) em um conjunto de consultas, quando um servidor de títulos recebe um retorno DNS contendo, bem como, o mapeamento de um nome de hospedeiro para um endereço IP, assim realiza o cache das informações do retorno em sua memória local.

Quando se tem uma LAN com muitos computadores é aconselhável, possuir um servidor cache DNS, impedindo assim, consultas desnecessárias aos servidores DNS externos a LAN de sites frequentemente acessados.

2.1.2 Dynamic Host Configuration Protocol (DHCP)

De acordo com Severino e Araújo (p. 4-5, 2016) o DHCP trabalha da seguinte maneira o computador expede uma solicitação de *broadcast* por endereço IP na própria rede. O mesmo faz isso emprega um pacote DHCP DISCOVER. Este pacote carece alcançar o servidor DHCP.

Bem como o servidor recebe a pedido, e acrescenta um endereço IP livre e o remete ao host em um pacote DHCP OFFER. Para poder isso laborar até ainda quando os hosts não têm endereços IP, o servidor adaptar-se um host aproveitando seu endereço Ethernet (que é transportado no pacote DHCP DISCOVER).

O DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Host) é responsável por ministrar as configurações de rede como endereço 22 IP, máscara de subrede, endereço do *gateway*, endereço dos servidores DNS, em meio a outras configurações para os aparelhamentos que se acoplarem a rede.

As configurações de rede podem ser conseguidas manualmente em todo equipamento conectado à rede. Em redes menores, isto se torna fácil de ser feito,

mas em redes maiores resulta uma tarefa muito adversa e sujeita a falhas (FERREIRA, 2008, p. 459).

2.1.3 Redes Locais Sem Fio (WLAN)

Da Silveira (2003) explica que as WLANs estão cada vez mais populares em casas e prédios de escritórios. De regra cada computador há um rádio modem com uma antena, que comunica-se com um AP. O padrão de LAN sem fio é chamado de 802.11, popularmente conhecido como Wi-Fi, isto é, ponto de acesso *ap switch* rede cabeada.

Os padrões 802.11 mais empregados nos equipamentos sem fio consistir em: 802.11b, 802.11a, 802.11g e 802.11n. As diversificações entre eles são necessariamente a faixa de 23 frequências e a velocidade máxima.

2.1.4 LANs Virtuais (VLANs)

As VLANs (LANs virtuais) admite-se que a rede local física possa ser dividida em redes locais virtuais incluso de um mesmo switch.

De acordo com Da Silveira (2003) as VLANs apareceram com o objetivo de definir algumas dificuldades: Carência de isolamento do tráfego: com o uso de VLANs, torna-se admissível limitar o tráfego de broadcast (por exemplo, gráficos carregando mensagens DHCP) na rede, desta forma, além de aprimorar o desempenho da LAN, aperfeiçoaria questões de privacidade e segurança. Por exemplo, em uma universidade, alunos poderiam empregar um software analisador de embustes para capturar dados trafegados nos departamentos administrativos da instituição.

O modo ineficiente de switches: por exemplo, para decompor em três grupos uma LAN com 20 computadores, acoplados a um switch sem suporte a VLANs, seriam indispensáveis três switches. Gerenciamento de usuários: por padrão, em uma LAN, repartida em grupos que usando switches sem suporte a VLANs, caso um empregado mude de grupo, seria indispensável alterar o cabo de rede de switch. Dificuldade que não existiria em switches com VLANs, porquanto, seria necessário

unicamente alterar as configurações nos softwares de gerenciamento das VLANs. 24

As fundamentais implementações de VLAN são: VLAN embasadas em porta, a qual atua em switches da categoria 2 do modelo OSI e VLAN baseada em IP, empregando a categoria 3 do modelo OSI (FERREIRA, 2008, p.656).

2.1.5 Remote Authentication Dial In User Service (RADIUS)

O RADIUS (*Remote Authentication Dial In User Service*) é um protocolo para confirmação, habitualmente utilizado em provedores de Internet juntamente a redes sem fio. É um protocolo acertado na [RFC2865], deliberado como sendo constituindo e desenvolvido para a efetivação de autenticação, licença e encaminhamento de informações de configuração em meio a uma rede de acesso partilhada, que deseja autenticar as suas ligações, e um servidor de autenticação(FERREIRA, 2008, p.656).

2.1.6 Gerenciamento de redes

Pinheiro (2006) também afirma que o gerenciamento de rede pode ser conceituado, bem como o controle de atividades e monitoração de uso de recursos materiais como modems, roteadores, entre outros e protocolos, fisicamente disseminados na rede, tendo, na medida do possível a credibilidade, tempos de resposta asiláveis e segurança das informações. O modelo costumeiro de gerenciamento pode ser definido em três etapas:

a) Coleta de dados: uma técnica, em geral automática, que incide de monitoração sobre os recursos gerenciados;

b) Diagnóstico: visa na alimentação e análise realizadas a partir dos dados colhidos. O computador de gerenciamento adimple uma série de processos, seja por intermédio de um operador ou não, no intuito de gerar a causa do problema simulado no recurso gerenciado;

c) Ação ou controle: Uma vez diagnosticado a dificuldade, cabe uma ação, ou comando, sobre o recurso, caso o episódio não tenha sido passageiro, ou seja, incidente operacional.

Além disso, um sistema de gerência de rede pode ser visto como um conjunto de ferramentas agregadas para o monitoramento e domínio, que proporciona uma interface única e que apresenta informações sobre o status da mesma, pode-se oferecer até um conjunto de comandos que propende-se executar todas as atividades de gerenciamento sobre o sistema em questão.

A disposição geral dos sistemas apresenta quatro elementos básicos: os elementos gerenciados, as estações de gerência, os protocolos de gerenciamento e as informações de gerência. Os dados gerenciados são dotados de um software apontado como agente, que permite a vigilância e o controle do equipamento por meio de uma ou mais estações de gerência. Do mesmo modo, qualquer dispositivo de rede como, por exemplo, impressoras, roteadores, repetidores, switches entre outros pode ter um agente instalado (GALLO, 2003).

O sistema de gerenciamento é conectado e mesclado por um conjunto de instrumentos que monitora e controla o funcionamento. Um número mínimo de equipamentos separados é necessário, sendo que a maior parte das informações de hardware e software para controle está coligada aos equipamentos já existentes. Uma rede sem estruturas de gerência pode exibir problemas que irão afetar o tráfego de informações, bem como sua probidade, como dificuldades de congestionamento do tráfego, recursos mal usados, sobrecarregados, com problemas de segurança entre outros (PINHEIRO, 2006).

2.1.7 Segurança de redes

Anteriormente, boa parte dos acessos a Internet eram realizada por meio de conexão discada com baixas velocidades que ficavam por parte dos 56 Kbps. O usuário com um modem e uma linha telefônica, conectava-se ao provedor e mantemos esta vinculação apenas pelo tempo necessário para concretizar as ações que dependessem da rede. Entretanto, com os grandes avanços incidiram as novas alternativas, sendo que recentemente grandes partes dos computadores pessoais permanecem conectados à rede pelo tempo indeterminado e a velocidades que pode chegar até 100 Mbps1. Conexão à Internet também passou a ser possível a grande quantidade de equipamentos com acesso à rede, assim como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio. (PUGLIESE & LOVISI, 2015).

Deste modo, ao conectar-se à rede os usuários estão a sujeito a ameaças, como furto de dados e por meio da exploração de vulnerabilidades, o computador ou dispositivo móvel, pode ser infectado ou invadido, sem que o usuário saiba. Assim, ser vítima de ataques, ter dados indevidamente recolhidos e ser usado para o alastramento de códigos maliciosos. Ao mesmo tempo, aparelhamentos de rede como modems e roteadores vulneráveis novamente podem ser invadidos, terem as configurações modificadas ou fazerem com que as conexões sejam desviadas para sites fraudulentos.

Visto a grande quantidade de roubos de informações, este delito é precedido por na Lei Nº 12.737, de 30 de Novembro De 2012 que diz em seu texto.

> [...]Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> “Invasão de dispositivo informático [...]
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...]. (BRASIL, 2012).

Sendo assim como descrito em lei, é imprescindível que os órgãos e as empresas que utilizam da troca de dados procurem por maneiras diligentes de proteger seus dados. Tornando imperativa a criação de uma política de segurança de informações, isto é, um documento contendo normas que administrem a gestão de segurança de informações. Este documento deve mostrar o que deve ser feito pela empresa para afiançar os recursos computacionais e os dados (PUGLIESE & LOVISI, 2015).

2.2 Segurança da informação

Segurança da informação compreende um conjunto de medidas que visam proteger, preservar informações e sistemas de informações, assegurando integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade em sistemas de informações (MAFIOLETTI, 2013).

Nesse sentido, esses pilares, juntamente com mecanismos de proteção tem por objetivo prover suporte a restauração de sistemas informações, adicionando-lhes capacidades detecção, reação e proteção. Os componentes criptográficos da segurança da informação tratam da confidencialidade, integridade, não repúdio e autenticidade (PUGLIESE & LOVISI, 2015).

O estabelecimento de um Programa de Segurança da Informação em sua empresa deve passar sempre por ações que norteiam esses princípios. Tal modelo deve estar amparado por um Sistema de Gestão de Segurança da Informação que precisa ser planejado e organizado, implementado, mantido e monitorado (MAFIOLETTI, 2013).

2.3 Firewall

O nome de firewall começou a ser empregado no final da década de 80, quando unicamente roteadores separavam pequenas redes corporativas. Desta forma, as redes poderiam instalar seus aplicativos da forma como lhes fosse adequada sem que as demais redes fossem prejudicadas por lentidão. Firewall é um recurso de segurança fundamentada em hardware ou software, que a partir de um conjunto de regras ou instruções, avalia o tráfego da rede para distinguir operações válidas ou inválidas dentro de uma rede corporativa. Um firewall analisa o tráfego de rede entre a internet e a rede privada ou entre redes privadas (SEVERINO & ARAÚJO, 2016).

Dentre os vários modelos de firewall, os três principais tipos são:

2.3.1 Firewall em nível de pacote

O filtro de pacotes tem como desígnio permitir ou não a passagem de pacotes pela rede fundamentando-se em regras pré-definidas. Normalmente estes estão estabelecidos em roteadores, simulando o ponto de acesso dentre duas redes, admite-se que serviços controla o tráfego, sustentando-se a rede protegida.

Este é o *firewall* mais praticado atualmente, uma vez que é a proteção básica da rede, ao aceitar portas de comunicação danosas abertas e permitir o tráfego livre de pacotes, a rede fica apta a ataques (SEVERINO & ARAÚJO, 2016).

2.3.2 Serviços Proxy

Os servidores de serviço *proxy* são particularizados em aproveitamentos ou programas servidores que executa-se um *firewall*. Os mesmos pegam a solicitação e exigência dos usuários para o serviço da internet, examina-se as solicitações serão acatadas dentro do anexo de regras preestabelecidas e logo passam ou não a solicitação adiante para o serviço característico solicitado.

Estes servidores estão entre o usuário da rede interna e a internet que atuam bem como o próprio nome diz, isto é, um mediador. É corriqueiro utilizarem transparência nesses servidores, desta forma, ele fica transparente para o usuário, sendo sutil, porém atuando assim como filtro de pacotes (SEVERINO & ARAÚJO, 2016).

2.3.3 Circuit-Level Gateway

Este tipo de *firewall* cria um cabeamento entre o cliente e o servidor e não decodifica o protocolo de aplicação. Opera monitorando-se o *handshaking*, ou seja, a permuta de informações ao estabelecimento de comunicação, entre pacotes, objetivando definir se a sessão é autêntica.

A principal finalidade de um *firewall* é arranjar com que todos os dados trafegados entre as duas redes diferentes incidam sobre ele. Para que isso ocorra, é necessário que tenha um estudo sobre a arquitetura da rede que se almeja proteger (SEVERINO & ARAÚJO, 2016).

Atualmente com a segurança das informações vem tornando indispensável para empresas que estão constantemente fazendo troca da mesma, entretanto, ofensivas que antes apresentavam apenas a finalidade de realizar a autoafirmação de *hackers*, atualmente mostram-se perigosos e prejudiciais as empresas que não possuem proteção adequada (ARAÚJO, 2015).

Invasões em sistemas internos de empresas há muito tempo preocupam os profissionais da área de segurança da informação, porém, ataques que antes tinham muitas vezes somente a intenção de realizar a autoafirmação de *hackers*, hoje se mostram muito mais perigosos e danosos as empresas que não utilizam de uma proteção adequada (ZIENTARA, 2016)

No mercado de tecnologia de informação as ferramentas criadas deve atender as exigências implicada na ISO\27001 e satisfazer as ordens da ABNT. A ferramenta *PFSense* que possui propriedades de um firewall e/ou roteador de redes baixo custo, e hoje em dia a empresa a qual será implantado o sistema já possuir tal ferramenta, porém, em desuso, o presente projeto aspira aplicar, correlacionar e avaliar tal ferramenta. Apesar que o firewall não é o único elemento de segurança em uma rede, no entanto é crucial, pois realiza a segurança do perímetro da rede (ASGHARI, 2015).

Com o enriquecimento nos sistemas de comunicações, o acesso a informação está a cada dia mais democrático e genérico, e a *internet* tem papel essencial na evolução do mercado corporativo atual. Com esse amplo acesso a informações, tornou-se essencial o desenvolvimento de ferramentas com a aptidão de prover a segurança das informações trafegadas pela rede. Esses *softwares* são responsáveis por uma série de capacidades, como por exemplo, o domínio de acessos para evitar acessos nocivos ou não autorizados às informações (MAROCCO, 2016).

O regulamento que rege a segurança da informação são as normas ISO/IEC 27000 e ISO/IEC 27001 que incidem em definir um propósito para o desenvolvimento de um Sistema de Gestão e Segurança da Informação (SGSI) nas organizações, algo indispensável tendo em conta a abundância de informação produzida recentemente nas grandes corporações (ISO/IEC 27000, 2013).

O movimento de *software* livre trata-se de um movimento com embasamento no princípio do compartilhamento da informação e na solidariedade praticada pela inteligência coletiva integrada na rede mundial de computadores. A partir da

indignação de um integrante do MIT, Richard Stallman, contra o impedimento de se acessar o código fonte de um software, em 1985 foi criada a *Free Software Foundation*. O movimento de *software* livre começou pequeno que reunia e difundia programas e ferramentas livres, com o código-fonte aberto. Deste modo, todas as pessoas pode-se ter acesso não somente aos programas ao mesmo tempo aos códigos em que foram escritos. A ideia era produzir um sistema operacional livre que apresentasse a lógica do sistema Unix que era proprietário, ou seja, pertencente a uma empresa. Por isso, os vários esforços de programação eram reunidos em torno do nome GNU (Gnu Is Not Unix) (DA SILVEIRA, 2003, p. 438).

Infraestrutura de rede consiste na disposição do cabeamento que suporta qualquer equipamento relacionado a comunicação de dados/voz. Todos os sistemas finais que possuem algum meio de transporte de informação que conduzam informação através de algum meio físico é considerado infraestrutura de rede.

2.4 PFSense

O *PfSense* é uma ferramenta que faz a conexão de várias instrumentos que fazem parte de uma área da rede e sua segurança. Logo após, instalado sua manipulação é feita por meio de browsers acessando o endereço recebido da rede.

> [...] O *pfSense* é um *software* livre trabalhado para distribuição do *FreeBSD*, estando adaptado para uso de *firewall* e roteador, que é inteiramente gerenciado via interface WEB. Um poderoso *firewall*, ao mesmo tempo é uma plataforma de roteamento, o mesmo possui uma vasta lista de recursos que podem ser adicionadas através de *downloads* de pacotes admitindo assim a adição de funcionalidades de acordo com a necessidade do usuário. O projeto do *pfSense* principiou-se em 2004 distinguindo-se de outro projeto o *m0n0wall*, por ser um projeto para ser instalado completamente em um computador [...] (PFSENSE, 2013. p.1).

Esta ferramenta é um Sistema Operacional fundamentado no *FreeBSD*, que deriva do *UNIX*. O *PfSense* é uma compilação que traz vários serviços consigo. Como por exemplo, o *firewall, proxy*, domínio de acessos de usuários entre outras funcionalidades. O uso dele promove o gerenciamento e a segurança de rede, tanto pelo fio quanto como a rede wireless (ASGHARI, 2015).

Para a utilização de todos os seus recursos se faz necessário o aprofundamento no conhecimento desse sistema operacional e de alguns dos seus serviços e suas finalidades. A possibilidade de fazer configurações através da

interface web facilita muito as aplicações do gerente de rede. Por ser uma ferramenta *open Source*, gratuita é uma alternativa bem interessante para pequenas empresas, instituições de ensino ou no caso do CA de Sistema de Informação (ZIENTARA, 2016).

Além das funções citadas acima, ela auxilia na gerência na parte de controle de usuários, onde se pode limitar banda de rede, criar grupos distintos com gerência diferenciada.

2.4.1 Histórico e uma leitura inicial do PfSense

Como descrito Severino (2011), o *PfSense* é um *software* com a licença na base do BSD license. Embasando-se no sistema operacional *FreeBSD*, foi aperfeiçoado para que trabalhasse bem como uma ferramenta de firewall e/ou roteador para em redes.

Hoje a ferramenta vem com diversas tecnologias introduzidas, do mesmo modo, tornando um instrumento mais eficiente. O projeto iniciou por volta do ano de 2004, por Chris Buechler e Ullrich Scott. Auxiliado por diversos códigos durante um grande período de tempo, no projeto *monowall*, que por sinal é bastante semelhante ao *PfSense*, contudo com foco em dispositivos que pudessem rodar diretamente em memória principal, desta forma, muitos papéis ficaram a desejar, assim Chris juntou forças com Ullrich e iniciaram então o projeto (SEVERINO & ARAÚJO, 2016).

2.4.2 O FreeBSD

A licença da ferramenta prevê dois principais pontos, a de copiar código e dizer onde foi sua criação, assim como não o culpar-se por erros que venha ocorrer. Neste sentido:

> [...] Em síntese, FreeBSD é um sistema operacional UN*X-like para plataformas i386 e Alpha/AXP, baseado no “4.4BSD-Lite” da Universidade da Califórnia em Berkeley, com alguns aprimoramentos adotados do “4.4BSDLite2”. Baseado, indiretamente, na conversão de William Jolitz conhecida como “386BSD” para a plataforma i386 do “Net/2” da Universidade da Califórnia, em Berkeley; apesar de que pouquíssimo código originado do 386BSD ainda exista no FreeBSD.”[...] (FREEBSD, 2012).

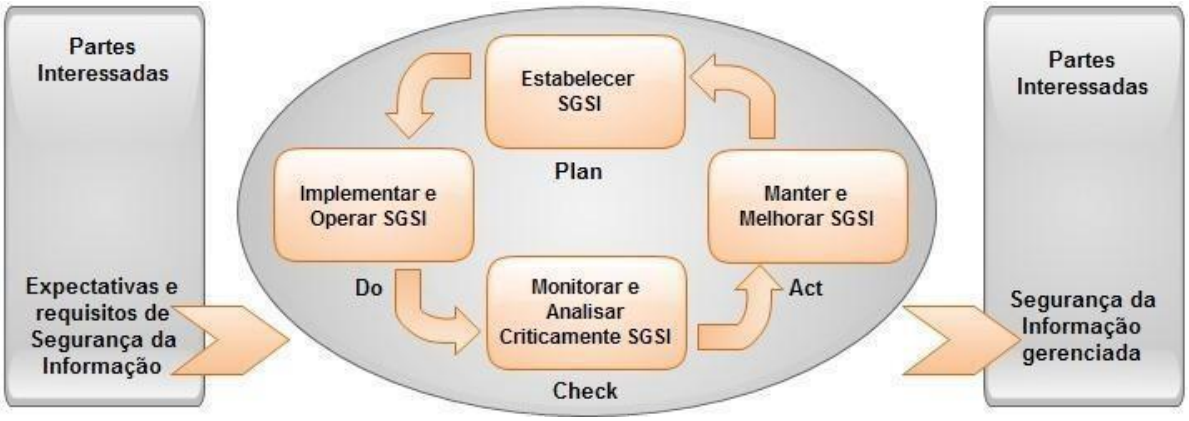
A ferramenta pode ser utilizada de forma habitual, de uso pessoal, e-mail, acesso a rede, editores de textos, etc. Além disso, serve para uso técnico e como servidores.

2.5 ABNT NBR ISO/IEC 27001

A ABNT NBR ISO/IEC 27001, ou seja, os Sistemas de gestão de segurança da informação – Requisitos, especifica-se as condições para um Sistema de Gestão de Segurança da Informação (SGSI). No qual, é um sistema de administração desenvolvido para a segurança da informação de organizações, fundamentado em uma abordagem de riscos do negócio (ABNT, 2006).

A norma indica a adoção de uma abordagem de método para um SGSI, visto que a organização deve apontar e gerenciar os processos abrangidos em um SGSI, bem como distinguir suas interações. Ao mesmo tempo, a ABNT NBR ISO/IEC 27001 ainda adota o ciclo denominado PDCA (Plan, Do, Check, Act) para embasar todos os procedimentos envolvidos em um SGSI. O PDCA é uma ferramenta gerencial que permite a melhoria contínua de métodos e a solução de problemas demonstrado no organograma 1 (ABNT, 2006).

Organograma 1 - Ciclo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação



Fonte: Profissionais TI (2010)

Como demonstrado na figura a ABNT NBR ISO/IEC 27001 está coligada as normas ABNT NBR ISO 9001:2000 e a ABNT NBR ISO 14001:2004, de forma sistemática a consentir que seja combinada com outros sistemas de gestão.

> [...] Qualquer exclusão de controles considerada necessária para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles forem excluídos, reivindicações de conformidade a esta Norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis [...] (ABNT, 2006, p. 2).

A ABNT (2006) ainda especifica que a mesma NBR ISO/IEC 27001 apresenta-se como escopo especificar requisitos para a organização como a configuração, a operação, a monitoração, o diagnóstico crítico, a conservação e o melhoramento de um SGSI. Os pré-requisitos são gerais de maneira a consentir que sejam aproveitáveis a quaisquer organizações, involuntariamente do tipo, tamanho e natureza.

3 METODOLOGIA

O presente estudo foi realizado no Instituto Alfa LTDA ME da região de Caratinga-MG, onde ainda não havia sido aplicado uma metodologia de segurança da informação, sendo de grande valia a realização deste trabalho. As metodologias e ferramentas utilizadas poderão ser aplicadas em outras empresas que possuem uma estrutura de rede de computadores similar a esquema que será apresentado.

A ABNT NBR ISO/IEC 27001 fornece recomendações que auxiliam no desenvolvimento da política de segura. A norma foi publicada pelo ISO e IEC em 2005, sendo voltada para especificar os requisitos que vão estabelecer, implementar, operacionalizar, monitorar, revisar e manter a melhoria contínua do Sistema de Gestão de Segurança da Informação.

A instituição Alfa encontra-se em Caratinga desde 2012, com uma proposta de vender e administrar plataformas online, de modo a oferecer cursos de especialização modo Lato senso. Atualmente a empresa possui um total de 90 funcionários, no quais são divididos em setores. Estes são eles: Marketing, Marketing

Mídia, Recursos Humanos, Tecnologia da Informação, Central de Relacionamento, Financeiro, Pedagógico, Secretaria, Sac. e Pós venda.

O Instituto Alfa LTDA ME ainda não havia investido em uma padronização do seu ambiente de rede de computadores para manter o desempenho e a segurança dos dados. Com a análise do ambiente de redes da empresa destacou-se os pontos decisivos para promover a segurança da informação. Assim, foi possível a criação de uma política de segurança para eliminação das ameaças aos documentos.

Logo, tornou-se imprescindível um estudo sobre Redes de Computadores e Gerência de Segurança, Segurança da Informação, a ferramenta *PFsense* e norma estabelecida pela ABNT NBR ISO/IEC 27001.

Mais adiante, foi a analisado os processos internos da empresa com a finalidade de conhecer compreender o papel de cada setor, as regras do negócio e os tipos de dados manuseados por cada usuário.

A rede de computadores do mesmo modo foi analisada com a intenção de destacar as vulnerabilidades que posteriormente seriam tratadas. Os pontos considerados foram servidores, desempenho no compartilhamento de dados, *Switches*, roteadores e o uso da internet.

Em seguida, após todo o levantamento de dados realizado na empresa, executou-se as mudanças necessárias na rede de computadores com o intuito de eliminar as vulnerabilidades encontradas.

3.1 Ambiente de Estudo

Como a maior parte das empresas, o Instituto Alfa LTDA ME depende da sua rede de computadores e da internet para desempenhar suas atividades mais importantes. Com o levantamento realizado, obteve-se uma boa visão dos processos da empresa.

Primeiramente analisou-se toda a estrutura de equipamentos da rede de computadores demonstrado no organograma 2, no ambiente de estudado, onde foi revisto a necessidade de executar alterações buscando a melhoria. Após a análise, constou-se que alguns equipamentos da rede como *Switches* e roteadores não estavam atingindo usabilidade aceitável, com relação à taxa de transferência, desempenho e segurança. Estes equipamentos que trabalhavam com taxas de

transferência 10/100 Mbps, acarretando falhas em momentos de maior utilização no ambiente empresarial deixando fluxo de informação mais lento.

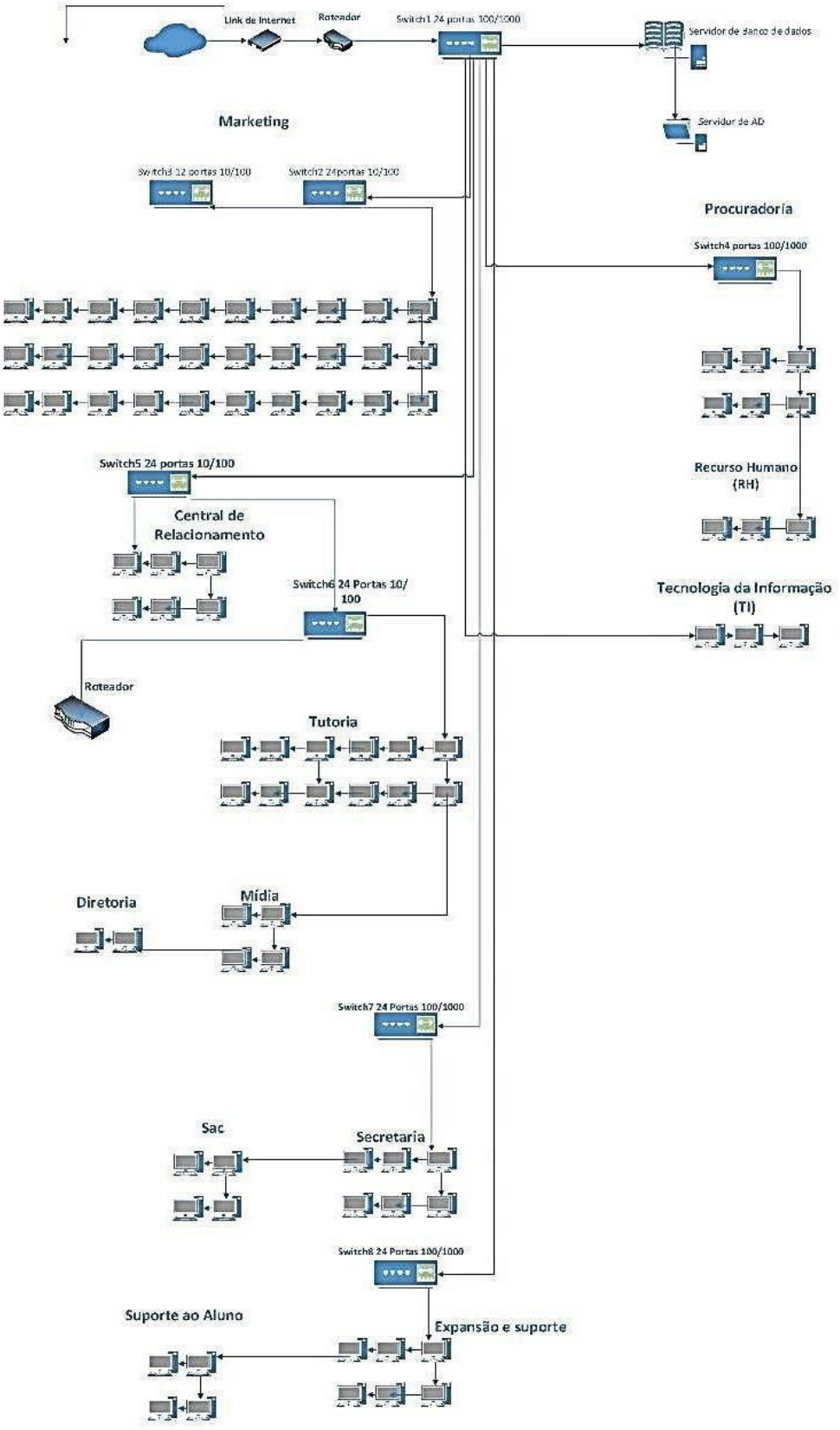
A rede de computadores demonstrado no organograma 2 possui um servidor de banco de dados SQL Server e servidor *active directory windows* server 2012 rodando no sistema operacional *Windows Server* 2012 *Standard*. Antes da política de segurança, no entanto, os dados não eram protegidos por um servidor de Firewall. A rede possuía somente um link de internet ADSL com velocidade de 30 Mbps. Logo após o modem ADSL, está um roteador convencional para compartilhamento da internet.

A rede wireless era utilizada pelos notebooks e celulares dos líderes do Instituto Alfa LTDA ME, porém não eram cogitados em se tratar da segurança da rede sem fio. O roteador trabalhava com mesma faixa de IP da rede interna, sendo assim, quem tivesse acesso ao roteador teria acesso a rede interna da mesma.

Não obstante, a rede wireless da empresa foi inteiramente reestruturada. Com a adicão de novos roteadores de perfil empresarial, com a utilização de senhas fortes e filtragem por MAC.

Já na estrutura física retiraram-se todos os *Switches* 10/100 e substitui-se por *switch* 100/1000, tornando os padronizados. Igualmente foi adquirido 1 *Switches* 100/1000 reserva para uma substituição rápida caso necessário.

Organograma 2 - Desenho da rede de computadores antes da política de segurança



Fonte: Próprio autor

3.2 Imagem da Rede

A configuração de um *Firewall* torna-se um ponto eficaz no presente trabalho, pois a ferramenta *Pfsense* permite a configuração para sua utilização como um *firewall*, possibilita-se o bloqueio do acesso às portas de conexão de ambiente de trabalho. O *PFSense* é um *software* livre, licenciado sob BSD *license*, baseando-se no sistema operacional *FreeBSD* supracitado, que adaptado para assumir o papel de um *firewall*. Permitindo a configuração de vários tipos de serviços como: servidor de *Firewall, VPN, Wireless* AP/cliente, *Proxy* e entre outros.

Para a liberação das portas no *Firewall* foi empregada o redirecionamento para o equipamento ou serviço interno exclusivo, esse ato aumentou o nível de segurança, porquanto que a porta de conexão em questão, não vai estar aberta para todos os dispositivos da rede. O acesso a conteúdo na internet foi restrito a assuntos exclusivos e controlados pelas regras definidas no *Proxy*.

O mesmo trabalha do seguinte formato: as requisições de conexão na internet do roteador são direcionadas para a porta definida no *Proxy*, onde é controlada qual a máquina vai ter acesso liberado ao conteúdo da internet e qual vai ter acesso limitado.

3.3 Realizações das Modificações

Analisando as necessidades da empresa, notou-se a inópia de contratar outros links de internet, pois caso um dos links fique inacessível a possibilidade do outro link assumir de imediato. A diretoria foi informada do fato ocorrido e logo fez-se a contratação da mesma. Deste modo, foi contratado um provedor de internet a cabo de 20 Mbps dedicados, assim atende perfeitamente às necessidades da organização.

Contudo, na parte física da rede não houve quaisquer alterações. Os servidores já se encontravam em uma sala de fácil acesso e também já possuíam um ar-condicionado para climatizar o ambiente, tendo assim lugar adequado para os equipamentos.

No controle de falhas nos pontos mais cruciais da rede, foram substituídos quatros Switches. Dois dos Switches com velocidade de transferência 10/100 Mbps ficando posicionado no departamento de Marketing. Para garantir o desempenho nas transferências dos dados e a segurança, foi adquirido um novo Tp-link 24 portas com taxas de transferência 100/1000 Mbps, substituindo o antigo equipamento. E outros dois Switch de 24 portas com taxas de transferência 10/100 Mbps, que permaneciam nos setor Central de Relacionamento e no Pedagógico, não obstante, houve-se a necessidade de substituição deste Switch para padronizar a rede.

3.3.1 Política de Backup

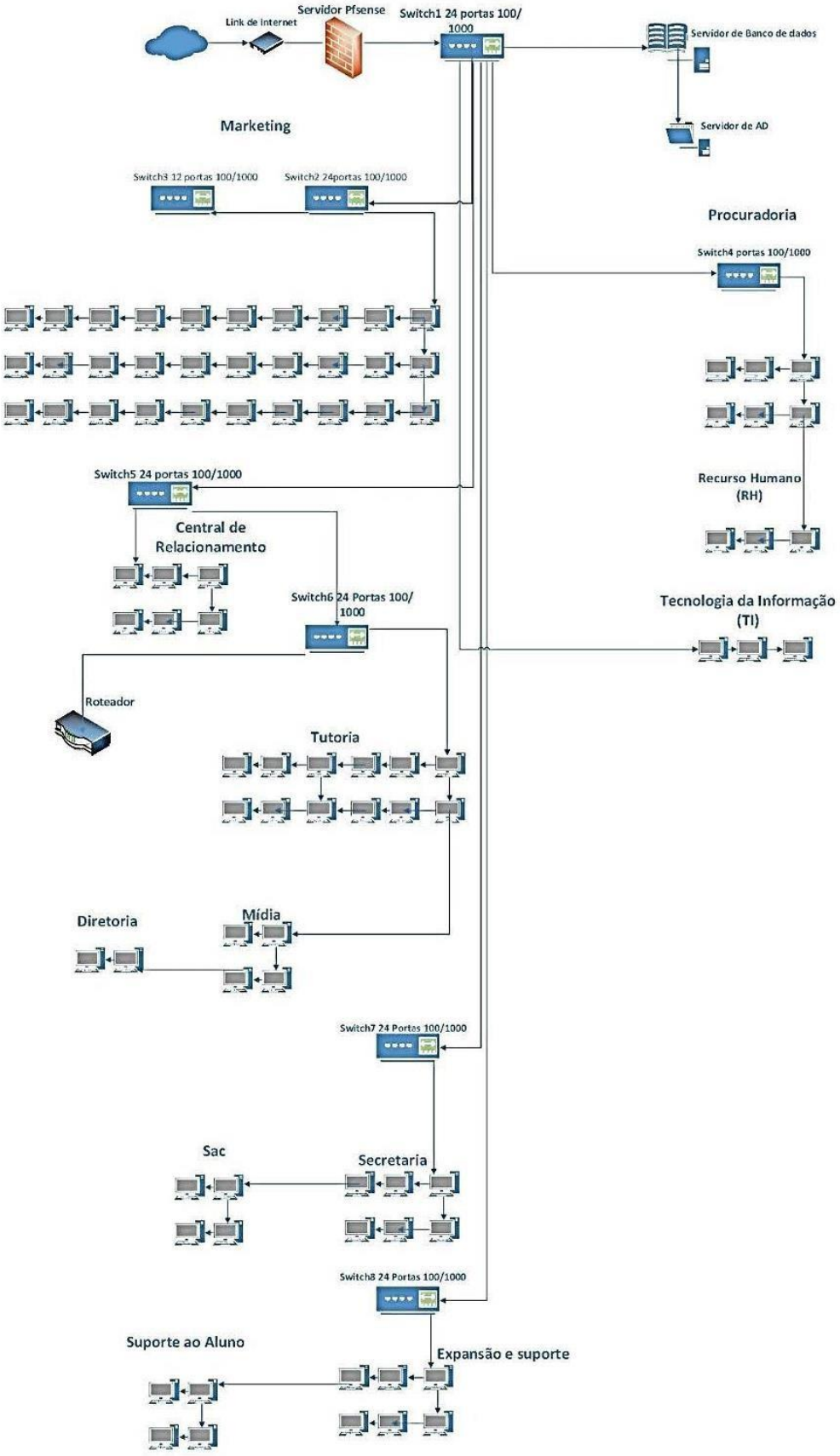
Determina a configuração do backup do Windows, onde são salvos os arquivos dos usuários juntamente com uma imagem do sistema operacional. Neste local os arquivos são copiados todos os dias em um local de rede externo para assim garantir a segurança dos backups.

3.3.2 Prevenção contra queda de Eletricidade.

Já em relação a proteção contra riscos por faltas de energia elétrica, os servidores estão ligados em um nobreak 1300va Mono net Winner- com autonomia de até 80 minutos. A cópia de segurança dos backups do servidor é realizada pela a

rede três vezes ao dia 10 horas da manhã, 15 horas da tarde e com o último realizado às 21 horas da noite.

Organograma 3 - Rede de computadores após as mudanças.



Fonte: Próprio autor

Observa-se no organograma 3 da rede, o roteador com conexão wireless manteve-se no mesmo local, os switches foram padronizados e o servidor *PFsense* foi implantado.

3.4 Segurança na Rede Sem Fio.

O sinal da rede sem fio continuou sendo usado normalmente, mas com algumas melhorias, pois toda a rede wireless agora possui senha segura, com modo de segurança WPA2 Personal. Outra configuração de segurança importante que foi executada é a associação dos endereços MAC dos dispositivos nos roteadores, assim somente serão aceitas conexões de dispositivos com o MAC informado no filtro do roteador.

O filtro de endereços MAC é de grande importância pois nele estão definidos para recusar a conexão de aparelhos que não estão informados na regra. Com isso, esta configuração aprimorou muito a segurança, pois mesmo tendo conhecimento da senha do sinal wireless, o usuário não conseguirá conectar outros aparelhos que não tenham o seu MAC confirmado na lista do roteador

3.5 Configuração do Servidor Pfsense Como Firewall

O ponto chave para a segurança da rede de computadores do Instituto Alfa LTDA ME foi à inclusão do servidor *pfsense*, gerenciando todo o tráfego na rede. Em seguida, serão apresentados os procedimentos realizados durante a configuração Firewall.

3.5.1 Requisito mínimo para instalação da ferramenta.

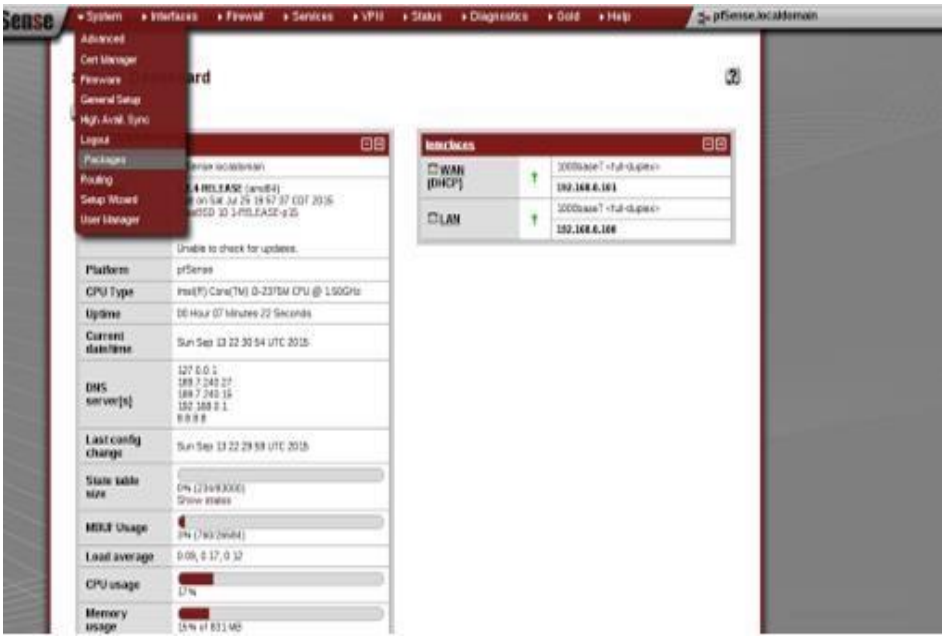
Deve-se realizar o download da ISO que se encontra no link a seguir. https://www.pfsense.org. Aconselha-se utilização de um servidor com pelo ao menos 1.5 GHZ de processador e 512 de Ram. Necessita-se usar no mínimo duas placas de rede.

3.5.2 Instalando os pacotes do Squid e SquidGuard e configuração o proxy transparente

A instalação e configuração do *Squid* e *SquidGuarde* são imprescindível para o bloqueio dos acessos internos e externos. Apesar de existir outros tipos *proxy*, no presente trabalho utilizou-se o proxy transparente levando-se em consideração que a mesma atende perfeitamente a necessidades da impressa.

No menu "*System*", seleciona-se "*Packages"* na figura 1:

Figura 1 - Menu System



Fonte: Próprio do autor

Na Available *Packages*, busca por *Squid* e *SquidGuard* entre os pacotes e em seguida instalá-se como módulos no *pfSense*.na figura 2 e 3:

Figura 2 - Busca por Squid e SquidGuard

squid	Network	Stable platform: 2.2 2.2.999	High performance web proxy cache. No package info, check the forum
squid3	Network	beta 0.3.2 platform: 2.2	High performance web proxy cacl It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package info
squidGuard	Network Management	Beta platform: 2.2	High performance web proxy URL filter. Works with both Squid 2.x and No package info, check the forum

Fonte: Próprio do autor

3.6 Configurando o Proxy Server

3.6.1 Configurações Gerais

Em Services→ *Proxy* Server e na aba "*General*" marque-se a opção "*Transparent proxy*" e "*Allow users on interface*" e deixando a interface do *Proxy* configurada para a placa de rede interna na figura 3:

Figura 3 **-** Configuração da interface

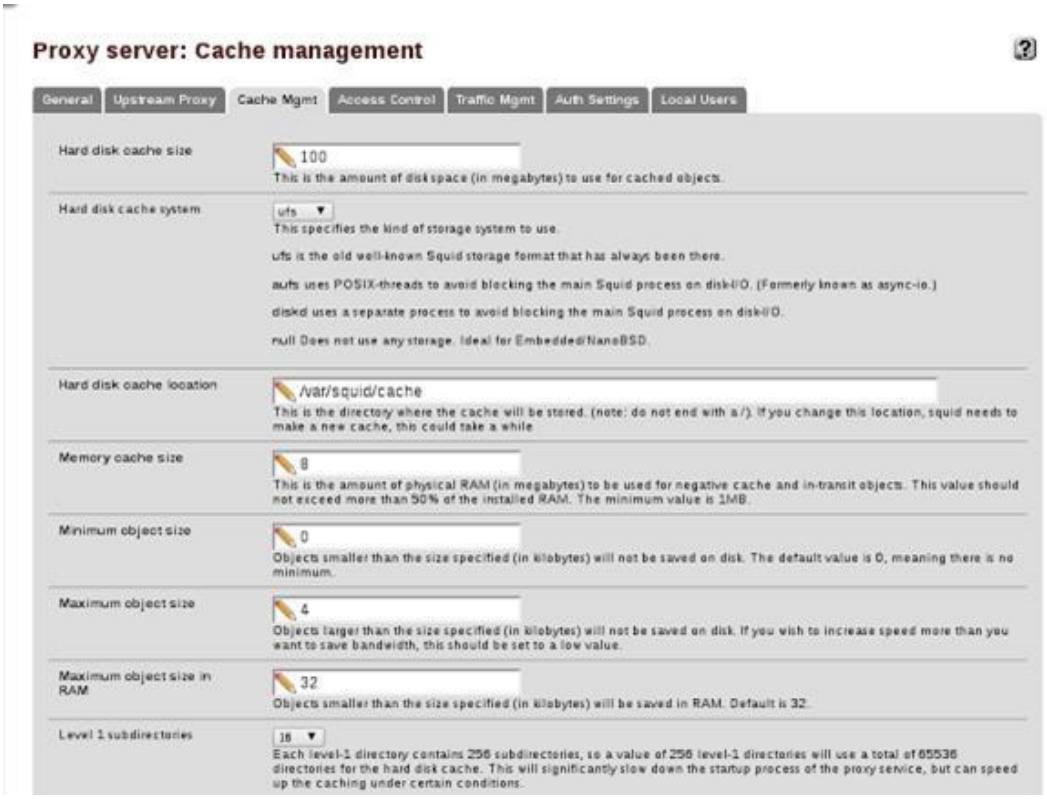
Fonte: Próprio do autor

No campo "*Bypass proxy for these source IPs*" coloca-se os IPs da rede que não passará pelo *Proxy*.

3.6.2 Configurando o Cache de Disco

No campo *Cache Mgmt* irá configurar o cache do sistema de *Proxy* na figura 4:

Figura 4 **-** Configuração do cache do sistema



Fonte: Próprio do autor

Hard Disk Cache: Irá decidir o tamanho do cache que será guardado no disco.

Hard Disk Cache System: Local onde são guardados os arquivos de cache. Deixe o mesmo no diretório /var/squid/cache por Default.

Memory Cache Size: Define o tamanho de memória do sistema para colocar os arquivos cacheados.

Minimum Object Size: Define o volume mínimo dos arquivos armazenados em cache. Deve-se deixar em 0 por Default.

Maximum Object Size: Permanece a dimensão máximo de arquivos guardados em cache.

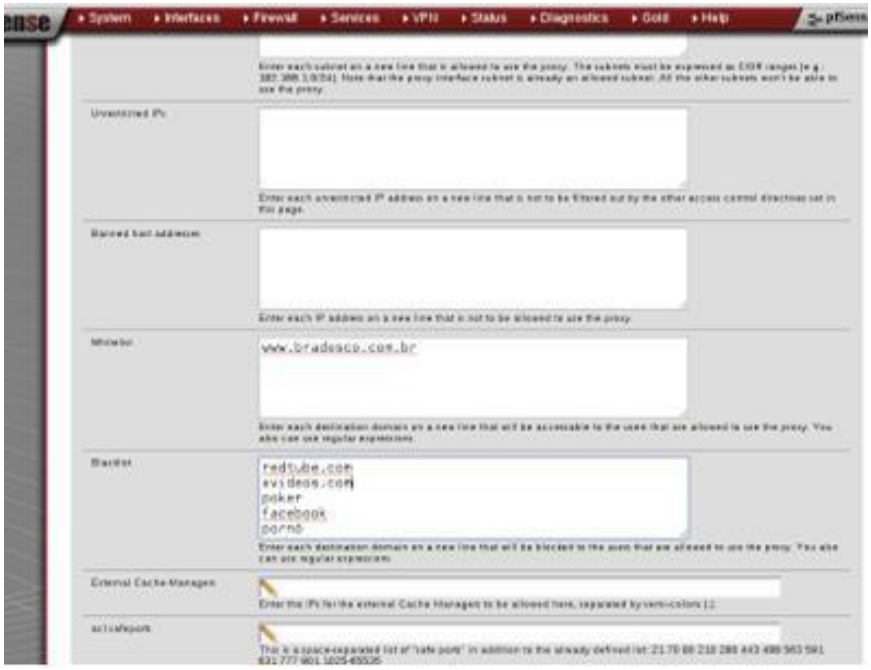
Maximum Object Size in RAM: Define a quantidade máxima de objetos guardados dentro da memória Ram do servidor.

Do Not Cache: Deverá preencher quais serão os domínios, IP’s que não serão cacheados pelo o servidor. Ex: www.posgraduacaoalfa.com.br.

3.6.3 Controlando o acesso de usuário.

Na figura 5 no campo *Acess Control* irá decidir algumas configurações referentes à rede e aos filtros.

Figura 5 **-** Configuração dos filtros



Fonte: Próprio do autor

Allowed subnets: Local para definir as sub redes em que o *Proxy* vai se aplicar.

Whitelist: Define os sites que deverão passar livres pelo *Squid*.

Blacklist: Define os sites e termos que deverão ser bloqueados imediatamente pelo *Squid*. Logo, basta, salvar as configurações.

4 RESULTADOS

4.1 Análise do Ambiente de Estudo.

Mediante este ambiente de insegurança onde os dados estão inseridos e fluem nos sistemas e redes de computadores, muitas empresas adotam políticas de segurança, que são conjuntos de regras, leis e práticas de gestão visando à

proteção. De acordo com ABNT (2006) “Promover...” O instituto Alfa LTDA ME, com propensão de obedecer às regras descrito na ISO foi criado uma normativa para os funcionários que estão cientes dos riscos do má utilização da rede.

O Instituto Alfa LTDA ME antes da implantação da ferramenta e a criação da Política de Segurança não seguiam as normas determinadas pela ISO/27001 ABNT (2006) o que acarretava em um sistema falho e que ocasionava em uma rede corporativa sem proteção adequada, pois todos usuários tinha livre acesso podendo acessar tudo o que desejavam, como por exemplo rede sociais, site de compras, entre outros. E sem o conhecimento necessário ficando exposta a insegurança dos dados coletados dos clientes.

4.2 Análise do pfSense de acordo com as normas estabelecidas pela Iso/27001

A ABNT na ISO no tópico A.6 diz que:

> [...] A.6.1.1: A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação. [...] A.6.1.2: As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes. [...] A.6.1.3: Todas as responsabilidades pela segurança da informação devem estar claramente definidas. [...] A.6.1.4: Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação. [...] A.6.1.5: Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular. [...] A.6.1.3: Todas as responsabilidades pela segurança da informação devem estar claramente definidas. [...] (ABNT, 2006).

Desta forma, a direção do Instituto Alfa LTDA ME se propôs através de um documento que descreve o comprometimento com a segurança das informações transitadas via rede computadores. Assim, todos os líderes de diferentes setores devem efetivamente obedecer às regras estabelecidas pela ISO. Deste modo, cada setor da empresa tem a sua responsabilidade, levando em consideração que todos têm acesso a política de segurança da mesma.

Além disso, no tópico A.6.2 a mesma específica que:

> [...]A.6.2.1: Os riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas devem ser identificados e controles apropriados devem ser implementados antes de se conceder o acesso. [...]A.6.2.2: Todos os requisitos de segurança da informação identificados devem ser considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização. [...] (ABNT, 2006).

Sendo assim, a ferramenta *pfsense* atende prontamente a ISO devido ter sido configurada como um firewall na rede, de forma que controla toda informação que entra e sai pela rede interna.

As normas também estabelecem os seguintes parâmetros no tópico A.7.2:

> [...]A.7.7.2.1: A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização. [...]A.7.7.2.2: Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização [...] (ABNT; 2006).

A ferramenta possibilita os acessos as informações internas de forma controlada a cada nível. Pois, cada usuário só tem acesso àquilo que lhe é permitido tanto o acesso a internet ou a pasta interna.

ABNT no tópico A.8 afirma que:

> [...] A.8.1.1: Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação da organização. [...]A.8.1.2: Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e da organização para a segurança da informação. [...] A 8.1.3: Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e da organização para a segurança da informação [...] (ABNT, 2006).

De tal modo, a política desenvolvida pela diretoria defende que todo funcionário que é contratado pelo setor de recurso humanos será orientado através do documento o modo de utilização dos equipamentos e *softwares* da empresa e após as orientações o mesmo receberá uma cópia da política de segurança assinada como um termo de compromisso. Logo após, os colaboradores do setor de

Tecnologia da informação estará disposição para o treinamento do mesmo. Atendendo assim, as normas da ABNT.

A norma ainda, no tópico A.8.2 define que:

> [...] A.8.2.1: A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. [...] A.8.2.2: Todos os funcionários da organização e, onde pertinente, fornecedores e terceiros devem receber treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções [...] A.8.2.3: Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação. [...] (ABNT, 2006).

Toda a direção do instituto alfa LTDA ME trabalha juntamente com equipe de TI, orientando e dando treinamento para os funcionários. Assim, todos os colaboradores da empresa caso cometa alguma violação da segurança o mesmo será encaminhado para setor de recurso humano para que seja tomada as devidas providências**.**

Igualmente no tópico A.8.3 assegura que:

> [...] A.8.3.1: As responsabilidades para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas. [...] A.8.3.3: Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades. [...] (ABNT, 2006).

No entanto, a ferramenta por si só não é capaz de realizar o desligamento automático. Deste modo, toda a mudança de funcionário, seja troca de setor ou mesmo a demissão, primeiramente o setor de Recurso Humano (RH) que comunicando com setor da Tecnologia da informação (TI), para assim realizar todos os bloqueios e acessos no mesmo.

A ABNT no tópico A.9.2 informa que:

> [...] A.9.2.1: Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado [...] A.9.2.2: Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades. [...] (ABNT, 2006).

Por conseguinte, como solicitado na norma todo equipamento é centralizado em único lugar, sendo permitido o acesso semente pelo colaborador autorizado facilitando a manutenção do equipamento. A empresa adquiriu a um *nobreak* 1300 va *Mono net Winner* - com autonomia de até 80 minutos, sendo assim, caso tenha falha de energia os equipamentos permaneçam ligados por um determinado período.

Além disso, a norma no tópico A.10.5 assevera que “A.10.5.1: Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida [...]” (ABNT, 2006).

Ao utilizar a ferramenta como um firewall na rede. Ela não realiza nenhum tipo de *backup* em forma de pasta ou arquivo dos usuários. Desta forma, nesta parte a mesma não atende o termo supracitado. Ou seja, todo o backup deverá ser realizado pelo servidor de banco de dados *SQL Server*, rodando em um *Windows server* 2012.

A norma ainda cita no tópico 10.6 que “A. 10.6.1: Redes deve-se ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito. [...]” (ABNT, 2006).

Todavia, o tráfego que entra e sai da rede é filtrado pela *Pfsense* / *package Squid Proxy Reports* onde é gerenciado. Isto é, a mesma atende a norma supracitada. Como indicado na figura 6 uma amostra de um relatório de IP.

Figura 6 - Relatório de IP

Relatório de Acesso

Usuário: [redacted] Aqui ficara: nome ou ip usuario
Grupo: ?
Data: 09 Nov 2017
-= =-
User download "Big Files"

otal			**71.1 M**
#	Sites acessados	Conexões	Bytes
1	cdn3.bluestacks.com	38	40.8 M
2	universa.faveni.edu.br	2 513	17.0 M
3	www.posgraduacaofaveni.com.br	351	10.0 M
4	cdn-bgp.bluestacks.com	55	2.7 M
5	lh3.googleusercontent.com	3	154 862
6	bluestacks-cloud.appspot.com	9	118 529
7	faveni.edu.br	4	90 729
8	ava.faveni.edu.br	7	90 643
9	ava.institutoalfa.com.br	10	83 719
10	www.faculdadefuturo.com.br	56	46 736
11	cdn.bluestacks.com	23	44 867
12	ajax.googleapis.com	1	34 568
13	cloud.bluestacks.com	39	25 189
14	www.gstatic.com	2	17 742
15	r5---sn-bg07dnsl.gvt1.com	4	17 303
16	logc236.xiti.com	12	8 304
17	redirector.gvt1.com	6	8 240
18	r2---sn-bg07dnle.gvt1.com	1	6 468
19	eb.bluestacks.com	17	5 872
20	r3---sn-bg0e7n7z.gvt1.com	1	5 328
21	fonts.googleapis.com	2	4 529

Fonte: Próprio autor

Novamente, a norma no tópico A.10.8 e A.10.10 afiançam que:

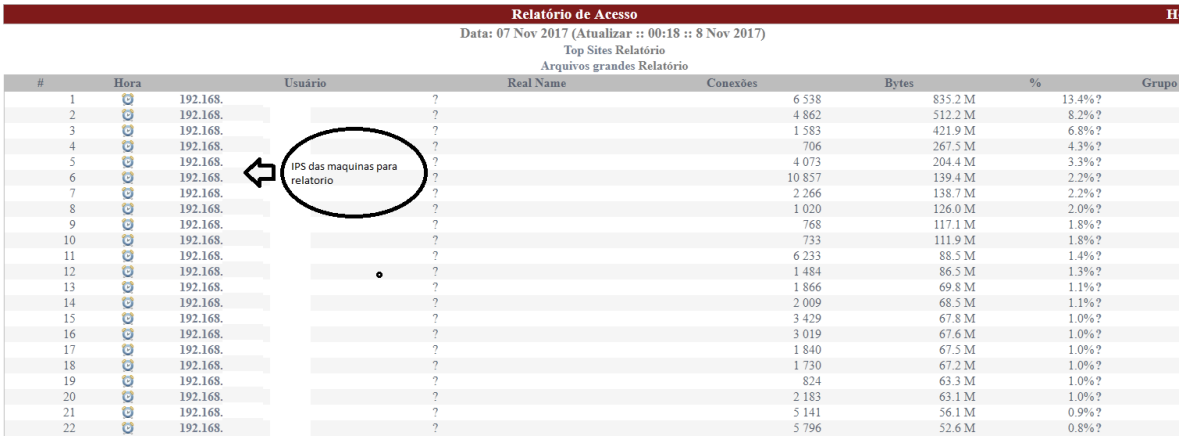
> [...] A.10.8.1: Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação. [...]A.10.8.2: Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio. [...] A.10.10.1: Registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso. [...]A.10.10. 2: Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente, de forma regular [...] (ABNT, 2006).

Dessa forma, todos os tráfegos na rede são filtrado pela *PFsense* melhorando o acompanhamento das atividades dos funcionários em geral, que original os relatórios que podem ser recolhidos ao final do mês, posteriormente poderão ser solicitados pela diretoria para análise e nas auditorias semestrais. Atendendo assim, os requisitos supracitados. Como são mostrados nas figuras 7 e 8, assim os relatórios podem ser filtrados pelo dia semana, mês ou ano.

Figura 7 - Relatórios através de filtros

Fonte: Próprio do autor

Figura 8 - Relatórios através de filtros



#	Hora	Usuário	Real Name	Conexões	Bytes	%	Grupo
1		192.168.	?	6 538	835.2 M	13.4%?	
2		192.168.	?	4 862	512.2 M	8.2%?	
3		192.168.	?	1 583	421.9 M	6.8%?	
4		192.168.	?	706	267.5 M	4.3%?	
5		192.168.	?	4 073	204.4 M	3.3%?	
6		192.168.	?	10 857	139.4 M	2.2%?	
7		192.168.	?	2 266	138.7 M	2.2%?	
8		192.168.	?	1 020	126.0 M	2.0%?	
9		192.168.	?	768	117.1 M	1.8%?	
10		192.168.	?	733	111.9 M	1.8%?	
11		192.168.	?	6 233	88.5 M	1.4%?	
12		192.168.	?	1 484	86.5 M	1.3%?	
13		192.168.	?	1 866	69.8 M	1.1%?	
14		192.168.	?	2 009	68.5 M	1.1%?	
15		192.168.	?	3 429	67.8 M	1.0%?	
16		192.168.	?	3 019	67.6 M	1.0%?	
17		192.168.	?	1 840	67.5 M	1.0%?	
18		192.168.	?	1 730	67.2 M	1.0%?	
19		192.168.	?	824	63.3 M	1.0%?	
20		192.168.	?	2 183	63.1 M	1.0%?	
21		192.168.	?	5 141	56.1 M	0.9%?	
22		192.168.	?	5 796	52.6 M	0.8%?	

Fonte: Próprio do autor

Já no tópico A.11.2 a norma estabelece que “A.11.2.1: Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços. [...]” (ABNT, 2006).

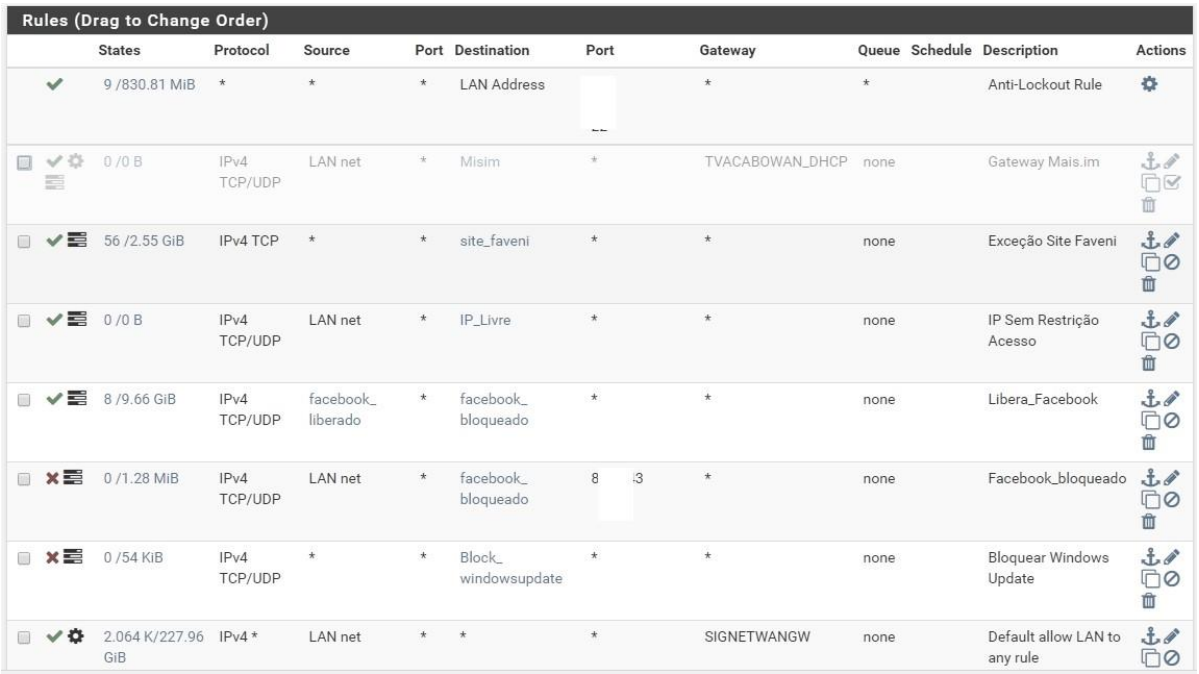
A ferramenta por se si não realiza tal ato automaticamente, deste modo, no instituto Alfa LTDA ME o colaborador que é remanejado deve seguir as normas descrito na política como já citado anteriormente.

Ao mesmo tempo, os usuários que necessitam da criação de senha para o acesso ao e-mail, programas instalados entre outros, tem que respeitar um padrão mínimo também descrito pela política de segurança e consentido com norma “A.11.2.3: A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal. [...] A.11.3.1: Os usuários devem ser orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas. [...]” (ABNT, 2006).

A norma ainda alega no tópico A 11.4 que “A.11.4.1: Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar [...]” (ABNT, 2006).

Como servidor de firewall, a *PFsense* controla toda saída e entrada de informação na rede, e todo o acesso do usuário, dessa forma foi criado grupo e cada um tem sua regra para o acesso, assim satisfazendo as regras da norma. Como pode ser observado na figura 9.

Figura 9 - Controle do firewall



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	9 /830.81 MiB	*	*	*	LAN Address		*	*		Anti-Lockout Rule	
✓	0 /0 B	IPv4 TCP/UDP	LAN net	*	Misim	*	TVACABOWAN_DHCP	none		Gateway Mais.im	
✓	56 /2.55 GiB	IPv4 TCP	*	*	site_faveni	*	*	none		Exceção Site Faveni	
✓	0 /0 B	IPv4 TCP/UDP	LAN net	*	IP_Livre	*	*	none		IP Sem Restrição Acesso	
✓	8 /9.66 GiB	IPv4 TCP/UDP	facebook_ liberado	*	facebook_ bloqueado	*	*	none		Libera_Facebook	
✗	0 /1.28 MiB	IPv4 TCP/UDP	LAN net	*	facebook_ bloqueado	8 :3	*	none		Facebook_bloqueado	
✗	0 /54 KiB	IPv4 TCP/UDP	*	*	Block_ windowsupdate	*	*	none		Bloquear Windows Update	
✓	2.064 K/227.96 GiB	IPv4 *	LAN net	*	*	*	SIGNETWANGW	none		Default allow LAN to any rule	

Fonte: Próprio do Autor

De acordo com figura 10 pode-se observar as regras de bloqueio que foi criada, aonde há os grupos de IPs livre e grupo de IPs Bloqueados.

A ABNT no tópico A 11.5 refere-se que:

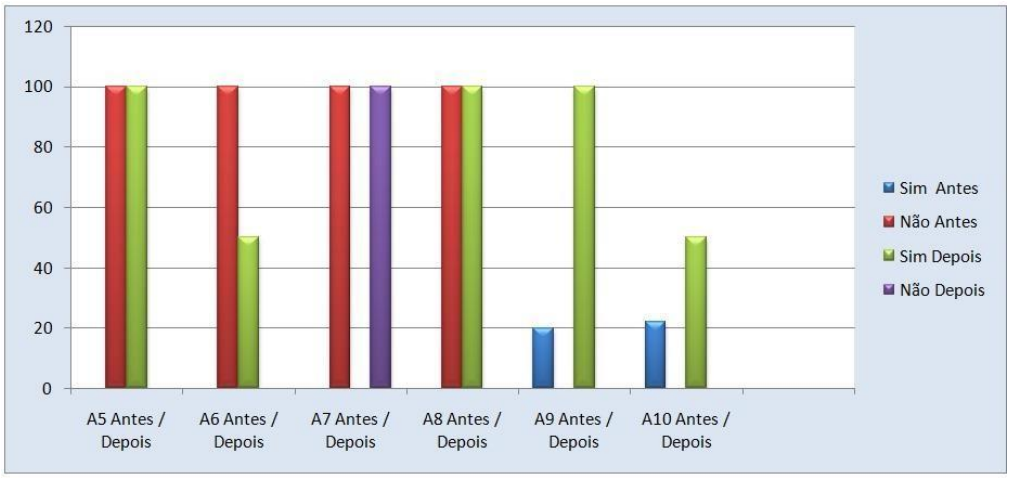
> [...]A.11.5.1: O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (*log-on*). [...]A.11.5: Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário. [...] A.11.5.3: Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade [...] (ABNT, 2006).

A ferramenta não foi configurada para esse serviço uma vez que, para controle de acesso as máquinas cliente utiliza-se um servidor *active directory windows* 2012 o mesmo que controla a autenticação de *logon* do sistema operacional.

A mesma não exerce tal função, devido não haver necessidade acesso remoto através de VPN. Além que, todos os processos de controle de informação e acesso a mesma e realizado pelo servidor de arquivos *windows server* 2012 ele que controla a integridade física dos dados.

Os gráficos 1 e 2 a seguir demonstram os cenários antes e depois da implantação da ferramenta pfSense na rede de computadores do Instituto Alfa com base nas normas da ISO\27001.

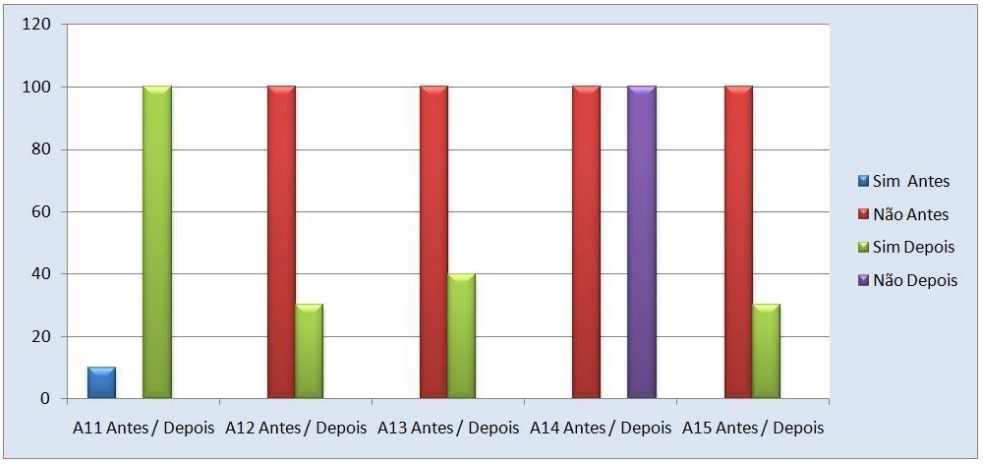
Gráfico 1 - Análise comparativa das normas A5 e A10 da ISO 27001/06 e a utilização da ferramenta *pfSense*



Fonte: Próprio do Autor

No gráfico 1 no tópico A7 como supracitado na análise, apesar da ferramenta não atender automaticamente, a norma será obedecida pela Política de segurança e pela equipe de TI da empresa.

Gráfico 2 - Análise comparativa das normas A11 e A15 da ISO 27001/06 e a utilização da ferramenta *pfSense*

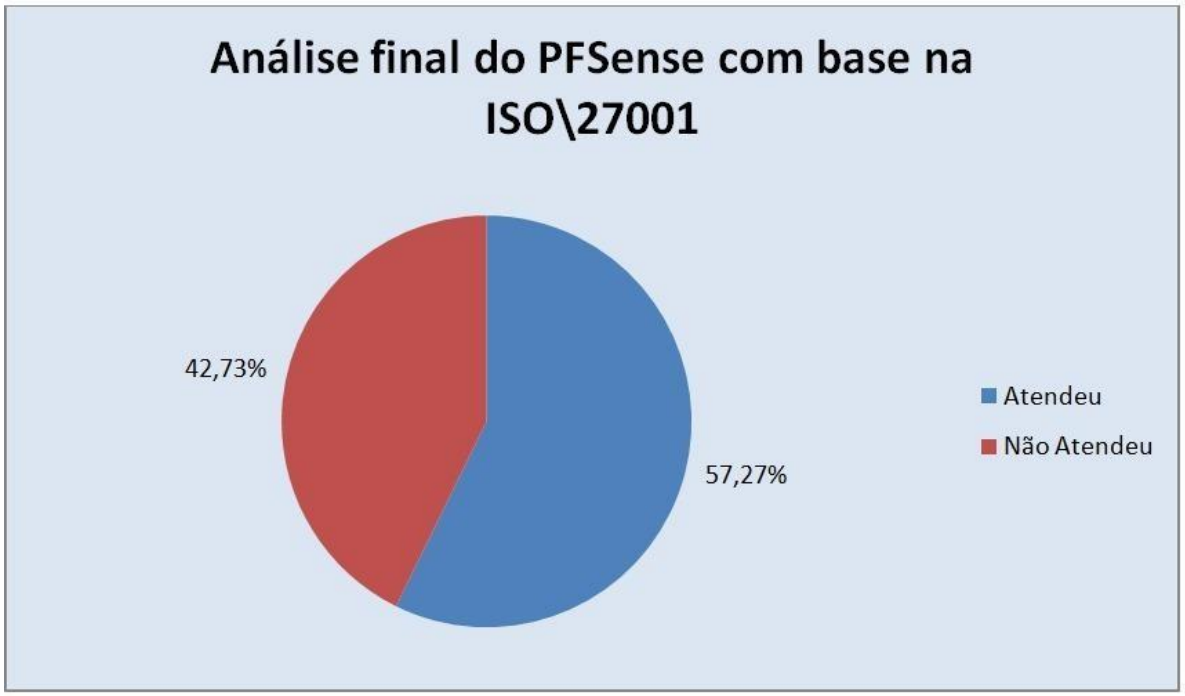


Fonte: Próprio do autor

Novamente no gráfico 2 os tópicos A14, serão atendidas através da Política de Segurança e a equipe de TI da empresa, assim atendendo os pré-requisitos estabelecidos pela norma.

Por fim o gráfico 3 traz o resultado final da porcentagem que a ferramenta pfSense, juntamente com a política de segurança, atendeu às normas da ISO\27001 indicando, portanto, que atendeu em 57,27% tais normas.

Gráfico 3 - Análise final do pfSense com base na ISO\27001/06



Fonte: Próprio do autor

CONCLUSÃO

Por tanto, o desenvolvimento do presente trabalho, permitiu a analise e a aplicação para promover a segurança da informação em um ambiente de rede de computadores empresarial em uma pequena empresa, foi utilizado a ferramenta o *PFsense* como um *firewall,* com baseamento nas diretrizes estabelecida pela ABNT NBR ISO/IEC 27001 de 2006. O estudo preeminente utiliza-se de várias referências bibliográficas, assim o conhecimento técnico para o desenvolvimento do mesmo, como os recursos podem auxiliar promovendo a segurança da informação.

A utilização da *PFsense* apoiado pelas normas da ABNT NBR ISO/IEC 27001 e a Política de Segurança da Informação documentada teve-se resultados aceitáveis. Através da ferramenta a empresa pode-se ter um melhor controle de acesso dos colaboradores, aonde que todos os funcionários poderá acessar aquilo que realmente é de interesse, demonstra-se que a ferramenta é um sistema que possui métodos eficazes para promover a segurança da informação em ambiente de redes corporativas. Além disso, a empresa aderiu a Política de Segurança da Informação que foi registrada nos autos da empresa que foi divulgada para todos os funcionários. Com essa ação, todos os usuários obteve-se conhecimento da importância que a organização atribui à segurança dos seus dados.

A finalidade geral do trabalho foi promover a segurança dos dados da organização aonde não havia um processo padronizado com este propósito. Tendo em vista, análise da ferramenta pode se afirmar que objetivo foi alcançado. Salientando que a ferramenta por ser um software livre a empresa teve mínimo de gasto com mesmo, ou seja, o projeto demonstrou que qualquer empresa que tem o desejo de promover segurança de suas informações, tem essa possibilidade através da *pfSense*, gerindo a segurança dos mesmos com baixo custeio. Bastando um conhecimento técnico para a sua implantação e a criação de uma política interna. Desta forma, a ferramenta se mostra eficaz mediante a seu custo e benefício.

TRABALHOS FUTUROS

Como direcionamento para possíveis linhas de trabalhos futuros tem-se:

- A análise e aplicação da ferramenta em uma empresa de grande porte, a fim de verificar se a ferramenta daria suporte a uma rede com maior complexidade.
- Análise comparativa de desempenho da ferramenta pfSense com outras ferramentas utilizadas como firewall.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. *ABNT NBR ISO/IEC 27001* – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.

ALMANZA, Pedro Alejandro Jasso; VARGAS, María de Jesús Rodríguez. *Gestión De Ancho De Banda En Un Esquema De Gateway*. Jóvenes En La Ciencia, v. 1, n. 1, p. 362-367, 2015.

ARAÚJO, Francisco Renato Cavalcante. Uso de Ambientes Virtualizados para o Ensino de Infraestrutura de Redes. *Anais da Escola Regional de Informática da Sociedade Brasileira de Computação (SBC)–Regional de Mato Grosso*, v. 6, p. 208- 210, 2015.

ASGHARI, Vahid; AMIRI, Shima; AMIRI, Shabnam. Implementing UTM based on PfSense platform. In: *Knowledge-Based Engineering and Innovation (KBEI), 2015 2nd International Conference on.* IEEE, 2015. p. 1150-1152.

BRASIL. *LEI Nº 12.737*, promulgada em 30 de Novembro de 2012. Brasília: Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htmL>. Acesso em: 13 out 2017.

BRENNER, Joel. ISO 27001: Risk management and compliance. Risk management, v. 54, n. 1, p. 24, 2007.

CALDER, Alan; WATKINS, Steve. *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd., 2008.

DA SILVEIRA, Sérgio Amadeu. *Inclusão digital, software livre e globalização contra-hegemônica.* Software Livre e Inclusão Digital - Organizadores: Sergio Amadeu de Silveira e João Cassino, v. 7, p. 11, 2003.

DISTERER, Georg. *ISO/IEC 27000, 27001 and 27002 for information security management.* 2013.

ISO/IEC 27000. *Norma ISO/IEC 27000***.** Disponível em: www.iso27000.com.br. Acesso em: 01 nov. 2013.

JUNIOR, Machado; MOREIRA, Dorival. *Proposta de Hardening em Conformidade com a ISO 27001 para um Firewall em Linux com Balanceamento de Carga.*

KUNDE, Diogo Otto; KONZEN, Marcos Paulo. *Utilização de um Firewall com Controle de Acesso no Instituto Federal Farroupilha*–Campus Júlio de Castilhos.

MAFIOLETTI, Rafael. *Uso Do Pfsense Para O Controle De Acesso Em Uma Rede Local. Repositório De Relatórios*-Sistemas de Informação, v. 1, n. 2, 2012.

MAFIOLETTI, Rafael; FURTADO, Rafael Gattino. *Uso De Gateway E Proxy Para Controle De Acesso Na Rede Do Centro Acadãšmico De Sistemas De Informação* DA UNIPLAC USANDO PFSENSE. Revista UNIPLAC, v. 1, n. 1, 2013.

MAROCCO, Carlos Alberto Duarte. *Proposta de topologia de rede de dados com segurança e foco na produtividade, utilizando ferramentas de software livre*. 2016.

MOLINA[1], Denison; SILVEIRA, Sidnei Renato; DOS SANTOS, Fernando Beux. *Implantação de Um Ambiente de Segurança de Redes de Computadores:* Um Estudo de Caso na Prefeitura Municipal de Palmeira das Missões-RS.

NEVES, Filipe Campos das; MACHADO, Leonardo Alves; CENTENARO, Rodrigo da Fontoura. *Implantação de Firewall PfSense.* 2014. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

PFSENSE. *pfSense***.** Disponível em: < www.pfsense.org.br >. Acesso em: 28 jun. 2017.

PINHEIRO, José Maurício Santos. *Gerenciamento de Redes de Computadores:* Uma Breve Introdução. BICSI, 2006.

Conhecendo a ABNT NBR ISO/27001. Profissionais do TI, 2010. Disponível em: < https://www.profissionaisti.com.br/2010/10/conhecendo-a-abnt-nbr-isoiec-27001-parte-1/> Acessado em: 10 de out de 2017.

PUGLIESE, Bruno Zata; LOVISI, Alexandre Luiz Moraes. *Virtualização De Servidores: Estudos Comparativos Entre Ferramentas*. Caderno de Estudos em Sistemas de Informação, v. 2, n. 1, 2015.

RIBEIRO, Matheus Phillipe De Oliveira. *Utilização Do Sistema De Roteamento Mikrotik Para Promover A Segurança Em Rede De Computadores Com Base Nas Diretrizes Da AbntNbrIso/Iec 27001.* 2016.

SEVERINO, Paulo Jacinto Rosa; ARAÚJO, Fabrício Geraldo. *Implementação De Uma Infraestrutura De Rede Abordando Vlans, Utilizando Pfsense No Roteamento.* Revista do COMINE, v. 1, n. 1, 2016.

WILLIAMSON, Matt**.** *Livro do PFSense*: Um guia prático com exemplo ilustrados de configurações, para usuários iniciante e avançados sobre o PFSense 2.0. Packt Publishing. 2011.

ZIENTARA, David. *MasteringpfSense.* Packt Publishing Ltd, 2016.

ANEXO 1: AUTORIZAÇÃO PARA APLICAÇÃO DE ESTUDO DE CASO

FAVENI

Formulário de liberação para redação de estudo de caso.

Empresa: Instituto Educacional Alfa LTDA - ME

CNPJ: 14.086.522/0001-62

Endereço: Rua Joao Pinheiro nº204, Centro, Caratinga MG

Telefone: (33)3329-2500

Pelo presente, em nome do INSTITUTO EDUCACIONAL ALFA LTDA – ME, a qual represento neste ato, afirmo que o aluno **Fernando Oliveira de Almeida** iniciará um estudo de caso para fins acadêmicos para FACULDADES INTEGRADAS DE CARATINGA (FIC). Autorizo assim, utilizar o nome empresarial para redação, podendo distribuir e publicá-lo em sites, revista, livros, coletâneas entre outros de casos, desde que venham a ser organizados pela citada escola, sem nenhum ônus, cedendo todos os diretos inerentes a intelectual do caso a FIC.

Caratinga, 25 de junho de 2017.

Sheila Valquiria Gomes Timóteo

Representante legal

ANEXO 2: POLÍTICA DE SEGURANÇA DO INSTITUTO ALFA LTDA ME

FAVENI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
DO INSTITUTO ALFA
CARATINGA – MG

1 INTRODUÇÃO

A informação é um ativo muito importante, eficaz para o funcionamento das empresas e consequentemente necessita ser protegida. Ela pode ser apresentada em diversas formas: impressa ou escrita em papel, falada em conversas, armazenada eletronicamente em arquivos de som, imagem, vídeo, texto, entre outros.

Este documento contempla um conjunto de instruções e procedimentos mínimos para padronizar e melhorar a visão dos usuários sobre a segurança da informação.

1.1 Instituto alfa e política de segurança

Juntamente com diretoria as normas aqui listadas foram analisadas e aprovadas. Todos os colaboradores devem seguir com cuidado as orientações da política de segurança. Ao receber uma cópia das normas internas de segurança o (a) funcionário (a) compromete-se a cumprir todos os tópicos listados e está ciente de que seus e-mails, conteúdo acessado a internet ou na rede interna podem estar sendo monitorados.

1.2 Opondo-se a política de segurança

Não havendo o cumprimento das orientações ou normas dessa política de segurança, acarretará em uma advertência administrativa ou podendo ocorrer o desligamento do funcionário dependendo do nível ou gravidade do ocorrido.

FAVENI

1.3 Autenticação

O meio de autenticação nos sistemas informatizados será baseado por uma senha. A utilização de senhas que contenham nome de usuário, combinações simples (abcd1234), substantivo próprio ou datas são comuns.

1.4 Políticas de senha

As políticas de complexidade de senha são projetadas para deter ataques de força bruta aumentando o número de possíveis senhas. Quando a política de complexidade de senha é imposta, as novas senhas devem atender às seguintes diretrizes:

- A senha não contém o nome de conta do usuário.
- A senha tem um comprimento de pelo menos oito caracteres.
- Letras maiúsculas latinas (A a Z).
- Letras minúsculas latinas (a a z).
- 10 dígitos base (0 a 9).
- As senhas terão tempo de validade determinada pelo departamento de tecnologia da informação, após o vencimento desse prazo a mesma irá expirar e para ter acesso novamente ao sistema o usuário deverá redefinir uma nova senha. Não sendo permitido a renovação da antiga senha.
- O usuário será responsável por tudo que for executado com sua senha, por isso e de grande importância mantê-la secreta.

FAVENI

1.5 Acesso à internet

- Será permitida somente a navegação em sites ou sistema online relacionados, ao trabalho.

- O uso de redes sociais não poderá acontecer durante o horário de expediente, exceto quando houver alguma autorização da diretoria.
- O acesso a conteúdo na internet é bloqueado, somente sites relacionados com o trabalho terá acesso livre.
- O uso da internet para envio de mensagens instantâneas somente será permitido para funcionários com autorização da diretoria.

1.6 Uso das estações de trabalho

- Os equipamentos da rede de computadores possuem um endereço IP tornando possível a sua identificação.
- Cada colaborador tem sua estação de trabalho e tudo que for executado será de responsabilidade de cada um.
- Os logs e históricos do sistema poderão ser acessados para apurar as causas de determinados acontecimentos.
- De nenhuma maneira será permitido a instalação de software nos computadores. Caso tenha necessidade a equipe de TI deverá ser comunicada.
- Não será permitido que tenha em seu computador tipo de arquivos MP3, filmes, software com direitos autorais.
- Não será permitida a utilização de mídias removíveis como por exemplos como pen drive, CD's, ou DVD's.

FAVENI

- Não será permitida a utilização de mídias removíveis como por exemplos como pen drive, CD's, ou DVD's.

1.7 E-mail

A seguir possui tópicos que orientarão para a utilização do e-mail empresarial de forma segura.

- Não abra anexos de e-mail com assuntos desconhecidos onde no campo remetente e destinatário está informado o mesmo endereço de e-mail.
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft, crianças desaparecidas, criança doente, etc.
- Não utilize e-mail da empresa para assunto pessoal. Utilize sempre sua assinatura para enviar e-mails. Em caso de dúvida sobre algum link ou anexo em um e-mail procurar departamento de TI antes de tentar visualizar o conteúdo.

FAVENI

DIRETORA GERAL
SHEILA TIMÓTEO

GERENTE ADMINISTRATIVO
DENISE MUNIZ

GERENTE DE RECURSOS HUMANOS
TALLIS ALEXANDRE

GERENTE DE TECNOLOGIA DA INFORMAÇÃO
EMERSON JOSÉ FERNANDES

FAVENI

SUPERVISOR DE TECNOLOGIA DA INFORMAÇÃO
CÉSAR BENTO DA SILVA