

MATHEUS PHILLIPE DE OLIVEIRA RIBEIRO

**UTILIZAÇÃO DO SISTEMA DE ROTEAMENTO MIKROTIK
PARA PROMOVER A SEGURANÇA EM REDE DE
COMPUTADORES COM BASE NAS DIRETRIZES DA ABNT
NBR ISO/IEC 27001**

BACHARELADO

EM

CIÊNCIA DA COMPUTAÇÃO

FIC – CARATINGA

2016

MATHEUS PHILLIPE DE OLIVEIRA RIBEIRO

**UTILIZAÇÃO DO SISTEMA DE ROTEAMENTO MIKROTIK
PARA PROMOVER A SEGURANÇA EM REDE DE
COMPUTADORES COM BASE NAS DIRETRIZES DA ABNT
NBR ISO/IEC 27001**

Monografia apresentada à banca examinadora da Faculdade de Ciência da Computação das Faculdades Integradas de Caratinga, como requisito parcial para obtenção do título de bacharel em Ciência da Computação, sob orientação do professor Jonilson Batista Campos.

FIC – CARATINGA
2016

MATHEUS PHILLIPE DE OLIVEIRA RIBEIRO

**UTILIZAÇÃO DO SISTEMA DE ROTEAMENTO MIKROTIK
PARA PROMOVER A SEGURANÇA EM REDE DE
COMPUTADORES COM BASE NAS DIRETRIZES DA ABNT
NBR ISO/IEC 27001**

Monografia submetida à Comissão
examinadora designada pelo Curso de
Graduação em Ciência como requisito para
obtenção do grau de Bacharel.

Profº. Jonilson Batista Campos
Faculdades Integradas de Caratinga

Profª. Msc. Fabrícia Pires de Souza
Faculdades Integradas de Caratinga

Profº. Wanderson Miranda Nascimento
Faculdades Integradas de Caratinga

Caratinga, 13 / 12 / 2016

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, meu irmão José Francisco por toda contribuição e conselhos durante esse período acadêmico.

Agradeço ao Paulo Alves por permitir a realização do trabalho em sua empresa. Aos demais funcionários da Minasvel, que também contribuíram com o presente trabalho.

A todos os professores, pela partilha de conhecimentos e ensinamentos que serão levados por toda a 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

Antes mesmo da evolução da tecnologia já existia um certo cuidado com a integridade das informações. As facilidades trazidas com os meios de transmissão e compartilhamento de dados, trouxeram também as ameaças e vulnerabilidades que comprometeram os sistemas. A fim de minimizar este problema foram criadas leis, normas e padrões com a finalidade de garantir a privacidade das pessoas e organizações.

Os grandes problemas gerados pela perda acidental de dados ou acesso e divulgação não autorizados, tem causado grandes prejuízos para as pessoas e empresas. Sendo assim, o foco deste trabalho foi direcionado a segurança da informação, que visa avaliar, melhorar e manter esse quesito que ultimamente tem chamado muito a atenção das pessoas.

Buscando solucionar alguns destes problemas, foi realizado um estudo na concessionária de veículos Fiat de Caratinga-MG, onde o ambiente de pesquisa é a própria rede de computadores da organização. O objetivo deste trabalho foi utilizar como ferramenta principal, o *Mikrotik RouterOS* para promover a segurança. Também foram seguidas algumas das diretrizes da ABNT NBR ISO/IEC 27001, que orientam o processo de desenvolvimento e divulgação da política de segurança. A finalidade de utilizar a ISO neste trabalho não é a obtenção de certificação com a norma, mas sim utilizar seus recursos para alcançar melhores resultados. Espera-se apresentar através dos resultados deste estudo, como a utilização do *Mikrotik RouterOS* juntamente com uma política de segurança da informação bem definida, podem trazer vantagens frente às ameaças a um dos ativos mais importantes das empresas, a informação.

Palavras chaves: Redes de Computadores, Segurança da Informação, ISO27001, *RouterOS*.

ABSTRACT

Even before the evolution of technology there was already a certain care with an integrity of the information. The facilities brought in with the means of transmission and sharing of data, as well as threats and vulnerabilities that compromise the systems. In order to minimize this problem laws, standards and standards have been created with a view to ensuring the privacy of individuals and organizations.

The major problems caused by the accidental loss of data or access and unauthorized disclosure have caused great harm to people and companies. Therefore, the focus of the work was directed to the information security, that the visa is good, to improve and maintain this item that lately is very called attention to people.

In order to solve some of these problems, a study was carried out at the Fiat car dealership in Caratinga-MG, where the research environment is a computer network of the organization. The purpose of this work was used as the main tool, the Mikrotik RouterOS to promote a security. Some of the guidelines of ABNT NBR ISO / IEC 27001 were also followed, which guide the process of developing and disseminating security policy. The purpose of using an ISO in this work is not to obtain certification with a standard, but rather to use its resources for results results. It is expected to show on the results of this study, such as the use of the Mikrotik RouterOS together with a well-defined information security policy, can bring advantages against the threats to one of the most important elements of enterprises, information.

Keywords: *Computer Networks, Information Security, ISO 27001, RouterOS.*

LISTA DE FIGURAS

Figura 1. Princípios Básicos da Segurança da Informação	22
Figura 2. Desenho da rede de computadores antes da política de segurança	37
Figura 3. Planos de manutenção <i>Management Studio</i>	40
Figura 4. <i>Backup</i> do <i>Windows</i>	41
Figura 5. Desenho da Rede Computadores após a política de segurança.....	42
Figura 6. Filtro de MAC dos roteados da rede wireless interna	44
Figura 7. Regra do <i>Firewall</i> aba <i>General drop</i> porta 2000	46
Figura 8. Regra do <i>Firewall</i> aba <i>Action drop</i> porta 2000	47
Figura 9. Regra do <i>Firewall</i> aba <i>General</i> redirecionamento por NAT	48
Figura 10. Regra do <i>Firewall</i> aba <i>Action</i> redirecionamento por NAT	49
Figura 11. Regra que restringe <i>login</i> para serviços FTP	50
Figura 12. Configurações do <i>web proxy</i>	53
Figura 13. Regras do <i>Web Proxy Access</i>	55
Figura 14. Regras do <i>web proxy</i> liberações e bloqueios.....	56
Figura 15. Modelo de um tonel PPTP	57
Figura 16. Servidor PPTP	58
Figura 17. Inclusão de usuários no servidor PPTP	58
Figura 18. Painel de controle do <i>Avast for Business</i>	61
Figura 19. Execução da ferramenta <i>PING</i>	71
Figura 20. Execução da ferramenta <i>HPING3</i>	71
Figura 21. Execução da ferramenta <i>DNSMAP</i>	72
Figura 22. Execução da ferramenta <i>DNSMAP</i> com a <i>Word List</i> gerada	73
Figura 23. Execução da ferramenta <i>NMAP -sV</i>	74
Figura 24. <i>Address Lists</i> do <i>Firewall</i>	75

LISTA DE TABELAS

Tabela 1. Pessoas que podem causar problemas de segurança e seus motivos para fazê-lo	19
Tabela 2. Principais ameaças.....	23
Tabela 3. Vulnerabilidades da Segurança da Informação	25

LISTA DE GRÁFICOS

Gráfico 1. Organização atual dos dispositivos	78
Gráfico 2. Qualidade da rede atual	79
Gráfico 3. Acesso aos <i>softwares</i> utilizados	80
Gráfico 4. Sua segurança sobre as informações	81
Gráfico 5. Praticidade de acesso as informações.....	82
Gráfico 6. Recuperação de serviços após falhas.....	83
Gráfico 7. Utilização das redes <i>wireless</i>	84
Gráfico 8. Importância da segurança para a empresa.....	85
Gráfico 9. Importância que você atribui a segurança da informação	86
Gráfico 10. Atitudes da empresa para proporcionar a segurança da informação	87
Gráfico 11. Suas atitudes para proporcionar a segurança da informação.....	88
Gráfico 12. Seu comportamento com relação a segurança da informação.....	89
Gráfico 13. Investimento da empresa em segurança da informação	90
Gráfico 14. Qualidade dos serviços prestados referente a segurança da informação	91
Gráfico 15. Importância das orientações sobre as práticas de segurança da informação	92

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
ADSL - *Asymmetric Digital Subscriber Line*
CRM - *Customer Relationship Management*
DMS - *Dealer Management System*
FTP - *File Transfer Protocol*
ICMP - *Internet Control Message Protocol*
IEC - *International Electrotechnical Commission*
IP - *Internet Protocol*
ISO - *International Organization for Standardization*
LAN - *local area network*
MAC - *Media Access Control*
MAN - *metropolitan area network*
MBPS - *Megabit por segundo*
MG - Minas Gerais
MPPE - *Microsoft Point to Point Encryption*
NAT - *Network Address Translation*
OS - Ordem de Serviço
PPP - *Point to Point Protocol*
PPTP - *Point to Point Tunneling Protocol*
SBC - *Single Board Computer*
SQL - *Structured Query Language*
TCP - *Transmission Control Protocol*
TCU - Tribunal de Contas da União
TI - Tecnologia de Informação
UDP - *User Datagram Protocol*
VPN - *Virtual Private Network*
WAN - *wide area network*
WPA2 - *Wired Protected Access*

SUMÁRIO

INTRODUÇÃO.....	14
1. REFERENCIAL TEÓRICO	16
1.1 REDES DE COMPUTADORES.....	16
1.1.1 Gerenciamento de Redes.....	17
1.1.2 Segurança em redes.....	18
1.2 SEGURANÇA DA INFORMAÇÃO	20
1.2.1 Ameaças	22
1.2.2 Vulnerabilidades.....	24
1.3. FERRAMENTAS DE AUDITORIA EM REDES DE COMPUTADORES.....	25
1.3.1 <i>Kali Linux</i>	25
1.3.2 Metodologia do Teste de Penetração	26
1.3.3 Detecção de Sistemas Ativos (<i>PING</i>)	27
1.3.4 <i>HPING3</i>	27
1.3.5 <i>DNSMAP</i>	28
1.3.6 <i>NMAP</i>	28
1.3.7 <i>Hydra</i>	29
1.4. FERRAMENTAS PARA SEGURANÇA DA INFORMAÇÃO	29
1.4.1 <i>Mikrotik</i>	29
1.5 ABNT NBR ISO/IEC 27001	31
2. METODOLOGIA	33
2.1 OBJETIVO DE ESTUDO	33
2.2 AMBIENTE DE ESTUDO.....	34
2.3 EXECUÇÃO DAS MUDANÇAS.....	38
2.3.1 Alterações nas Estruturas Físicas e Lógicas.....	38
2.3.2 Política de <i>Backup</i>	39
2.3.3 Proteção Contra Falhas de Eletricidade	41
2.3.4 Mapa da Rede Após a Implementação	41
2.3.5 Segurança na Rede <i>Wireless</i>	43
2.3.6 <i>Firewall</i>	44
2.3.7 <i>Web Proxy</i>	51

2.3.8 Rede Privada Virtual	56
2.3.9 Antivírus e Monitoramento	59
3. RESULTADOS	63
3.1 RECOMENDAÇÕES DA ABNT NBR ISO/IEC 27001	63
3.1.1 Política de Segurança da Informação	63
3.1.2 Comprometimento da Direção com a Segurança da Informação.....	64
3.1.3 Atribuição de responsabilidades para a segurança da informação	65
3.1.4 Identificação dos riscos relacionados com partes externas	65
3.1.5 Inventário dos ativos	66
3.1.6 Antes da Contratação de Colaboradores	66
3.1.7 Conscientização, Educação e Treinamento em Segurança da Informação	67
3.1.8 Retirada de Direitos de Acesso	67
3.1.9 Controles de Entrada Física.....	68
3.1.10 Utilidades	68
3.1.11 Documentação dos Procedimentos de Operação	69
3.1.12 Controle Contra Códigos Maliciosos	69
3.2 TESTES DE INVASÃO	70
3.2.1 <i>Ping</i>	71
3.2.2 DNSMAP	72
3.2.3 NMAP	73
3.2.4 Regra de Prevenção Contra os Ataques de Força Bruta.....	75
3.2.5 <i>xHydra</i>	76
3.3 QUESTIONÁRIO REFERENTE A SEGURANÇA DA INFORMAÇÃO	77
4. CONCLUSÃO.....	93
4.1 TRABALHOS FUTUROS	94
REFERÊNCIAS	95
ANEXO 1 – AUTORIZAÇÃO PARA REDAÇÃO DE ESTUDO DE CASO	97
ANEXO 2 – DOCUMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO MINASVEL	98
ANEXO 3 – TERMOS DE RESPONSABILIDADE NO USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO.....	104
ANEXO 4 – INVENTÁRIO DOS ATIVOS.....	105
ANEXO 5 – RETORNO DA EXECUÇÃO DO NMAP COM AS FUNÇÕES –T4 –A –s..	107
ANEXO 6 – LOG DO ATAQUE COM XHYDRA.....	109

ANEXO 7 – QUESTIONÁRIO SOBRE A SEGURANÇA DA INFORMAÇÃO NA
EMPRESA..... 110

INTRODUÇÃO

A segurança da informação surgiu para manter a integridade, confidencialidade, autenticidade e disponibilidade de determinados dados, preservando seus respectivos valores para seus proprietários (TRINUNAL DE CONTAS DA UNIÃO, 2012). Na atualidade, com a grande expansão da tecnologia e o aumento constante dos dados que as organizações têm lidado, passou-se a investir mais em equipamentos para armazenamento, compartilhamento e transmissão desses dados. Ao mesmo tempo, com as facilidades surgiu também um problema, que é manter a informação íntegra, segura, utilizando-se de recursos acessíveis.

Os dados das empresas aumentam de forma exponencial, tornando-se cada vez mais preciosos e desta forma necessitam de maior atenção e investimento na segurança dos mesmos. De acordo com uma pesquisa realizada no terceiro trimestre 2016 pela empresa *Akamai Technologies*, o Brasil é o quinto país que mais envia ataques *hackers* pelo mundo, ficando atrás apenas da China, Estados Unidos, Reino Unido e França, além de ser o segundo país que mais recebe ataques *hackers* do mundo, ficando atrás apenas dos Estados Unidos (AKAMAI, 2016).

É grande a quantidade de relatos de empresas que sofrem prejuízos por terem seus dados sequestrados ou perdidos de forma acidental (PWC, 2016). Outra questão preocupante, é que não existem muitos especialistas na área de segurança da informação disponíveis no mercado e a procura por eles tem crescido muito. As empresas veem a necessidade de ter este tipo de profissional para implantar e manter metodologias de segurança para seus dados.

O presente trabalho foi desenvolvido em uma concessionária de veículos da cidade de Caratinga-MG. Verificado diversos erros nos procedimentos e configurações da infraestrutura de computadores, que poderiam colocar em riscos as informações da empresa, foram estabelecidas medidas para solucionar os problemas.

O objetivo geral deste estudo, foi promover a segurança da informação em redes de computadores empresariais, utilizando o *Mikrotik RouterOS* com base nas diretrizes da ABNT NBR ISO/IEC 27001.

O diferencial deste trabalho é a utilização do sistema operacional de roteamento *Mikrotik*, sendo um servidor de baixo custo de aquisição que possui grande capacidade de roteamento. Outro ponto importante que vale ser destacado é a aplicação das diretrizes da ABNT NBR ISO/IEC 27001. Tal norma especifica itens obrigatórios para a implementação

de uma Política de Segurança da Informação.

Para a execução deste trabalho foram necessários estudos relacionados com redes de computadores, segurança da informação, sistemas de roteamento e a ABNT NBR ISO/IEC 27001, estando descritos no primeiro capítulo.

No segundo capítulo, estão detalhadas todas ações executadas para a adequação dos problemas relacionados à segurança da informação. Um mapa de toda a estrutura da rede de computadores da empresa foi criado com o intuito de eliminar as falhas presentes nos dispositivos e sistemas de informação. Ainda no segundo capítulo, poderão ser vistos detalhes da reestruturação da rede de computadores, políticas de *backups* implantadas, configurações definidas no *Firewall* e *Web Proxy*, configuração de uma rede privada virtual e sistemas para detecção de *softwares* maliciosos.

Os resultados obtidos foram apresentados no terceiro capítulo. Nesse capítulo, poderão ser observadas as diretrizes da ABNT NBR ISO/IEC 27001 que foram utilizadas e atendidas durante o estudo. Como medida de comprovação de eficiência do *Firewall* implantado na empresa, são apresentados os resultados dos testes de invasão que foram executados contra o servidor. Além da coleta de dados realizada pelo autor para apresentação dos resultados, também houve a aplicação de um questionário na empresa, onde foram obtidas informações referentes as mudanças após a implantação da Política de Segurança da Informação.

Por fim, no quarto capítulo será possível observar a conclusão do estudo e sugestões para trabalhos futuros.

1. REFERENCIAL TEÓRICO

Neste capítulo serão abordados alguns conceitos referentes ao tema abordado. Serão apresentados assuntos como: Redes de Computadores, Segurança da Informação, *Mikrotik* e ABNT NBR/ISO IEC 27001.

1.1 REDES DE COMPUTADORES

O termo Redes de Computadores é definido por Tanenbaum (2003) como um conjunto de computadores autônomos interconectados por uma única tecnologia. Essa conexão pode ser por meio de fios de cobre, fibras ópticas, ondas de infravermelho e satélites.

Seu surgimento originou da necessidade de troca de informações tornando possível o acesso a dados que estão fisicamente distantes. As redes existem desde os primeiros computadores, antes da era dos computadores pessoais. Com o avanço tecnológico surgiram novas padronizações que resultaram em uma melhoria na comunicação e uma redução em seu custo (TORRES, 2001).

Para normatizar as redes de computadores temos os protocolos, que são um conjunto de regras que formam um acordo de comunicação. O termo padrão é diferente de protocolo onde um padrão se refere a um protocolo adotado por uma organização de padronização e empresas do ramo (FOROUZAN, 2008).

Para caracterizar uma rede pode-se observar seu tipo de conexão, sua topologia física e sua classificação referente ao seu tamanho. De acordo com Forouzan (2008), existem dois tipos de conexões: a ponto-a-ponto e a multiponto. Na conexão ponto-a-ponto há apenas um enlace dedicado entre dois dispositivos, onde um comunica apenas com o outro. Na conexão multiponto mais de um dispositivo se comunica com outros através de um mesmo enlace.

Segundo Forouzan (2008) as redes podem ser classificadas com as seguintes topologias:

- a) Topologia Malha: cada dispositivo possui um link aos demais dispositivos da rede.
- b) Topologia Estrela: cada dispositivo se comunica dedicadamente a um controlador ou concentrador no centro da estrutura.

- c) Topologia Barramento: é utilizado um cabo como uma espinha dorsal onde os dispositivos conectam através de segmentos de cabos e conectores de pressão.
- d) Topologia Anel: cada dispositivo está ligado a mais dois dispositivos próximo ao mesmo.

Por fim, uma rede pode ser classificada de acordo com seu tamanho. Seguindo este critério uma rede pode ser classificada em (TANENBAUM, 2003):

- a) LAN (*local area network*): ou rede local, são redes privadas contidas muitas vezes em um edifício ou campus com apenas alguns quilômetros de extensão.
- b) MAN (*metropolitan area network*): ou rede metropolitana, são redes que abrangem uma cidade.
- c) WAN (*wide area network*): ou rede geograficamente distribuída, são redes que abrangem uma grande área geográfica, como um país ou continente.

A importância em saber como classificar uma rede está relacionado a conhecer como é o seu funcionamento de acordo com suas características para assim prover meios que deem segurança a rede. Esta preocupação com a segurança em redes de computadores surgiu devido ao seu crescimento e uso corporativo, onde cada vez mais empresas se preocupam com as informações de negócios que podem ser obtidas por uma invasão. Desta forma, garantir a segurança em uma rede de computadores é garantir que pessoas mal-intencionadas não possam ter acesso a informações enviada a outro destinatário (TANENBAUM, 2003).

Sendo assim surgiu a necessidade de um gerenciamento de redes para manter seu perfeito funcionamento e a segurança das informações que trafegam nesta rede. A seção seguinte aborda o tema gerenciamento de redes e apresenta conceitos importantes relacionados a este tema.

1.1.1 Gerenciamento de Redes

No início da utilização de redes de computadores, quando ainda eram utilizadas apenas como objetos de pesquisa, não existia o termo gerenciamento de redes. Os erros ocorridos nas redes poderiam ser descobertos através de testes simples, sendo possível tomar medidas em cima do descoberto. Na atualidade o cenário é diferente, já que existem redes de infraestrutura usada por milhões de pessoas através da internet. Por ser uma rede pública, surgiu a necessidade de um gerenciamento tanto de *hardware* quanto de *software* par garantir

seu funcionamento e a segurança dos dados que são transportados. Desta forma, o gerenciamento foi dividido em cinco principais áreas (KUROSE; ROSS, 2009):

- a) Gerenciamento de desempenho: seu objetivo é medir, quantificar, informar, analisar e controlar o desempenho dos diversos componentes que compõem a rede.
- b) Gerenciamento de falhas: seu objetivo é registrar, detectar e reagir as falhas de uma rede de forma imediata.
- c) Gerenciamento de configuração: permite que o responsável pela rede saiba quais os componentes fazem parte de sua estrutura e suas configurações de *hardware* e *software*.
- d) Gerenciamento de contabilização: tem por objetivo especificar, registrar e controlar o acesso de usuários e dispositivos aos recursos da rede.
- e) Gerenciamento de segurança: tem como meta controlar o acesso aos recursos da rede conforme uma política pré-estabelecida. Várias ferramentas foram criadas para auxiliar este gerenciamento.

Ao compreender o que é o gerenciamento de redes e o que cada uma das cinco áreas representam, torna-se visível a sua necessidade para uma rede eficiente em seu funcionamento. Outro ponto importante que deve ser estudado com maior detalhe é a segurança em redes que foi abordado na seção a seguir.

1.1.2 Segurança em redes

Roubo de senhas de cartões de crédito, roubo de segredos industriais e comprometimento de sistemas empresariais, são alguns exemplos de crimes virtuais que atingem desde pessoas simples à grandes empresas. Devido a isso, estes incidentes de segurança tiveram a necessidade de serem registrados, identificados e mensurados para que assim possam ser tomadas medidas de segurança, para que este mesmo incidente não volte a acontecer (CARVALHO, 2005).

A maior parte destes incidentes são causados por pessoas maliciosas, com a intenção de prejudicar alguém, chamar a atenção ou obter algum benefício. Tanenbaum (2003), lista os principais tipos de invasores:

Tabela 1. Pessoas que podem causar problemas de segurança e seus motivos para fazê-lo

ADVERSÁRIO	OBJETIVO
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte: (TANENBAUM, 2003, p. 543)

Através desta lista, Tanenbaum (2003) exemplifica que para ter um sistema seguro não basta mantê-lo sem erros de programação, mas é necessário estar preparado para lidar com adversários inteligentes e em sua maioria bem financiados. Segundo registros policiais os principais adversários são pessoas que estão descontentes com a organização a que pertencem, sendo assim ao projetar o sistema de segurança deve-se estar atento a este fato.

Segundo Kurose e Ross (2010), as propriedades desejáveis para que haja uma comunicação segura são:

- a) Confidencialidade: somente o remetente e o destinatário devem ter conhecimento do conteúdo da mensagem, sendo assim ela deve ser cifrada para que um interceptador não consiga entender seu conteúdo.
- b) Autenticação do ponto final: remetente e destinatário devem certificar a identidade da outra parte envolvida na comunicação.
- c) Integridade de mensagem: deve garantir que o conteúdo da mensagem não seja alterado.
- d) Segurança operacional: utilização de mecanismos operacionais para deter ataques a redes organizacionais através de invasões pela Internet pública.

Estas propriedades definem o que se conhece como segurança em rede. Ao usar o termo segurança em rede tem-se como foco os mecanismos que devem ser usados para

garantir tal segurança, porém para saber qual melhor mecanismo a ser usado e para que ele seja eficiente é necessário saber qual o tipo de ameaça o sistema está sujeito (CARVALHO, 2005).

As ameaças e as vulnerabilidades são definidas pela segurança da informação que é uma área do conhecimento com a finalidade de proteger ativos da informação contra acessos não autorizados (SÊMOLA, 2014). A seção seguinte contextualiza a segurança da informação e os principais conceitos ligados a ela.

1.2 SEGURANÇA DA INFORMAÇÃO

De acordo com Sêmola (2014), pode-se definir segurança da informação como:

Uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. (SÊMOLA, 2014, p. 41)

Conforme o Tribunal de Contas da União – TCU (2012), informação tornou-se um ativo importante para qualquer instituição. Uma informação adulterada, não disponível ou em posse de uma pessoa má intencionada pode comprometer uma instituição, tanto a sua imagem como o seu processo institucional. Por isso é importante zelar pela segurança da informação.

Os sistemas de informação facilitaram o acesso a informação e conseqüentemente as tornaram mais susceptível às ameaças. Desta forma, para promover a segurança da informação é necessário mais do que a implantação de equipamentos específicos, é necessária uma política que determine como empregar estes equipamentos e quem terá acesso ao sistema (DANTAS, 2011; CARVALHO, 2005).

De acordo com Dantas (2011, p. 117) “um sistema de segurança compõe todo um arcabouço de políticas, procedimentos, recursos humanos, tecnologia de suporte e infraestrutura necessários ao funcionamento das atividades voltadas para a segurança de uma organização”. Para prover segurança é necessário definir os requisitos de segurança. Os requisitos de segurança são importantes para identificar para o que está protegendo. Desta forma o sistema de segurança deve ser estabelecido de acordo com os controles que atendam

as condições levantadas (DANTAS, 2011).

Torna-se necessário a criação de uma política de segurança de informações, ou seja, um conjunto de normas que conduzem a gestão de segurança de informações. Estas normas mostram o que deve ser feito pela instituição para garantir seus recursos computacionais e suas informações (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

A política de segurança de informação serve de apoio e orientação para uma gestão de segurança de informações, onde para melhor compreensão devido a sua amplitude, é dividida em três partes principais (SÊMOLA, 2014):

- a) Diretrizes: tem papel estratégico e demonstra a importância que a instituição dá a segurança. Deve expressar as preocupações dos executivos e delimitar as linhas de ação que conduzirão as atividades táticas e operacionais.
- b) Normas: detalha ambientes, situações e processos específicos. Fornece instrução para o uso apropriado das informações.
- c) Procedimentos e instruções: deve descrever detalhadamente cada ação e atividade ligada a cada situação diversa de uso das informações.

Um sistema de gestão de segurança de informação é formado por requisitos responsáveis por sua implementação, operação e melhora, para isso a utilização de uma norma internacionalmente reconhecida como padrão trará maior confiabilidade além de proporcionar maior segurança. Desta forma, a adoção de uma ISO precisa de uma atenção especial para obter bons resultados (DANTAS, 2011).

Para que haja um sistema de gestão de segurança de informação capaz de proteger sistemas computacionais de ataques e invasões é necessário conhecer as tecnologias usadas para infringir políticas de segurança, ou seja, os tipos de ataques e as pessoas que as utilizam.

A informação está presente em todos processos de uma empresa, se tornando elemento determinante na tomada de decisões, podendo gerar lucros ou prejuízos.

A tríade da segurança da informação é baseada nos princípios da Confidencialidade, Integridade e Disponibilidade (GIAVAROTO; SANTOS, 2013).

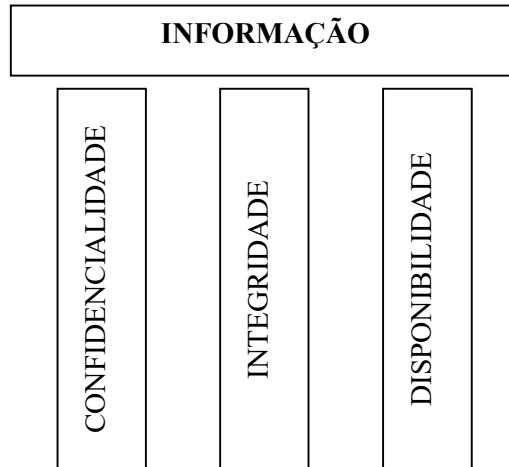


Figura 1. Princípios Básicos da Segurança da Informação

Fonte: (GIAVAROTO; SANTOS, 2013, p. 31)

- **Confidencialidade:** este princípio determina que somente pessoas autorizadas poderão acessar determinada informação. A confidencialidade é violada, quando alguma pessoa acessa uma informação, intencionalmente ou não, sem ter autorização (GIAVAROTO; SANTOS, 2013).
- **Integridade:** determinada informação será considerada íntegra, se estiver sem alterações. A informação perde sua confiabilidade, sendo adulterada intencionalmente ou não. Um aluno que tenta mudar sua média em um sistema de notas, é um exemplo de quebra de integridade (GIAVAROTO; SANTOS, 2013).
- **Disponibilidade:** este princípio define que a informação deverá estar acessível, para uma pessoa autorizada, sempre que for necessário. Um ataque de negação de serviço contra um servidor, é um exemplo de quebra de disponibilidade (GIAVAROTO; SANTOS, 2013).

A seção a seguir aborda as ameaças existentes e suas classificações.

1.2.1 Ameaças

Denomina-se ameaças todo agente ou condição que causem incidentes que venha a comprometer as informações através de vulnerabilidades, provocando a perda da integridade, confidencialidade e disponibilidade (SÊMOLA, 2014). Segundo Dantas (2011, p. 30)

“ameaças são agentes ou condições que, ao explorarem as vulnerabilidades, podem provocar danos ou perdas”. Estas perdas podem causar impactos desastrosos nos negócios.

As ameaças podem ocorrer por diversos motivos. Para entender melhor, Sêmola (2014) classifica as ameaças de acordo com suas intencionalidades, dividindo-as em três grupos:

- a) Naturais: são ameaças que tem a origem de fenômenos naturais, como enchentes, terremotos, tempestades e etc;
- b) Involuntárias: são ameaças não-intencionais, decorrentes de erros ou acidentes quase sempre causadas por falta de conhecimento;
- c) Voluntárias: são ameaças causadas com o objetivo de causar algum dano e são causados por agentes humanos como *hackers*, invasores, ladrões ou espíões.

De acordo com DANTAS (2011 apud *Módulo Security Solutions*, 2003), em sua 9ª Pesquisa Nacional de Segurança da Informação, as principais ameaças são as apresentadas no quadro a seguir.

Tabela 2. Principais ameaças

PRINCIPAIS AMEAÇAS	%
USO DE NOTEBOOKS	31
FALHAS NA SEGURANÇA FISICA	37
HACKERS	39
FRAUDES, ERROS E ACIDENTES	41
VAZAMENTO DE INFORMAÇÕES	47
ACESSOS LOCAIS INDEVIDOS	49
DIVULGAÇÃO DE SENHAS	51
FUNCIONÁRIO INSATISFEITO	53
VÍRUS	66

Fonte: (DANTAS 2011, p. 35-36 apud *Módulo Security Solutions*, 2003)

De acordo com a tabela apresentada, onde 682 respondentes apontaram quais os principais tipos de ameaças, deixa evidente que mesmo com políticas de segurança da informação, ainda há ameaças que exigem atenção. De acordo com a pesquisa, as ameaças de vírus e funcionários insatisfeitos estão à frente dos demais com 66 e 53% respectivamente, ou

seja, a maioria dos entrevistados consideram estes dois itens as principais ameaças à segurança da informação. É necessário compreender que as ameaças existem baseadas em vulnerabilidades existentes em sistemas de informação e aproveitando destas vulnerabilidades as ameaças provocam os incidentes. Na seção seguinte é apresentado os conceitos ligados a vulnerabilidades.

1.2.2 Vulnerabilidades

Vulnerabilidades para Sêmola (2014) são:

São fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. (SÊMOLA, 2014, p. 46)

As vulnerabilidades não provocam incidentes, as ameaças originadas destas fragilidades é que são responsáveis. As vulnerabilidades podem ser dos seguintes tipos (SÊMOLA, 2014):

- a) Físicas: instalações em ambientes sem regulamentação ou de acordo com as boas práticas como uso de extintores; controle de acesso defectivo em ambiente que possuem informações importantes e confidenciais;
- b) Naturais: equipamentos instalados próximo a locais sujeito a desastres naturais.
- c) Hardware: falhas causadas pelo uso, exposição ao tempo e componentes defeituosos;
- d) *Software*: erro de codificação, instalação ou configuração;
- e) Mídias: dispositivos de mídias e documentos que podem ser perdidos ou danificados;
- f) Comunicação: problemas nas infraestruturas de comunicação;
- g) Humanas: falta de treinamento ou de conscientização; verificação de antecedentes para verificar se a pessoa pode agir de má-fé.

Conforme pesquisa realizada pela *Módulo Security Solutions* (2003), os principais pontos identificados que estão ligados a vulnerabilidades e segurança da informação estão descritos na tabela a seguir:

Tabela 3. Vulnerabilidades da Segurança da Informação

Vulnerabilidades		
Pontos de Invasão	Sistemas internos	23%
	Internet	60%
Responsáveis	Prestadores de serviços	4%
	Funcionários	23%
	Hackers	32%
Obstáculos para a segurança da informação	Conscientização dos usuários	14%
	Conscientização dos executivos	23%

Fonte: (DANTAS 2011, p. 24-25 apud *Módulo Security Solutions*, 2003).

De acordo com a tabela apresentada, as empresas entrevistadas afirmam que a internet é o principal ponto onde ocorrem as invasões com 60%, mostrando que esta tecnologia ajudou no aumento de vulnerabilidades nos negócios. Sobre os responsáveis, a maioria afirma que são os *hackers* com 32% e os próprios funcionários 23%. Sobre os obstáculos enfrentados para a segurança da informação, a conscientização dos próprios executivos foi apontada pela maioria com 23% dos entrevistados.

Após compreender o que são vulnerabilidades e quais são seus tipos, deve ser tomado medidas para prevenir que incidentes ocorram. Para que haja esta prevenção, foram criadas ferramentas para auxiliar na segurança. Na seção a seguir serão apresentadas as ferramentas escolhidas para o presente estudo.

1.3. FERRAMENTAS DE AUDITORIA EM REDES DE COMPUTADORES

1.3.1 *Kali Linux*

O *kali Linux* é uma distribuição Linux baseada no Debian utilizado em testes de invasão e auditoria de segurança. O sistema operacional possui centenas de ferramentas

destinadas a operações de segurança da informação, tais como, teste de penetração, aplicações forenses e engenharia reversa (*KALI LINUX*, 2016).

O *Kali Linux* é financiado e mantido por *Offensive Security*, uma empresa especializada em treinamento de segurança da informação. Sua primeira versão foi lançada em 13 de março de 2013, substituindo o *BackTrack*, sistema também destinado a auditorias em redes. Também vale destacar que o *Kali Linux* é um sistema operacional de distribuição livre, ou seja, totalmente gratuito (*KALI LINUX*, 2016).

1.3.2 Metodologia do Teste de Penetração

Os testes de penetração são métodos utilizados para testar e descobrir vulnerabilidades em uma rede de computadores, ou sistemas operacionais. Durante o processo são analisadas e exploradas todas as possíveis vulnerabilidades.

O autor dos testes, ou *pentest*, utiliza métodos de avaliação em uma rede de computadores ou sistema, simulando ataques como se fosse um estranho mal-intencionado, determinado a invadir o sistema de computador. Tais testes possibilitam verificar a real estrutura do sistema alvo, onde são detectadas falhas em hardware e *software* que poderão ser corrigidas posteriormente (GIAVAROTO; SANTOS, 2013, p. 19).

Segundo Giavaroto e Santos (2013), os testes de penetração são de grande importância para as organizações que possuem sistema informatizados. Com as constantes mudanças de hábitos, devido ao avanço da tecnologia, além da grande disseminação de informações por mecanismos de pesquisas e a busca constante por retornos financeiros, faz com que muitas empresas instalem sistemas de computadores, sem critérios relacionados com segurança da informação.

Neste trabalho, os testes de penetração utilizados são definidos como *White box* (teste de caixa branca). Essa definição caracteriza que o agente de origem dos testes, possui total conhecimento da estrutura do sistema-alvo.

O *White box* executa teste reais em um ambiente de redes empresarial durante seu horário de expediente, ou quando ocorre vazamento de informações. Nesta situação, o invasor pode ter acesso a informações privilegiadas como diagrama da rede, endereços IP e informações sobre roteadores (GIAVAROTO; SANTOS, 2013).

1.3.3 Detecção de Sistemas Ativos (*PING*)

O *PING* é uma ferramenta básica, que geralmente é utilizada antes de qualquer outro teste e tem como objetivo a descoberta de *hosts* ativos na rede. Segundo Giavaroto e Santos (2013), o *PING* consiste no envio de pacotes ICMP_ECHO (tipo 8) e recebimento de mensagens ICMP_ECHO_REPLY (tipo 0).

1.3.4 HPING3

De acordo com Giavaroto e Santos (2013), a definição da ferramenta HPING3 é:

Um programa montador de datagramas para simular comunicações, a fim de testar a técnica SYN. Ele envia requisições de pacotes utilizando diferente tipos de *payloads* e *headers*. No caso, ele utiliza *libpcap* para operar conseguindo jogar pacotes através de filtros (GIAVAROTO; SANTOS, 2013, p. 38).

O HPING3 é uma ferramenta mais poderosa que o *PING* tradicional. Além de detectar *hosts* ativos é possível descobrir regras de *Firewall* e também executar varreduras de portas.

Durante a execução do HPING3, a ferramenta retorna um número maior de informações, se comparada ao *PING* normal. Ao estabelecer comunicação, o *software* exibe os valores presentes nos *flags*, que tem tudo a ver com *payload*. Quando é utilizado *Three-Way-handShake* na conexão TCP/IP, as portas do sistema retornam *flags* junto ao *payload*, definindo se elas estão abertas ou não para conexão (GIAVAROTO; SANTOS, 2013).

Valores do *flag*:

flag = SA significa disponível para conexão;

flag = RA significa indisponível para conexão.

1.3.5 DNSMAP

A função principal do DNSMAP, é a coleta de informações durante à avaliação de sistemas por *pentesters*. Durante a fase de enumeração, o auditor de segurança pode descobrir *netblocks*, nomes de domínios, números de telefones e outros dados da infraestrutura alvo.

A ferramenta DNSMAP é nativa do *Kali Linux* e sua primeira versão foi lançada originalmente em 2006 (*KALI LINUX TOOLS*, 2014).

1.3.6 NMAP

Um utilitário livre e *open source*, o NMAP é um *software* utilizado na descoberta de redes e auditoria de segurança. A ferramenta trabalho com pacotes IP brutos, verificando informações disponíveis na rede ou sistema alvo. Os resultados obtidos podem conter dados sobre nome e versão de serviços, nome e versão do OS (sistema operacional) e regras definidas em um *Firewall*.

O NMAP pode ser executado em todos os principais sistemas operacionais de computador. Seus pacotes binários oficiais estão disponíveis para *Linux*, *Windows* e *Mac OS X* (*KALI LINUX TOOLS*, 2014).

Segundo Giavaroto e Santos (2013), os métodos suportados pelo NMAP são:

- TCP SYN (-sS): examina portas de maneira rápida e indetectável. É um método mais difícil de ser descoberto pelo *Firewall*;
- TCP Connect (-sT): aplica a varredura utilizando o *Three-Way Handshake*, pode ser facilmente detectado;
- UDP (-sU): executa a varredura de protocolo UDP;
- TCP ACK (-sA): método utilizado para detecção de regras no *firewall*;
- TCP *Windows* (-sW): executa as varreduras por janelas, método parecido com o ACK, porém conseguiu detectar portas abertas versos filtradas e não filtradas.

1.3.7 Hydra

A ferramenta *Hydra* é conhecida por realizar quebras de senhas *online* e suportar vários protocolos para ataque. O utilitário possui um processamento rápido, além de permitir personalização dos métodos de ataques. O *Hydra* é utilizado por auditores de segurança da informação, demonstrando como é possível efetuar um acesso não autorizado, explorando vulnerabilidades dos sistemas (*KALI LINUX TOOLS*, 2014).

O *Hydra* suporta os seguintes protocolos: *Cisco AAA*, *Cisco auth*, *Cisco enable*, *CVS*, *FTP*, *HTTP(S)-FORM-GET*, *HTTP(S)-FORM-POST*, *HTTP(S)-GET*, *HTTP(S)-HEAD*, *HTTP-Proxy*, *ICQ*, *IMAP*, *IRC*, *LDAP*, *MS-SQL*, *MySQL*, *NNTP*, *Oracle Listener*, *Oracle SID*, *PC-Anywhere*, *PC-NFS*, *POP3*, *PostgreSQL*, *RDP*, *Rexec*, *Rlogin*, *Rsh*, *SIP*, *SMB(NT)*, *SMTP*, *SMTP Enum*, *SNMP v1+v2+v3*, *SOCKS5*, *SSH (v1 e v2)*, *SSHKEY*, *Subversion*, *Teamspeak (TS2)*, *Telnet*, *VMware-Auth*, *VNC* e *XMPP* (*KALI LINUX TOOLS*, 2014).

1.4. FERRAMENTAS PARA SEGURANÇA DA INFORMAÇÃO

Várias ferramentas e técnicas são utilizadas para detectar vulnerabilidades e prevenir contra possíveis ameaças. Existem ferramentas para prevenção e correção que são aplicadas de acordo com a política de segurança da informação. Para o presente estudo foi utilizado a ferramenta *Mikrotik RouterBoard*, sistema embarcado *Mikrotik* que será apresentado a seguir.

1.4.1 Mikrotik

A empresa *Mikrotik* criou em 1997 um sistema operacional baseado no *kernel Linux v2.6* nomeado *RouterOS*, sistema licenciado, *stand-alone* com diversas funcionalidades em redes de computadores, capaz de transformar um simples computador de arquitetura x86 em um poderoso roteador (LOPES, 2011).

Em 2002 a *Mikrotik* passou a fabricar placas compactas SBC (*Single Board Computer*)

com o sistema *RouterOS* adaptado para este hardware que foi denominado *RouterBoards* (LOPES, 2011; SILVA, 2012).

O sistema *Mikrotik RouterOS* possui as seguintes especificações de suporte de hardware (SILVA, 2012):

- a) Arquitetura compatível i386;
- b) Suporte a multiprocessamento;
- c) Mínimo de 32 MB de RAM e máximo de 2 GB de RAM;
- d) IDE, SATA, USB e flash como meio de armazenamento com o mínimo de 64 MB de espaço livre;
- e) Placas de rede suportadas pelo *Kernel Linux v2.6*.

O sistema *Mikrotik RouterOS* possui uma versão *DEMO* que libera todas as funcionalidades durante 24 horas que são contabilizadas durante o funcionamento do sistema, onde ao desligar, sua contagem regressiva é pausada até que o sistema seja novamente ligado. Após estas 24 horas, para que todas funcionalidades sejam novamente liberadas, será necessário inserir uma licença ou reinstalar o sistema, sendo obtida outra licença *DEMO* por mais 24 horas. A licença comercializada é de tempo ilimitado e permite que o sistema seja atualizado ou retroceder a sua versão durante 1 ou 3 anos de acordo com a licença adquirida. No caso, existem 6 níveis de licença onde cada uma possui características adicionais, sendo que, quanto maior o nível, maior o número de conexões permitidas. A licença está atrelada diretamente ao *RouterBoards* ou ao *drive* instalado, ou seja, trocando o *drive* uma nova licença deverá ser adquirida (SILVA, 2012).

O sistema pode ser administrado de três formas diferentes (LOPES, 2011):

- a) Local: configuração realizada no local através de console utilizando comandos;
- b) *WebBox*: configuração via navegador semelhante aos roteadores residenciais e também de fácil configuração;
- c) *WinBox*: ferramenta usada em plataforma *Windows* para administrar o sistema *RouterOS*.

A instalação do sistema é simples. O *download* pode ser feito diretamente no site da *Mikrotik*. A instalação pode ser feita por CD ou *Netinstall*, que ao ser iniciado abre uma tela para seleção dos pacotes que se deseja instalar. Após esta seleção o sistema é instalado e deverá ser configurado de acordo com a função destinada a ele (LOPES, 2011; SILVA, 2012).

Para uma política de segurança de informação eficiente, não basta apenas possuir uma ferramenta poderosa, é necessário definir diretrizes que irão assegurar isso. É indispensável o uso de boas práticas já reconhecidas para alcançar o resultado desejado. Devido a isso,

destaca-se na seção seguinte a ISO 27001, que apresenta normas para a implementação de um sistema de gestão de segurança da informação.

1.5 ABNT NBR ISO/IEC 27001

Em Sistemas de Gestão de Segurança da Informação, o padrão ISO é reconhecido internacionalmente e neste caso temos a ISO 27002 e a 27001. A ISO 27002 apresenta diretrizes e princípios gerais para um Sistema de Gestão de Segurança da Informação, já a ISO 27001 especifica os requisitos necessários para um Sistema de Gestão de Segurança da Informação documentado de acordo com os riscos de negócios de uma organização. Conclui-se então que enquanto a ISO 27002 apresenta um guia de boas práticas, a ISO 27001 apresenta itens obrigatórios para um Sistema de Gestão da Segurança da Informação (DANTAS, 2011).

Um Sistema de Gestão de Segurança da Informação baseado na ISO 27001 apresenta benefícios como políticas específicas para segurança da informação com controles baseados nos principais riscos em ambientes de negócios, conscientização sobre a segurança da informação, efetuação de ações de prevenção, correção e auditoria, além de utilizar uma norma conhecida internacionalmente (DANTAS, 2011).

A ISO 27001 possui 8 seções e um anexo normativo conforme descrito abaixo (ABNT, 2013):

- a) Objetivo: mostra o objetivo da ISO 27001 que é especificar requisitos para a implementação, operação, monitoração, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação;
- b) Referência normativa: referência a norma NBR ISO/IEC 17799: 2005 como indispensável para a aplicação da NBR ISO/IEC 27001;
- c) Termos e definições: apresenta os principais conceitos relacionados a ISO 27001;
- d) Sistema de gestão de segurança da informação: apresenta os requisitos necessários para um sistema de gestão de segurança da informação;
- e) Responsabilidade da direção: define o comprometimento da direção com o sistema de gestão de segurança da informação;
- f) Auditorias internas do ISMS: define o escopo das auditorias além dos métodos a serem utilizados;

- g) Revisão (análise crítica) do ISMS pela direção: determina a análise crítica realizada pela direção sobre o ISMS;
- h) Melhoria do ISMS: determina as ações preventivas e corretivas para melhoramento do ISMS;
- i) Anexo A – anexo normativo: tabela de controles conforme a ISO/IEC 17799:2005 considerado parte de um ISMS.

Com tudo, conclui-se que um Sistema de Gestão de Segurança da Informação se torna eficiente ao utilizar a ABNT ISO/IEC 27001. Sendo assim, esta norma foi adotada para o presente estudo. Nas seções seguintes, serão apresentados os métodos utilizados no desenvolvimento deste trabalho.

2. METODOLOGIA

2.1 OBJETIVO DE ESTUDO

O presente estudo foi realizado em uma concessionária de veículos da região de Caratinga-MG, onde nunca havia sido aplicado uma metodologia de segurança da informação, tornando-se 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 ao esquema que será apresentado.

A ABNT NBR ISO/IEC 27001 foi utilizada fornecendo recomendações que auxiliaram 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.

Fundada em 1979 a Minasvel Minas Veículos Ltda (Minasvel) é uma concessionária de veículos que trouxe para Caratinga a marca Fiat e seus carros. Em 2010 ocorreu a primeira certificação da empresa pelo IQA (Instituto de Qualidade Automotiva), após isso vem sendo re-certificada todos os anos. A Minasvel possui estrutura completa para vendas de veículos novos, acessórios, assistência técnica, balcão de peças e garantia.

O *software* de gestão de concessionárias de veículos (FIATNet) utilizado pela Minasvel, foi desenvolvido pela Monteiro Braga Informática Ltda (Dealernet). Fundada em 1990, a Dealernet se tornou ao longo dos anos uma das empresas líderes do mercado de DMS (*Dealer Management System*) no Brasil. Em 1994 foi lançada a primeira versão do sistema, sendo implantado inicialmente em 200 concessionárias Fiat. Atualmente a empresa possui mais 518 concessionárias Fiat utilizando seu sistema (DEALERNET, 2016).

Em 2005 a Fiat juntamente com a Dealernet realizou a migração dos sistemas das concessionárias para servidores *Windows*, que passou a executar o FiatNet, baseado numa arquitetura cliente/servidor com banco de dados relacional. As lojas que participaram da migração dos sistemas, tiveram um crescimento rápido de suas redes de computadores, isso aconteceu devido as novas funcionalidades que atenderam as demandas de todos os departamentos das concessionárias.

Apesar do FIATNet possuir controles bem definidos de permissões de usuários para o

acesso e processamento de informações, a rede de computadores em geral, tinha problemas que afetariam o funcionamento do sistema. A Minasvel nunca 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, foram destacados pontos críticos para a segurança da informação, onde a aplicação de uma política de segurança visando pessoas e tecnologia, se tornou muito importante para eliminação das ameaças às informações.

Para atingir o objetivo de promover a segurança da informação ao ambiente de rede de computadores da organização, primeiro foi necessário um estudo sobre Redes de Computadores e Gerência de Segurança, Segurança da Informação, *Mikrotik RouterOS* e ABNT NBR ISO/IEC 27001. Estes assuntos são primordiais para se definir uma metodologia voltada a segurança dos dados.

Após obter um conhecimento melhor sobre o tema, o próximo passo foi a análise dos processos internos da empresa. O objetivo desta etapa foi conhecer melhor cada departamento, as regras de negócio e os tipos de dados manipulados por cada usuário.

A rede de computadores da empresa também foi analisada com o objetivo de destacar vulnerabilidades que posteriormente seriam tratadas. Os pontos considerados foram segurança da rede *wireless*, servidores, desempenho no compartilhamento e transmissão de dados, roteadores e *switches*.

Depois de todo o levantamento de informações realizado na empresa, foram executadas as mudanças necessárias na rede de computadores com o intuito de eliminar as vulnerabilidades encontradas.

Por fim, houve a definição de uma política de segurança da informação que serviu para orientar e conscientizar os usuários. Essa política de segurança foi documentada e divulgada para todos os funcionários da organização.

2.2 AMBIENTE DE ESTUDO

Como a maioria das empresas, a Minasvel depende da sua rede de computadores e da internet para desempenhar suas atividades mais importantes. Cada setor da organização possui pelo menos um dispositivo conectado na rede. Obter o conhecimento de cada departamento e os sistemas utilizados foi de grande relevância no momento de definição das regras de

segurança, como por exemplo as permissões de acesso de um usuário. Com a análise do levantamento realizado, obteve-se uma boa visão dos processos da empresa. A mobilização e apoio da direção da empresa tornou-se um ponto importante para maior comprometimento com as devidas políticas, por parte de todos os colaboradores.

Grande parte dos problemas com a segurança da informação está relacionado com erros cometidos por usuários dos sistemas internos (NAKAMURA, 2007). Desta forma, todos que acessam ou trabalham com os dados da empresa, possuem suas responsabilidades para ajudar a manter a segurança em toda rede. Instruções de boas práticas de segurança podem contribuir para a diminuição destes problemas. Com isso, os usuários participaram de treinamentos e reuniões para orientação dos processos da política de segurança, assim, os usuários mais leigos puderam adquirir um conhecimento básico de boas práticas de segurança. Essa ação ajudou na eliminação de problemas relacionados com a internet, como por exemplo: identificação de e-mails falsos ou sites não confiáveis que, se acessados podem colocar em risco a segurança.

Foi de grande importância o conhecimento de como estão dispostos todos os dispositivos da rede e quais aplicações estão sendo executadas nos servidores, realizando um melhor gerenciamento. Inicialmente analisou-se toda a estrutura, equipamentos da rede de computadores do ambiente de estudo, onde foi revisto a necessidade de executar alterações buscando a melhoria. Após a análise, constatou-se que alguns equipamentos da rede como *Switches*, *rubs* e roteadores não estavam atingindo usabilidade satisfatória, com relação a taxa de transferência, desempenho e segurança. Equipamentos que trabalham com taxas de transferência 10/100 Mbps, apresentavam falhas em momentos de maior utilização no ambiente empresarial, diminuindo a segurança e causando insatisfação nas pessoas que utilizam os sistemas.

A rede de computadores possui um servidor de banco de dados *SQL Server 2008* rodando no sistema operacional *Windows Server 2008 Standard*. Também neste servidor está instalado o sistema de gestão de concessionárias *FiatNet* e *Clink* (CRM) que é utilizado por todos departamentos da organização. Antes da política de segurança, os dados não eram protegidos por um servidor de *Firewall* eficiente, além do *Firewall* nativo do *Windows Server* que estava desativado por motivos desconhecidos, colocando ainda mais em risco as informações da empresa.

Também pode ser visto na figura 2, a seguir, que a rede possuía somente um link de internet ADSL com velocidade de 5 Mbps. Logo após o modem ADSL, está um roteador convencional para compartilhamento da internet. Com este roteador não era possível

configurar serviços como *Firewall* com redirecionamento de portas ou um simples bloqueio de sites.

A rede *wireless* era utilizada para estender a conexão ao departamento de venda externa, que fica fisicamente mais distante das outras instalações da empresa, dificultando a passagem de cabos. Por ficar isolado dos outros departamentos e pelo motivo de serem poucos os equipamentos que se conectavam ao *Wifi*, não se dava a atenção necessária para a segurança da rede sem fio.

O roteador *wireless* não possuía nenhum tipo de senha, mas era necessário configurar o endereço IP manualmente no dispositivo que se conectasse a ele, permitindo acesso a rede interna da Minasvel. A rede *wireless* da empresa foi totalmente reestruturada, nos quesitos lógicos e também físicos. Essa parte da rede possuía uma falha crítica, pois se alguma pessoa tivesse conhecimento da classe de IP poderia acessar a rede facilmente. Tendo em vista esta situação, a rede *wireless* foi remodelada, adicionando novos roteadores de perfil empresarial, com a utilização de senhas fortes e criptografadas, além de filtragem por MAC.

Os pontos mais críticos da rede são os nós identificados nos *Switches0*, *Switches1*, *Switches2*. Se houver falha em um desses equipamentos, um departamento inteiro poderia parar de funcionar. Para prevenir que isso aconteça e uma ação ágil seja tomada, a empresa adquiriu 1 *Switch* reserva para uma substituição rápida caso necessário.

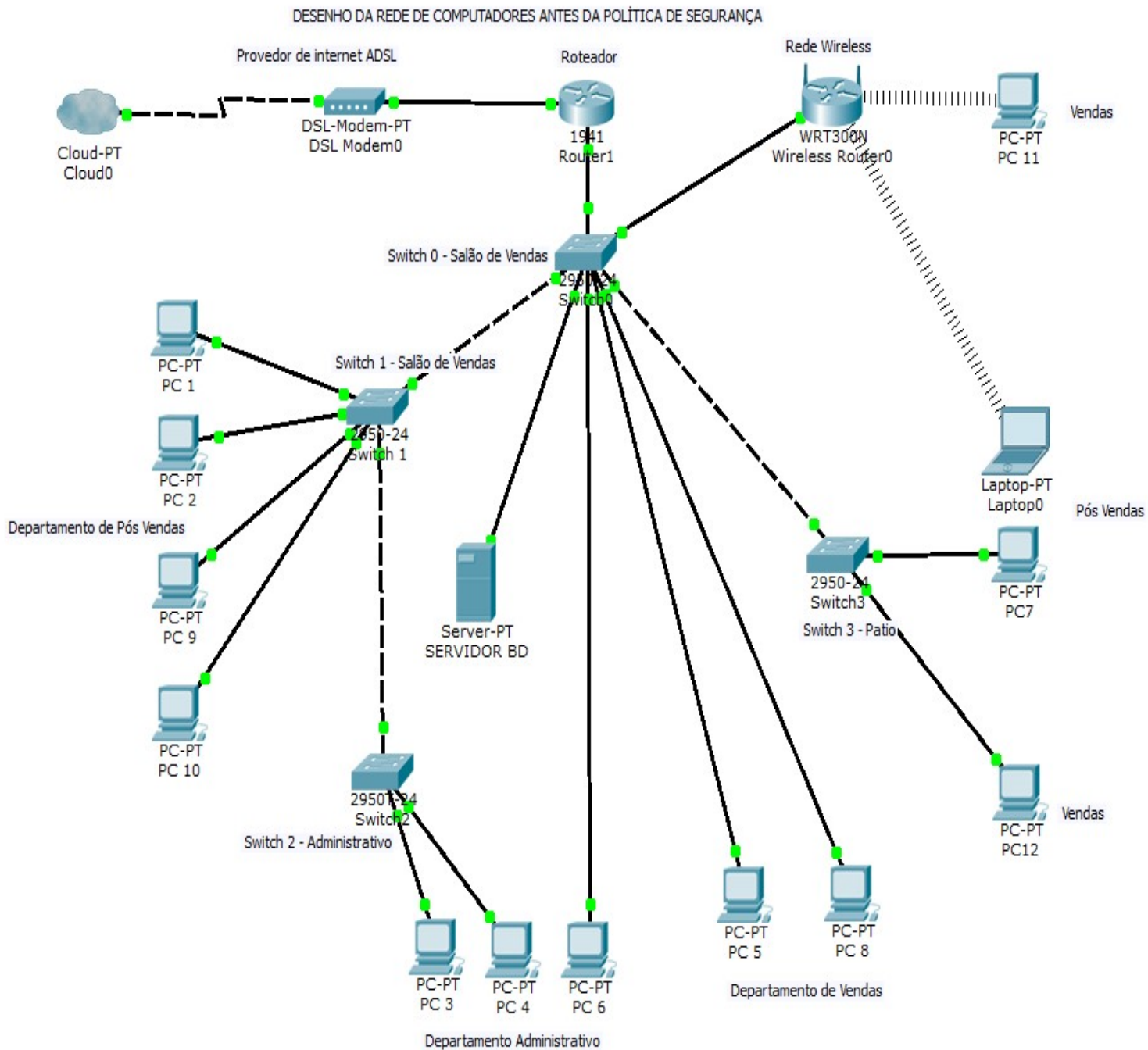


Figura 2. Desenho da rede de computadores antes da política de segurança

Fonte: Próprio autor

A configuração de um *Firewall* se torna ponto essencial neste trabalho. Foi configurado um *Firewall* no *Mikrotik RouterOS* versão 5.17 para bloquear o acesso as portas de conexão de serviços não utilizados pela empresa. O *Mikrotik* é um sistema operacional de roteamento (*RouterOS*) desenvolvido e mantido pela *Mikrotik Ltd*, empresa fundada na Letônia no ano de 1996. O *RouterOS* é baseado no Linux, possuindo baixo custo de aquisição

e permitindo a configuração de vários tipos de serviços como: servidor de *Firewall*, VPN, QOS, *Hotspot*, *Wireless AP*/cliente, *Proxy* e outros (MIKROTIK, 2016).

Para a liberação de portas no *Firewall*, foi utilizado redirecionamento para o equipamento ou serviço interno específico, essa ação aumentou o nível de segurança, pois a porta de conexão em questão não vai estar aberta para todos os dispositivos da rede. O acesso a conteúdo na internet foi restringido a assuntos específicos controlados pelas regras definidas no *Web Proxy*. Estes serviços também foram configurados no *Mikrotik RouterOS* versão 5.17. O *Web Proxy* funciona da seguinte forma: as requisições de conexão para a porta da internet do roteador são direcionadas para a porta definida no Proxy, onde é controlado qual máquina vai ter acesso liberado ao conteúdo da internet e qual vai ter acesso limitado. Para permitir melhor controle e organização das configurações, todos os dispositivos foram configurados com IP estático, facilitando a aplicação das regras e identificação dos *hosts* conectados na rede.

2.3 EXECUÇÃO DAS MUDANÇAS

2.3.1 Alterações nas Estruturas Físicas e Lógicas

Inicialmente, com as observações efetuadas no servidor de banco de dados da empresa, foi notado a necessidade de separar uma aplicação *web* que era executada no mesmo servidor. Essa aplicação *web* trata-se de um sistema interno chamado F&I (financiamentos e seguros) utilizado pelo departamento de vendas. Com a aplicação *web* sendo executado no mesmo servidor que o banco de dados, o risco a segurança das informações era maior, pois uma tentativa de invasão a aplicação *web* poderia prejudicar a disponibilidade do servidor de banco de dados. Com o intuito de sanar esta falha, foi necessário a aquisição de mais um servidor para uma instalação independente do sistema *web*. Com essa modificação, caso um dos servidores falhe o outro continuará funcionando normalmente, mantendo a disponibilidade dos serviços.

Analisando a necessidade da empresa, notou-se que a banda de internet contratada não estava sendo suficiente para manter um desempenho satisfatório. A internet utilizada era de um provedor que utiliza tecnologia ADSL e o plano contratado era de 5 Mbps. O *download*

de dados na internet com esse plano chegava a uma velocidade média de 580 Kbps e para upload era uma velocidade média de 48 Kbps. As reclamações de lentidão nas conexões com serviços *online* por parte dos usuários eram constantes, principalmente nos momentos de acessos simultâneos. A questão foi passada para a diretoria e como realmente havia a necessidade de contratação de um plano de internet melhor, a solicitação foi autorizada. O novo plano contratado com um provedor de internet a cabo é de 10 Mbps dedicados, atendendo perfeitamente as necessidades da organização.

Houve a necessidade de reposicionar algumas máquinas e equipamentos da rede de computadores para facilitar o gerenciamento. Os servidores foram trazidos para o departamento de TI, melhorando a segurança física dos mesmos. O *modem* do provedor de internet que ficava no departamento de vendas, também foi reposicionado para o departamento de TI. Com essas mudanças a manutenção desses dispositivos ficaram mais rápidas e com acesso direto do suporte técnico.

Para diminuir as falhas nos pontos mais críticos da rede, foram substituídos dois *Switches*. Um dos *Switches* com velocidade de transferência 10/100 Mbps ficava posicionado no departamento de TI e distribuía a conexão para os departamentos de vendas e administração. Para garantir o desempenho nas transferências dos dados e a segurança, foi adquirido um novo *switch* Dell 24 portas com taxas de transferência 100/1000 Mbps substituindo o antigo equipamento. O outro *Switch* de 8 portas com taxas de transferência 10/100 Mbps, ficava em uma área do pátio estendendo a conexão para a sala do SMD (sistema de medição diário). Houve a necessidade de substituição deste *Switch*, pois o mesmo apresentava perda de pacotes quando a carga de trabalho aumentava, causando muita lentidão naquele ponto da rede.

2.3.2 Política de *Backup*

O departamento financeiro é um ponto considerado crítico no desenvolvimento desta política de segurança. A empresa já sofreu com indisponibilidade de serviços causadas por falhas no sistema operacional e também de *hardware*. Tanto o computador do caixa, quanto o computador do administrativo financeiro, sofreram perda de dados que levaram dias para serem recuperados, sendo que outros tiveram que ser substituídos. Este tipo de problema além de demandar muito tempo para ser resolvido, possui custo maior, em relação a um plano de

prevenção.

Para solucionar e prevenir esse tipo de falha a empresa adquiriu unidades de armazenamento externo, permitindo *backups* diários dos computadores. É efetuado o *backup* das máquinas dos departamentos financeiro, recursos humanos, TI, contabilidade e fiscal. Além de salvar todos os arquivos e dados de aplicativos do usuário, também é criada uma imagem do sistema operacional, possibilitando uma restauração rápida no ponto do último *backup* realizado.

É importante ressaltar a política de *backup* implementada no servidor de banco de dados. São gerados três tipos de *backups* dos dados do servidor: o primeiro é o *FULL* que salva 100% dos dados (*backup* completo) e ocorre durante a noite; o segundo é o *DIFF* (diferencial) que ocorre 4 vezes durante o dia salvando as alterações feitas nos intervalos de tempo (a cada 4 horas); o terceiro tipo de *backup* é o LOG, que salva os logs de transações e ocorre a cada 30 minutos. Uma grande vantagem de se ter essa política de *backup*, está na possibilidade de restauração do banco de dados, no ponto em que foi realizado um dos *backups*.

A figura abaixo, exhibe os *backups* configurados nos planos de manutenção dos bancos de dados, na ferramenta *Management Studio*.

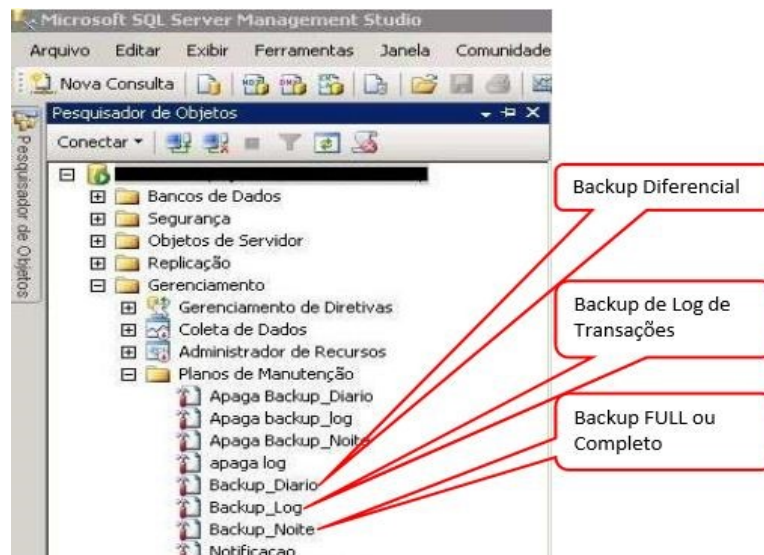


Figura 3. Planos de manutenção *Management Studio*

Fonte: Próprio autor

A quarta figura exhibe a configuração da ferramenta *backup* do *Windows*, onde são salvos os arquivos dos usuários e também uma imagem do sistema operacional.

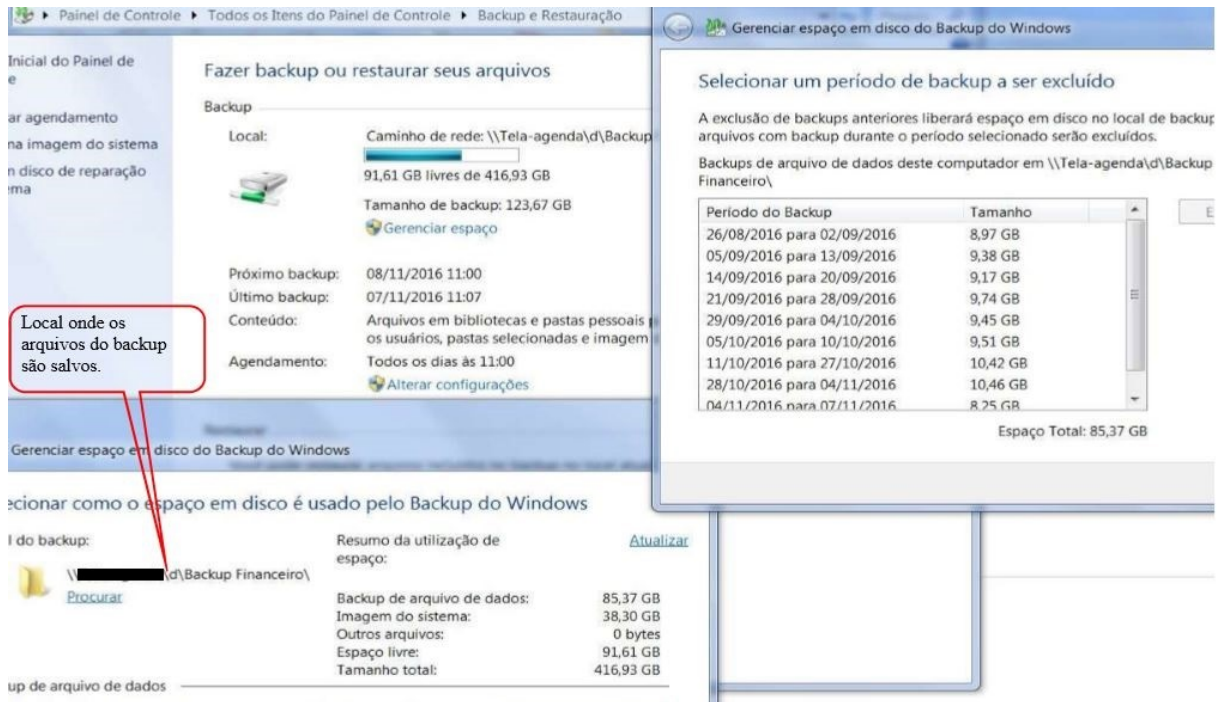


Figura 4. Backup do Windows

Fonte: Próprio autor

Como pode ser observado os arquivos são copiados todos os dias em um local de rede externo para garantir a segurança dos backups.

2.3.3 Proteção Contra Falhas de Eletricidade

Em relação a proteção contra riscos por faltas de energia elétrica, os servidores estão ligados em um *nobreak SMS Net Winner* de 1800VA com autonomia de até 80 minutos, o *Mikrotik Routerboard* e o computador onde é feita cópia dos *backups* já realizados, estão ligados em outro *nobreak SMS* de 1400VA. A cópia de segurança dos *backups* do servidor é realizada pela a rede durante a noite.

2.3.4 Mapa da Rede Após a Implementação

Na próxima figura é possível visualizar como ficou a estrutura da rede após realizar as modificações físicas e lógicas.

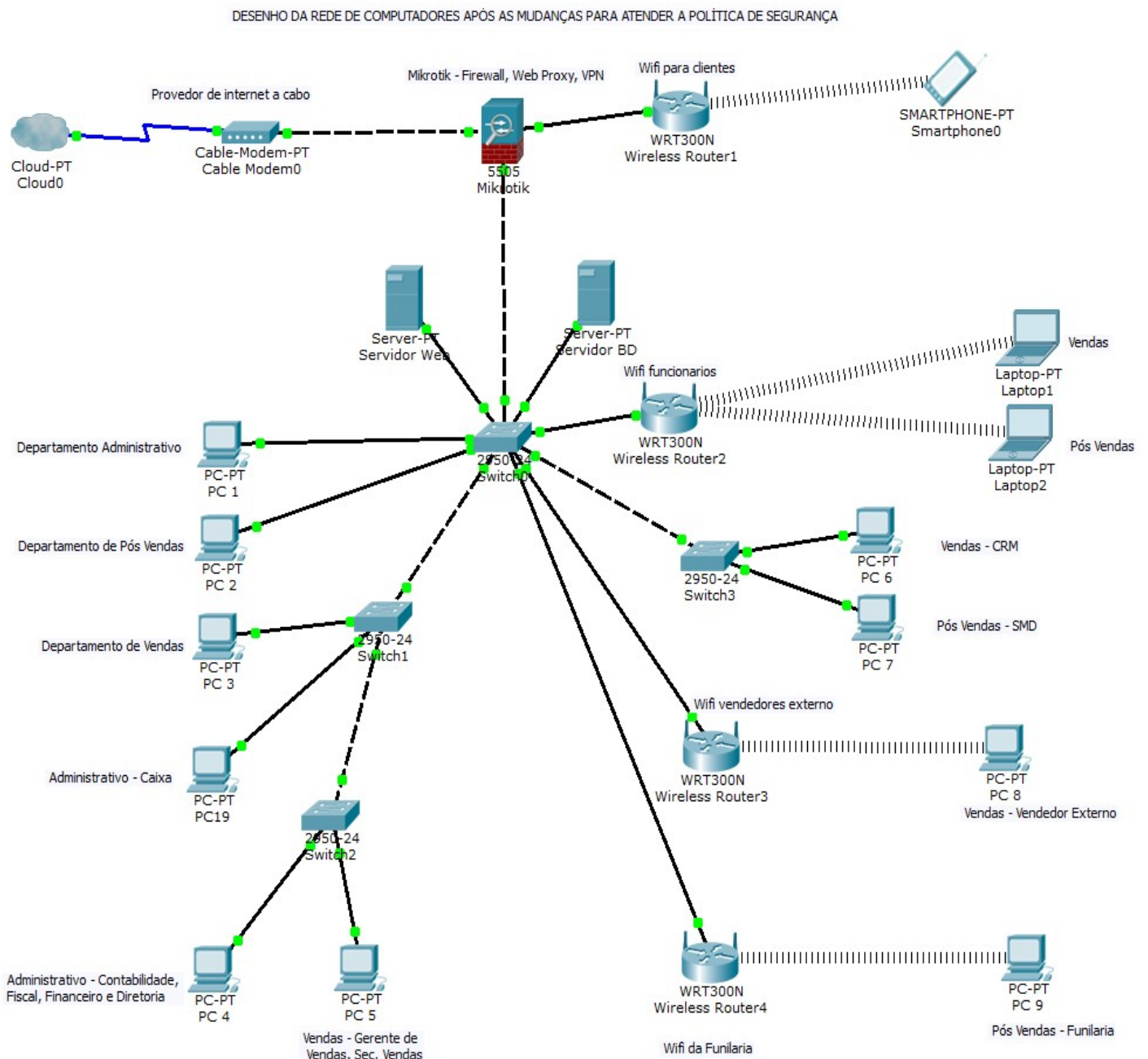


Figura 5. Desenho da Rede Computadores após a política de segurança

Fonte: Próprio autor

Como pode ser observado no desenho da rede, foi adicionado um novo roteador com conexão *wireless* para os clientes da empresa. Este roteador recebe sinal de internet por uma das interfaces do *Mikrotik Routerboard*. Cada interface funciona como uma placa de rede independente, pode-se imaginar como se fosse um servidor em torre, com 1 placa de rede *onboard*, mais 4 placas de rede *offboard* nos *slots* de expansão do servidor. Com isso, é possível criar sub redes independentes, onde uma não vai interferir na outra. Configurada

desta maneira, a rede *wireless* destinada para os clientes não oferece risco para os dados da empresa.

Foram adicionados mais dois roteadores *wireless* na rede interna, para conectar dispositivos da empresa utilizados pelos usuários no trabalho. A necessidade de adquirir esses roteadores veio com a substituição dos computadores do departamento de vendas por *notebooks*. Além dos vendedores, os mecânicos também possuem acesso ao sinal *wireless* do roteador identificado na figura anterior como *Wireless Router2*. No desenho da rede, o roteador identificado como *Wireless Router4* está configurado como repetidor, utilizando o sinal do roteador *Wireless Router2*. Neste roteador é conectado somente um computador, que foi adicionado na funilaria para realizar as marcações de tempo (tempo de mão de obra) de serviços executados, no sistema. Essa mudança foi executada para diminuir o tempo que os funileiros levavam para registrar seus serviços no sistema, pois eles tinham que ir até a oficina para utilizar os computadores dos mecânicos.

2.3.5 Segurança na Rede *Wireless*

O sinal *wifi* da sala de vendas externas, passou a ser usado somente pelos vendedores externos após a inclusão dos outros roteadores. Uma grande melhoria que vale ressaltar é que todas as redes *wireless* agora possuem senhas seguras, 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.

A figura abaixo demonstra a configuração do filtro de MAC de um dos roteadores. Os outros dois roteadores da rede interna foram configurados da mesma maneira, vinculado com o MAC dos respectivos dispositivos que se conectam a ele.

Filtro de Endereços MAC Wireless

SSID: default ▾

Filtro de Endereços MAC Wireless: Ativado Desativar

Regras de Filtro

Permitir os dispositivos sem regras habilitadas acessar a rede Wireless.

Negar os dispositivos sem regras habilitadas acessar a rede Wireless.

ID	Endereço MAC	Status	Descrição	Opções
1	██████████	Ativado	VENDEDOR EXTERNO 1	Alterar Excluir
2	██████████	Ativado	VENDEDOR EXTERNO 2	Alterar Excluir

Adicionar
Ativar Todos
Desativar Todos
Excluir Todos

Anterior
Próximo

Figura 6. Filtro de MAC dos roteados da rede wireless interna

Fonte: Próprio autor

Os filtros de endereços MAC estão definidos para negar a conexão de dispositivos que não estão informados na regra. Esta configuração melhorou 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 informado na lista do roteador.

2.3.6 Firewall

O ponto chave para a segurança da rede de computadores da Minasvel, foi a inclusão do *Mikrotik RouterOS* como *gateway* na estrutura, gerenciando todo o tráfego na rede. Como pôde ser observado na figura 5, são três conexões físicas no *Mikrotik RouterBoard*, ocupando 3 das 5 interfaces que ele possui. A primeira conexão vem do *modem* de internet a cabo, a segunda conexão compartilha a internet com a rede interna da empresa através *switch0* e a terceira *interface* está designada a compartilhar a *internet* para uma rede *wireless isolada*, destinada para uso dos clientes.

A seguir será demonstrado os procedimentos realizados durante a configuração do

Firewall no Mikrotik RouterBoard.

Primeiramente, para garantir maior segurança analisou-se todos os serviços utilizados dentro da empresa e as portas de conexão acessadas por cada um. As portas 1433 utilizada para conexão remota do *SQL Server* e 3389 utilizada para área de trabalho remota do *Windows* foram fechadas. Esses dois serviços eram utilizados para suporte remoto da empresa fornecedora do sistema *FiatNet* que acabaram sendo substituídos pelo *Teamviewer*. O *Teamviewer* é um *software* destinado a realização de acessos remotos pela rede interna ou externa e necessita de licenciamento para o uso empresarial. Sua metodologia de uso demonstrou maior segurança devido as conexões serem supervisionadas e a cada nova conexão uma nova senha ser gerada (TEAMVIEWER, 2016). Como não havia mais a necessidade de manter as portas 1433 e 3389 abertas, adicionou-se as seguintes regras no *Firewall*:

```
/ip firewall filter
```

```
add chain=input protocol=tcp dst-port=1433 action=drop comment="bloqueio da
porta SQLServer" disabled=no
```

```
/ip firewall filter
```

```
add chain=input protocol=tcp dst-port=3389 action=drop comment="bloqueio da
porta área de trabalho remota" disabled=no
```

Para melhor entendimento, será mostrado como funcionam os comandos acima nos tópicos a seguir.

- */ip firewall filter*: a primeira linha define onde os comandos vão ser executados, ou em qual serviço do *Mikrotik* serão definidas as configurações. Neste caso, como estão sendo adicionadas regras no *Firewall*, antes das definições devemos digitar: */ip firewall filter*. No caso de um menu gráfico seria respectivamente: *ip*→*firewall*→*filter*.
- *add chain*: nesta opção, é definido a necessidade de filtrar as entradas ou saídas. No exemplo anterior, definiu-se *input* (entrada).
- *protocol*: aqui é definido qual protocolo será utilizado.
- *dst-port*: nesta opção digita-se a porta de conexão que será bloqueada.

- *action*: nesta opção é configurado a ação que será executada para as conexões da porta definida. Pode ser utilizado *drop*, *accept*, *jump*, *log*, *reject* e outros.
- *comment*: opção onde pode ser acrescentado um comentário por questão de organização das regras no *Firewall*.
- *disabled*: defini se a regra vai estar ativa ou não. Valores *yes* ou *no*.

As regras e configurações dos serviços no *Mikrotik RouterOS* que serão demonstradas adiante, possuem a mesma lógica de configuração explicada acima.

Na figura abaixo é possível observar um exemplo de uma regra adicionada no *Firewall* através da interface gráfica *winbox*, qualquer outra porta pode ser fechada da mesma forma.

Figura da regra de bloqueio da porta de conexão 2000.

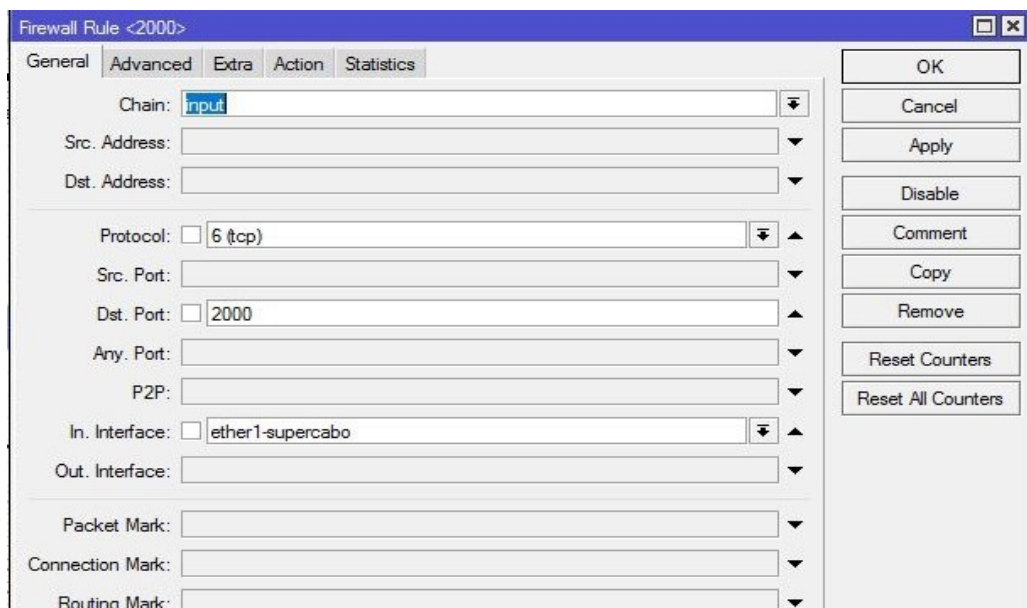


Figura 7. Regra do *Firewall* aba *General* *drop* porta 2000

Fonte: Próprio autor

Figura 8, regra de bloqueio da porta de conexão 2000 na aba *Action*. A ação definida para as conexões com essa porta foi o *drop*.

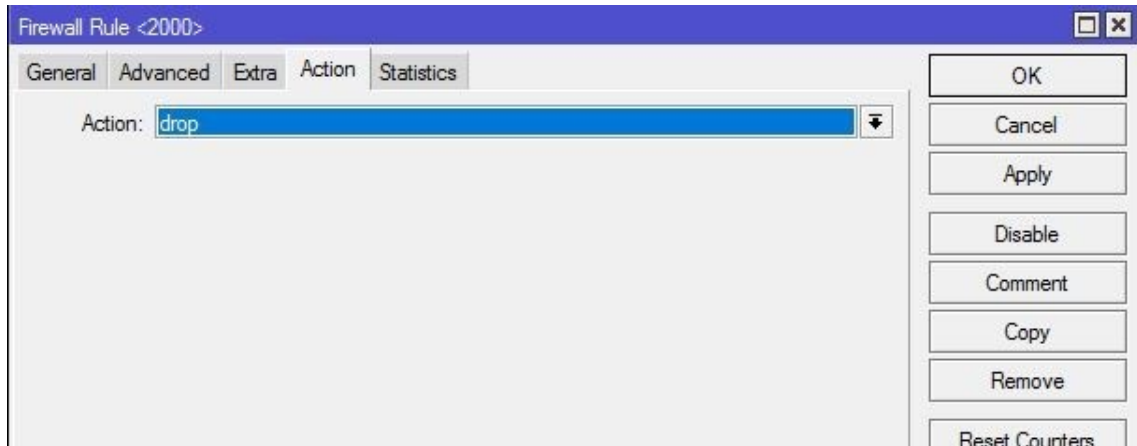


Figura 8. Regra do *Firewall* aba *Action drop* porta 2000

Fonte: Próprio autor

O *winbox* é um aplicativo que permite a administração do *Mikrotik RouterOS* usando interface gráfica. Pode ser executado nos sistemas operacionais *Windows*, *Linux* e *MacOS* (MIKROTIK, 2016). A conexão do *winbox* com o *Mikrotik RouterOS* pode ser estabelecida através do endereço IP ou do MAC utilizando usuário e senha.

A empresa também possui sistema de câmeras de monitoramento interno, onde as imagens podem ser visualizadas em computadores e dispositivos móveis. Para o funcionamento do aplicativo das câmeras foi necessário liberar acesso nas portas exigidas pelo fabricante do DVR *standalone* (*Digital Video Recorder*). Como as portas em questão são utilizadas somente pelo equipamento das câmeras de segurança, realizou-se um redirecionamento das mesmas, para o IP interno. Definindo a regra no *Firewall* desta maneira, obtém-se maior segurança, pois o acesso será realizado somente no dispositivo com o IP definido na configuração.

As regras do *Firewall* para conexão do sistema de câmeras ficaram da seguinte forma:

```
/ip firewall nat
add chain=dstnat protocol=tcp dst-port="número da porta de conexão" action=dst-nat
to addresses="IP de destino" to ports="número da porta de conexão"
comment="Conexão remota das câmeras" disabled=no
```

Neste caso, são três as portas de conexão necessárias para a visualização das imagens das câmeras remotamente. Deste modo, foi necessário executar os comandos acima três vezes. Em cada execução individual foram alterados somente os campos onde definimos as portas de conexão. O endereço IP de destino é sempre o mesmo, pois as portas estão sendo liberadas

para o mesmo dispositivo.

Abaixo pode ser observado a figura da regra definida no *winbox*. Configurações do *Firewall* na NAT.

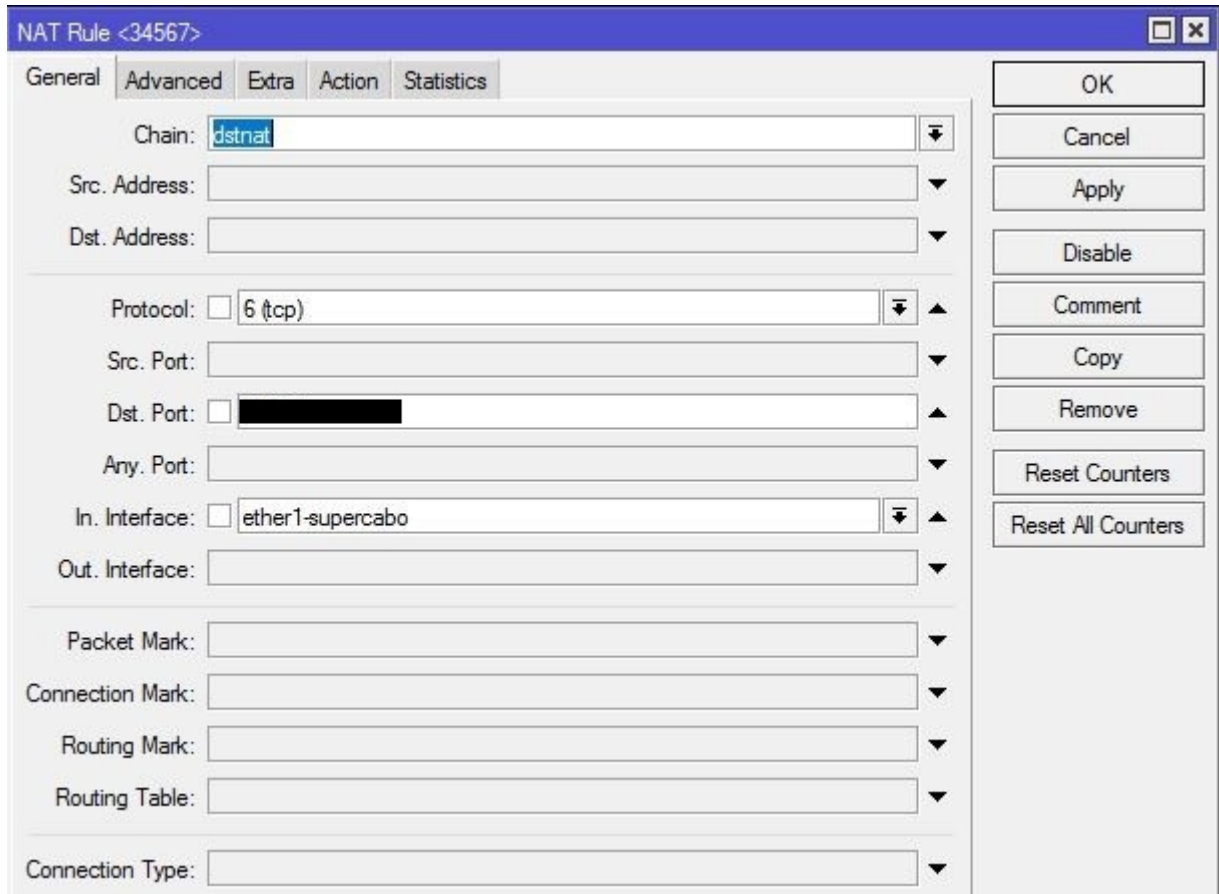


Figura 9. Regra do *Firewall* aba *General* redirecionamento por NAT

Fonte: Próprio autor

Figura 10, da aba *Action* onde o valor *dst-nat* define o endereço de destino *To Addresses* para a porta ou portas desejadas (*To Ports*).

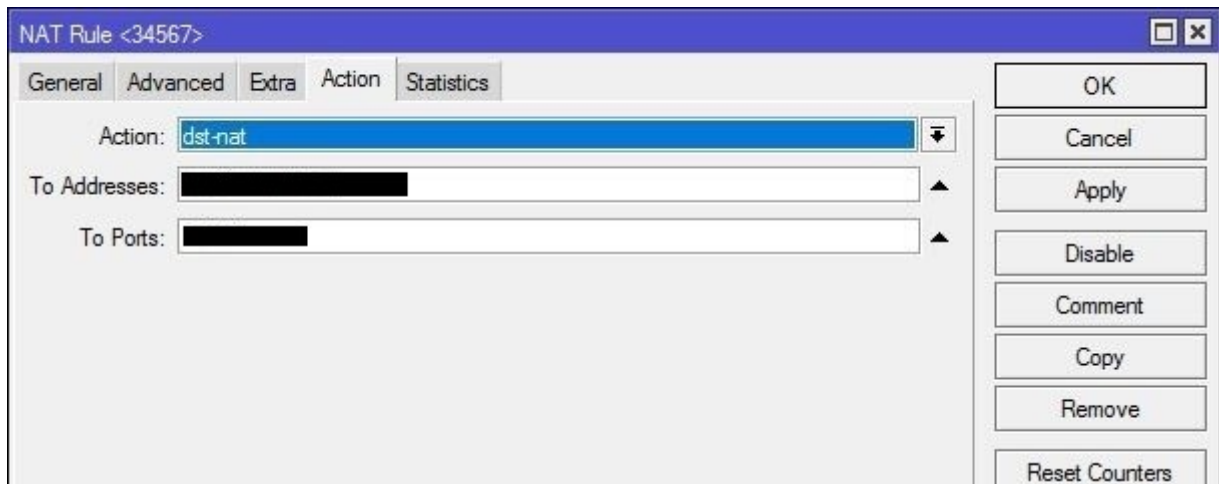


Figura 10. Regra do *Firewall* aba *Action* redirecionamento por NAT

Fonte: Próprio autor

Ainda nas configurações NAT do *Firewall*, foi necessário incluir algumas regras para o computador da Operadora de Seguros. Neste computador são executados alguns aplicativos das seguradoras, além de vídeo conferências que são realizadas com a concessionária. Para o correto funcionamento destes serviços, o departamento de tecnologia das seguradoras informa as portas que devem ser liberadas no *Firewall*. As portas solicitadas foram liberadas com redirecionamento para o computador da Operadora de Seguros.

As regras ficaram da seguinte forma:

```
/ip firewall nat
add chain=dstnat protocol=tcp dst-port="número da porta de conexão" action=dst-nat
to      addresses="IP de destino" to ports="número da porta de conexão"
comment="Portas liberadas para seguros" disabled=no
```

Para cada porta adicionada na regra do *Firewall*, foi necessário alterar somente os campos *dst-port* e *to ports*, o campo *to addresses* permanece com o mesmo valor, pois é o endereço para onde as portas foram apontadas.

Nas documentações do *Mikrotik RouterOS (Mikrotik wiki)*, existem procedimentos que orientam sobre implementações de regras no *Firewall*, que diminuem as chances de uma invasão. Um destes procedimentos é a inclusão de uma *blacklist* onde serão adicionados os IPs dos invasores. É possível editar a regra de forma que adicione o IP de origem dos ataques na *blacklist* após um determinado número de tentativas de acesso malsucedidas. O tempo que

os IPs inclusos na *blacklist* vão permanecer bloqueados é determinada pelo administrador de redes. Após a inclusão de um determinado IP na *blacklist* é possível estabelecer que o mesmo será bloqueado em conexões com qualquer tipo de serviço.

A próxima figura foi retirada da página *Mikrotik Wiki* e demonstra uma regra que pode ser configurada no *Firewall* onde é permitido apenas 10 tentativas de *login*. Neste caso, foi restringido o acesso a porta 21, que corresponde a serviços FTP.

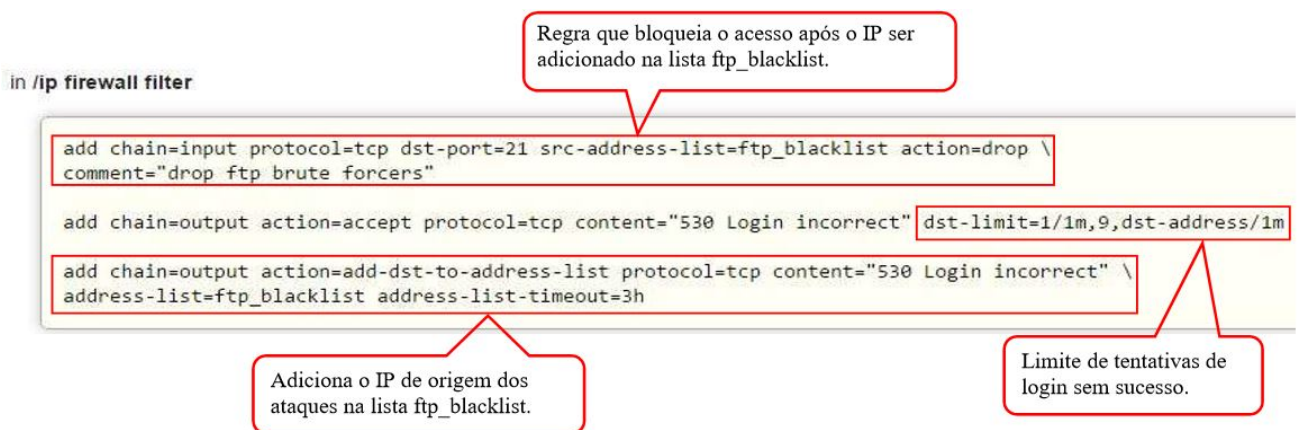


Figura 11. Regra que restringe *login* para serviços FTP

Fonte: (MIKROTIK WIKI, 2016, página. Prevenção de *login* força bruta)

Uma configuração similar a orientação documentada do *Mikrotik RouterOS* foi executada no *Firewall* da concessionária. Foram selecionadas algumas portas definidas pelo administrador da rede de computadores com base nas tentativas de acesso. Ao tentar acessar essas portas o endereço IP proveniente dos ataques é adicionado em uma lista chamada *hacker*. Os endereços IP inclusos na lista *hacker* vão ficar bloqueados por 90 dias, mas nesta configuração basta apenas uma tentativa de acesso para a inclusão na *blacklist*.

Como nas outras regras do *Firewall*, esta também foi definida em IP *Firewall* e configurada na aba *Filter Rules*. Os comandos para inclusão da regra ficaram da seguinte forma:

```

/ip firewall filter
add action=add-src-to-address-list address-list=hacker address-list-timeout=90d
00:00:00
chain=input comment="Bloqueia IPs que tentarem acesso" disabled=no
dst-port="porta de destino" in-interface="interface de internet" protocol=tcp
  
```

Esta regra define a lista *hacker* que pode ser visualizada na aba *Address Lists* do *Firewall*. Quando alguém tenta conexão na porta informada no campo *dst-port* (acesso direto ou um *scanner* de rede) seu IP é automaticamente incluído na lista *hacker* pela ação *add-src-to-address-list*, ou seja, adicionar o endereço IP de origem do ataque para a lista. Essa regra pode ser adicionada quantas vezes for necessário, modificando somente as portas de conexão necessárias.

Uma vez adicionados na *blacklist* do *Firewall* é necessário definir a ação que deve ser aplicada nos IPs que tentaram acessar o sistema. A seguinte regra define que todos os IPs inclusos na lista *hacker* vão receber a ação *drop*.

```
/ip firewall filter
add action=drop chain=input comment="Drop IPs da lista hacker"
disabled=no src-address-list=hacker
```

Para as regras acima não existem limites de tentativas de conexão com o servidor, qualquer tentativa de acesso pelas portas de conexão vai caracterizar bloqueio para o IP de origem do acesso. Se caso for necessário criar uma regra com o intuito de prevenir tentativas excessivas de *login*, em uma porta utilizada por algum serviço, deverá ser definido um limite conforme a figura 11, mostrada anteriormente.

2.3.7 Web Proxy

Os exemplos específicos mostrados anteriormente tiveram tratamento nas regras do *Firewall* do *Mikrotik RouterOS*, tornando possível permitir e negar conexões com maior facilidade para computadores dentro da rede, em casos onde um tipo de serviços é executado em apenas uma determinada máquina.

A seguir serão mostradas as configurações implementadas no *Web Proxy* do sistema operacional de roteamento, onde as regras afetam todos os terminais da rede de computadores.

Conforme as regras internas da empresa, ficou determinado que para proporcionar maior segurança e produtividade dos usuários, deveria ser implementado de alguma forma um meio que permitisse acesso a conteúdo na internet somente quando fosse relacionado com atividades do trabalho.

O *Mikrotik RouterOS* permite a configuração do *Web Proxy*, onde é possível controlar as conexões através de domínios, URL completa, portas de conexão ou até mesmo por palavras. Ao habilitar o *Web Proxy*, é necessário definir uma porta por onde passará o tráfego de conexões da internet. No *Firewall*, foi necessário incluir uma nova regra na aba NAT, direcionando as conexões da porta da internet para a porta definida no *Web Proxy*. Com essa configuração, todas as solicitações de saída para a internet são forçadas a passarem pelo *Proxy*. Após as configurações supracitadas, retorna-se a aba *Filter* no *Firewall*, onde foi incluído a regra aceitando as conexões vindas do *Web Proxy* na rede interna (MIKROTIK, 2016).

A seguir será demonstrado como foram realizadas as configurações descritas acima, com os comandos utilizados no terminal do sistema *Mikrotik* e também utilização da interface gráfica.

Na figura 12 é demonstrada a tela do *Web Proxy*, que fica localizada no menu IP *Web Proxy*. É nesta tela que é habilitado o serviço do *Proxy* e definida a porta do mesmo.

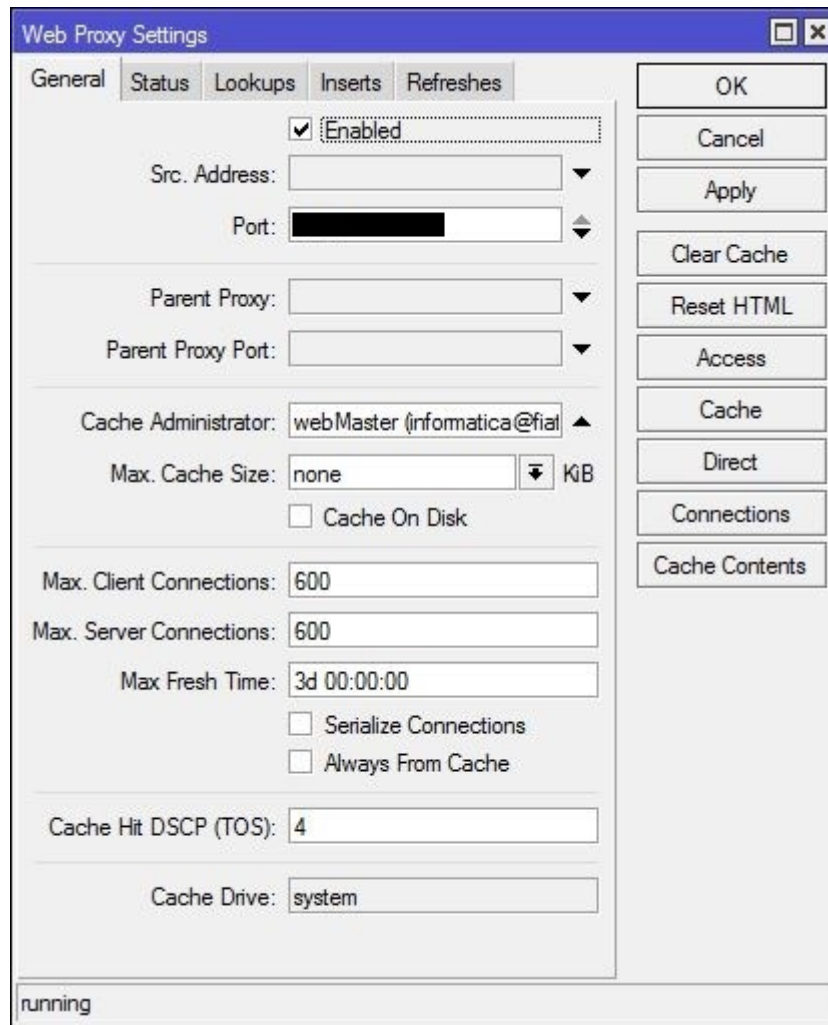


Figura 12. Configurações do *web proxy*

Fonte: Próprio autor

Como pode ser observado, basta selecionar o *checkbox Enabled*, aplicar e o *Web Proxy* já estará em funcionamento. O campo *Port* é onde foi informada a porta que recebera as conexões da internet. As outras configurações são executadas de maneira a atender melhor a cada situação, como por exemplo, os campos *Parent Proxy* e *Parent Proxy Port* que se configurados, o Proxy deixaria de ser transparente (MIKROTIK, 2016).

No próximo passo, será demonstrado o comando que foi executado para criar a regra que direciona a porta da internet para o Proxy.

```
ip firewall nat
add chain=dstnat protocol=tcp src-address="rede interna"
dst-port="porta da internet" In.Interface="interface da rede local"
action=redirect to-ports="porta definida no Web Proxy"
```

Nos filtros do *Firewall* a regra que vai permitir o tráfego do *Proxy* na rede local foi definida com os seguintes comandos.

```
ip firewall filter
add chain=input protocol=tcp src-address="rede interna"
dst-port="porta do Web Proxy" In.Interface="interface da rede local" action=accept
```

Observando os comandos acima é importante destacar que o campo *src-address* deve ser preenchido com o endereço da rede interna (ex: 192.168.0.0/24), que inclui todos os IPs disponíveis. Ou também pode ser informado apenas um *pool* de IPs determinados. O campo *dst-port* é onde foi informada a mesma porta definida no *Web Proxy*.

Com essas definições atribuídas no *Proxy*, foi possível controlar muito bem o conteúdo acessado *online* pelos os usuários da empresa. As configurações citadas anteriormente, foram primordiais no momento de aplicação da política interna de acesso e utilização da internet. A partir desta implementação foi possível controlar os sites e sistemas utilizados e também restringir o *download* de certos tipos de arquivos.

Os parágrafos a seguir vão explicar como são feitos os controles de liberação e bloqueio dos sites ou serviços acessados *online*. Também será mostrado a eficácia das políticas definidas nas configurações do *Web Proxy*.

Antes de mais nada, é necessário enfatizar sobre o modo com que o *Mikrotik* trata as regras adicionadas em seus serviços. Quando são incluídas novas regras na tabela *Access* do *Web Proxy* por exemplo, elas vão para o final da lista, onde a prioridade é menor. As regras que ficam acima ou no topo tem prioridade, ou seja, se for colocado uma regra que bloqueia determinado site e acima desta regra é adicionada outra regra liberando acesso para um determinado IP da rede, esse IP terá acesso e o restante da rede ficará com o acesso bloqueado.

A seguir, a figura 13 possui detalhes de algumas regras para o melhor entendimento de como é o funcionamento do *Proxy* para o controle de navegação na internet.

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits
8	● [redacted]						allow		34261
9	● [redacted]						allow		2463
10	● [redacted]						allow		13825
11	● [redacted]						allow		100395
12	● [redacted]						allow		602415
BLOQUEIA DOWNLOAD DE ARQUIVOS									
13	●				*.flv		deny		0
14	●				*.avi		deny		0
15	●				*.mp4		deny		0
16	●				*.mp3		deny		0
17	●				*.zip		deny		0
18	●				*.rar		deny		0
19	●				*.exe		deny		0
SEC-DEALER									
20	● [redacted]						allow		21017
SITES LIBERADOS									
21	●			*google.com*			allow		35610
22	●			*carros.com.br*			allow		4135
23	●			*ipe.org.br*			allow		3593
24	●			*receita.fazenda.gov.br*			allow		2517
25	●			*skype.com*			allow		1156
26	●			*correios.com.br*			allow		1267
27	●			*contabeis.com.br*			allow		1133
28	●			*nfe.caratinga.mg.gov.br*			allow		2198
29	●			*fazenda.sp.gov.br*			allow		628
30	●			*coad.com.br*			allow		581

Figura 13. Regras do *Web Proxy Access*

Fonte: Próprio autor

Para bloquear todas as conexões e liberar somente os sites permitidos, foi criado primeiramente a seguinte regra no *Proxy*.

```
/ip proxy access
```

```
add action=deny comment="BLOQUEIO GERAL" disabled=no
```

```
dst-port=0-65535
```

Como demonstrado, o campo *dst-port* recebeu o valor 0-65535 que é o intervalo de todas as portas e a ação para as mesmas foi *deny*, que bloqueia todo o acesso na internet. Esta ação também pode ser realizada adicionando o valor 0.0.0.0/24 no campo *dst address* (ip de destino) onde qualquer faixa de IP não poderá ser acessada. Após criar a regra de bloqueio, para executar a liberação de algum site, basta adicionar uma nova regra no *Proxy Access* e posicioná-la acima da regra de bloqueio. Para liberar o acesso total na internet para algum computador da rede, basta criar uma regra informando o IP do equipamento no campo *src address* (ip de origem) com a ação *allow* no *Proxy Access* e posicioná-lo no topo da lista de

regras.

A próxima figura mostra as configurações das regras supracitadas, só que na interface do *winbox*. Vale lembrar, que para o correto funcionamento elas devem estar posicionadas de forma adequada na lista de regras do *Web Proxy*, pois são processadas do topo para a base.

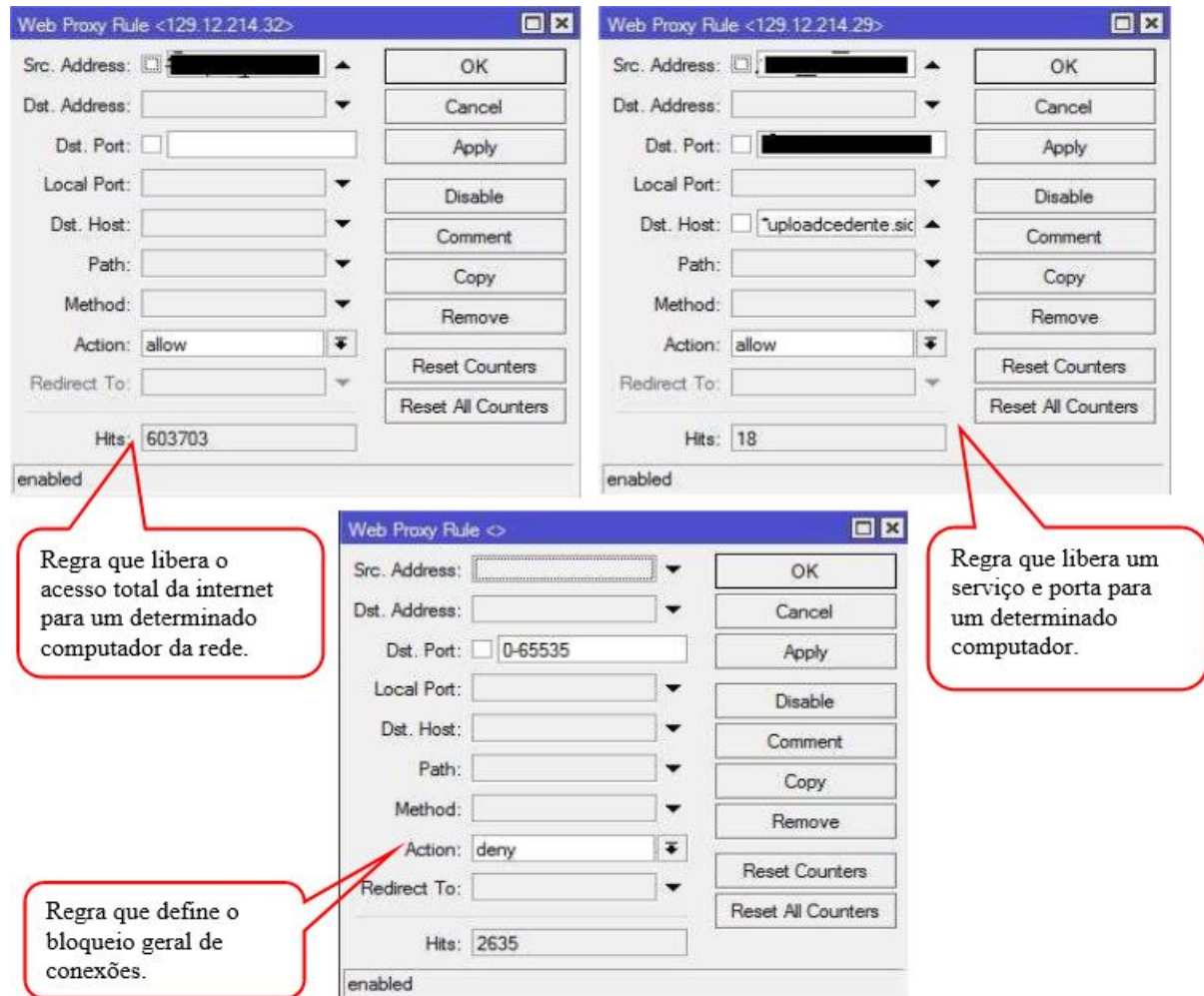


Figura 14. Regras do *web proxy* liberações e bloqueios

Fonte: Próprio autor

2.3.8 Rede Privada Virtual

A concessionária conta com vendedores externos que atendem em outros municípios vizinhos, além de eventos de exposição de veículos que ocorrem na região. Mesmo estando fora da concessionária os vendedores precisam ter acesso às informações do banco de dados, como cadastro de clientes e estoque de veículos.

Para proporcionar uma conexão segura entre os usuários que estão fora da empresa e o sistema interno, foi configurada uma VPN (*Virtual Private Network*) no *Mikrotik RouterOS*.

O sistema operacional de roteamento possui as opções de servidor PPTP (*Point to Point Tunneling Protocol*) e cliente PPTP. Com essas funcionalidades podem ser interligadas duas redes geograficamente distantes através de uma conexão criptografada com protocolo PPTP. Segundo o manual da *Mikrotik*, PPTP é um túnel seguro para transporte de tráfego IP usando PPP (*Point to Point Protocol*). PPTP inclui PPP e MPPE (*Microsoft Point to Point Encryption*) para fazer conexões encriptadas. O objetivo deste protocolo é fazer uma conexão segura entre roteadores ou clientes PPTP. No caso do sistema operacional *Windows*, é possível configurá-lo como um cliente adicionando uma nova conexão VNP nas configurações de rede (*MIKROTIK, 2016*).

A configuração a seguir mostrar como é feita a ligação de um computador remoto a uma rede interna.

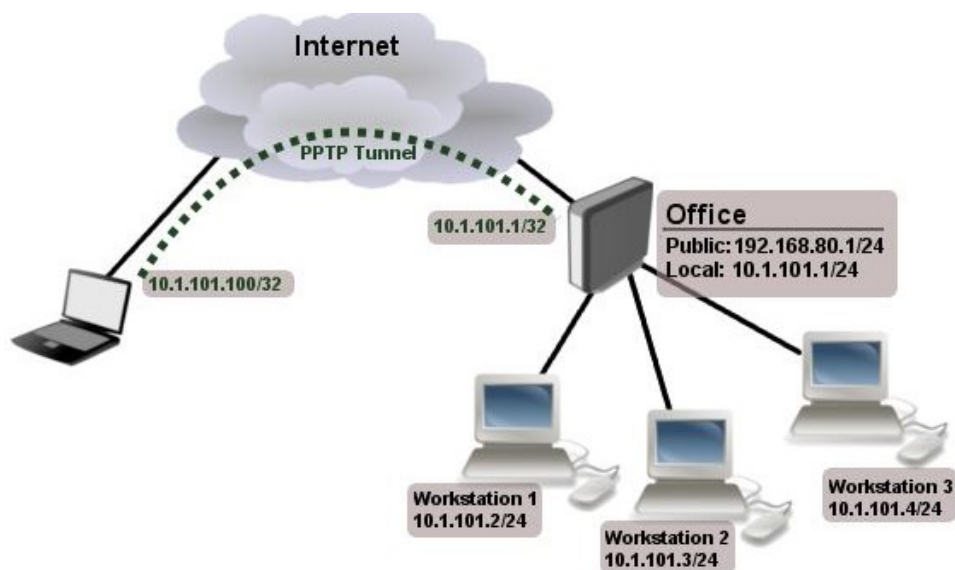


Figura 15. Modelo de um tonel PPTP

Fonte: (*MIKROTIK DOCUMENTATION, 2016, p. Interface / PPTP*)

Para realizar a configuração mostrada na figura 15 foi preciso habilitar o servidor PPTP no menu PPP do *winbox* da seguinte forma:

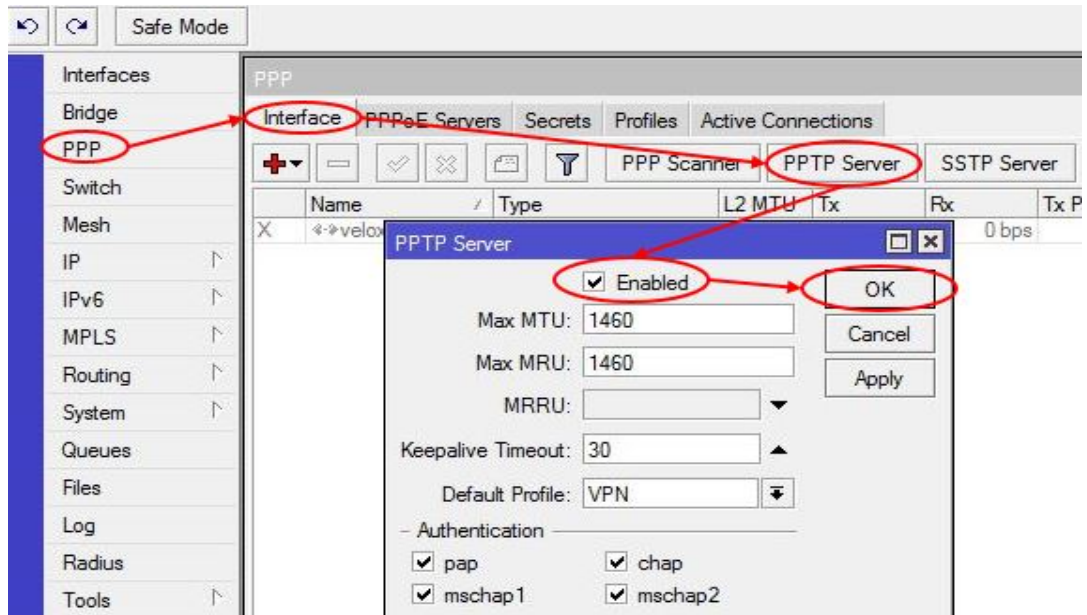


Figura 16. Servidor PPTP

Fonte: Próprio autor

Após a ativação servidor PPTP no *Mikrotik RouterOS* é necessário criar os usuários seguros que vão autenticar no serviço remotamente. A inclusão de novos usuários é executada na aba *Secrets* do menu PPP, a configuração é realizada conforme mostra a figura abaixo:

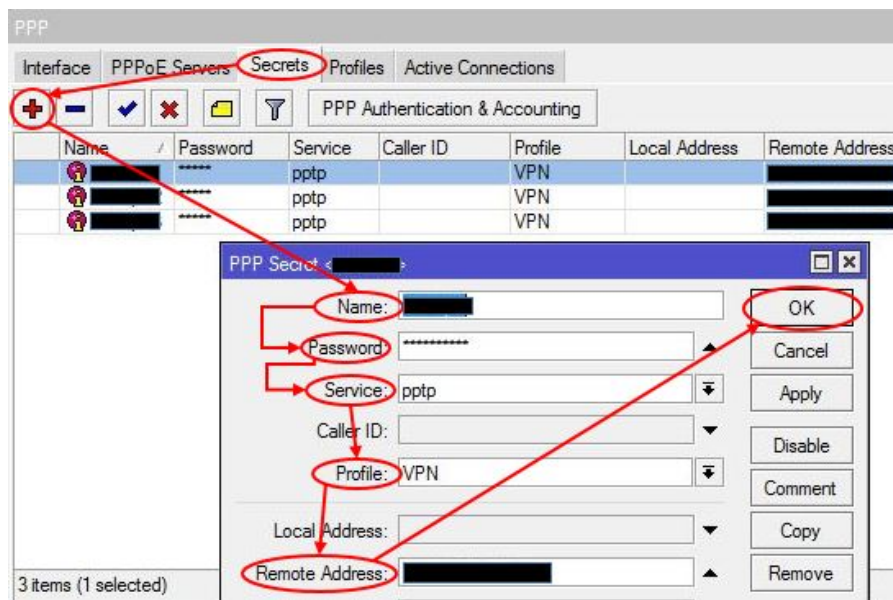


Figura 17. Inclusão de usuários no servidor PPTP

Fonte: Próprio autor

Ainda na janela PPP é possível acessar a aba *Secrets* e clicar do botão com sinal + (mais). Neste caso, uma nova janela *PPP Secret* é aberta onde se informa os dados do usuário

como: nome, senha, serviço, perfil e um endereço IP disponível da rede interna.

Com essas configurações definidas no sistema *Mikrotik* a concessionária passou a ter uma conexão segura com seus funcionários que trabalham externamente. Como o sistema operacional dos notebooks é *Windows*, basta adicionar uma nova conexão nas configurações de rede e defini-la como VPN. Nas definições da nova conexão deve ser informado o usuário e senha criados no *Mikrotik RouterOS*, também é necessário disponibilizar o endereço IP a nível WAN (IP quente) da concessionária ou o nome de um cliente DNS. O usuário não tem conhecimento sobre essas configurações em seu computador e a senha fica criptografada no sistema. Com acesso à internet, basta o usuário clicar em um botão e uma conexão segura entre seu terminal e a rede da concessionária será estabelecida.

2.3.9 Antivírus e Monitoramento

É indispensável para aumentar o nível da segurança um bom antivírus que ajude a manter *malwares* (*software* nocivo ou *software* malicioso) e *links* suspeitos distantes. A concessionária adquiriu o *Avast for Business*, sendo um sistema nas nuvens com segurança *endpoint* com um painel de gerenciamento de fácil utilização. Com o *Avast for Business* a empresa passou ter antivírus em seus sistemas clientes e também nos servidores de forma integrada. Através de um console que pode ser acessado remotamente, o administrador pode visualizar todos os dispositivos com o *Avast for Business* Antivírus instalado, além de ler notificações dos status atuais dos sistemas. A versão mais básica do sistema (*Avast for Business Basic* Antivírus) pode ser utilizada pelas empresas gratuitamente.

Para apresentar algumas funcionalidades do antivírus para empresas, serão descritos alguns tópicos que foram retirados da página do *Avast Business*. Por meio do console do sistema é possível, (AVAST, 2016):

- Acesso ao sistema pelo navegador com controle completo sobre o comportamento do antivírus em dispositivos *endpoint*;
- Gerenciamento centralizado de múltiplos dispositivos acessível de qualquer lugar;
- Visão geral completa do atual estado do ambiente com alertas imediatos;
- Acesso imediato ao suporte com chat dentro do produto;
- Atualizações automáticas.

Os pontos listados acima são características do *Avast for Business*. Os próximos pontos descritos são referentes ao *Avast for Business Antivírus*, ou seja, características do *software* antivírus instalado nos dispositivos da empresa (AVAST, 2016).

- Utiliza virtualização para garantir que informações confidenciais estão protegidas;
- Protege múltiplas plataformas PCs, Macs e servidores;
- Atualiza para a versão mais recente automaticamente ou manualmente;
- Adiciona proteção *firewall* extra para *endpoints* remotos;
- Oferece proteção completa para servidores;
- Protege e-mail cliente.

Todos os computadores clientes e servidores da empresa tem o antivírus *Avast* instalado e gerenciado pelo console *online*. O console permite ao administrador monitorar a rede de dispositivos inclusos no sistema, além de criar tarefas para toda a rede de uma só vez, como por exemplo: *updates* da base de dados de vírus e do programa, agendar escaneamentos de vírus personalizados, enviar mensagens para os aparelhos, desligar ou reiniciar os aparelhos.

Ao acessar o sistema, logo na tela inicial pode ser observado se existe algum dispositivo com problemas. Também podem ser vistas informações em gráficos sobre estatísticas de detecção de ameaças, último escaneamento executado e quantidade de aparelhos conectados.

O administrador da rede fica atualizado sobre todas ameaças detectadas dentro da organização, tornando uma ação preventiva mais rápida. As notificações sobre ameaças detectadas, *softwares* desatualizados ou módulos do antivírus desativados são enviadas diretamente no e-mail do responsável pela rede de computadores.

A figura 18 mostra como é o painel de controle do *Avast for Business* e como são exibidas as notificações:

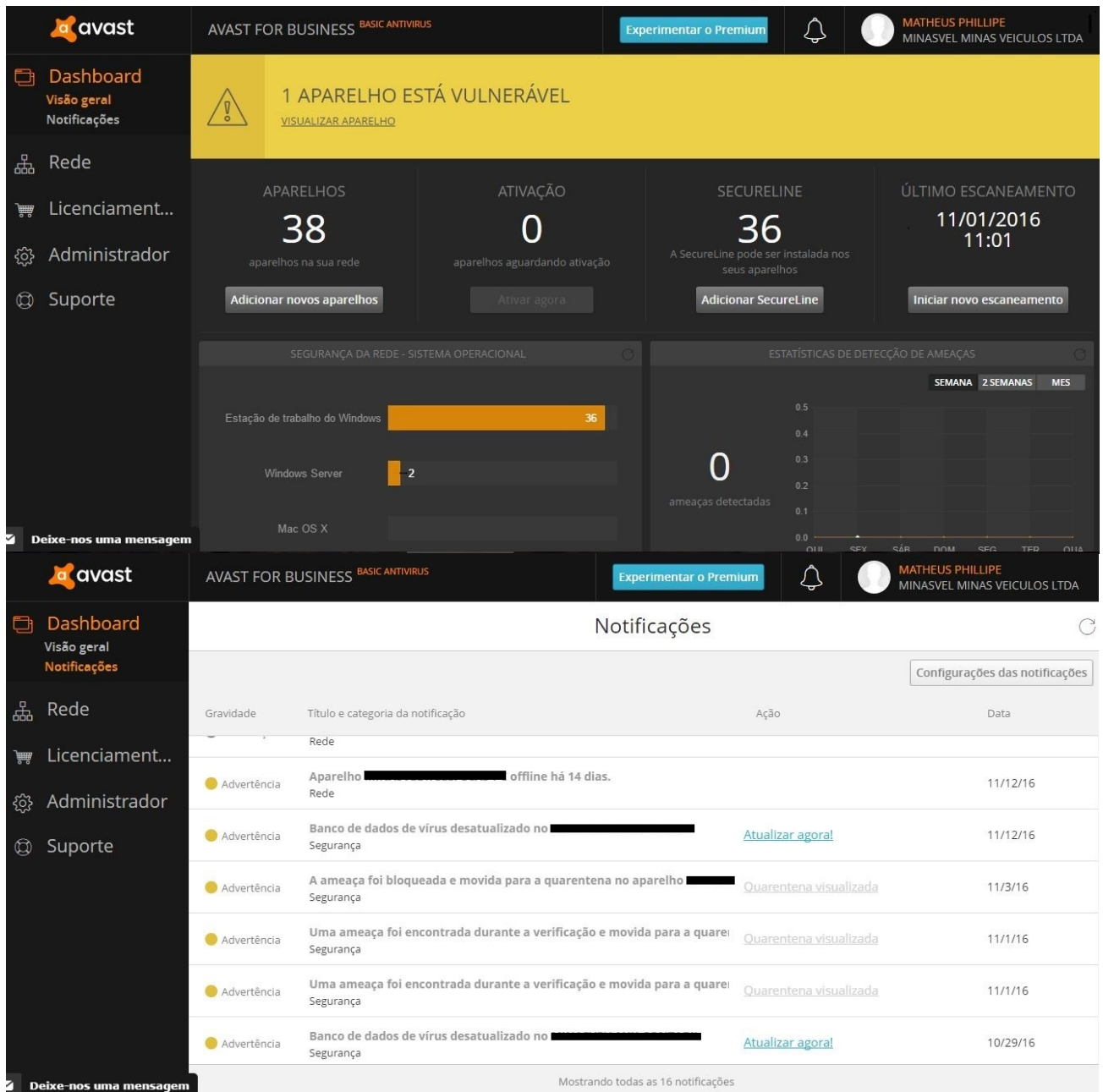


Figura 18. Painel de controle do *Avast for Business*

Fonte: Próprio autor

Como pode ser visto o administrador tem acesso a diversas informações como: aparelhos com vulnerabilidades de segurança, quantidade dispositivos conectados, último escaneamento executado, estatísticas de ameaças detectadas e notificações individuais dos aparelhos da rede.

A Minasvel teve um custo considerável com a aquisição dos equipamentos solicitados para a adequação da sua rede de computadores. Como pôde ser observado nesta metodologia foi adquirido um servidor *Dell*, três *switches*, três roteadores *wireless*, mídias de armazenamento externo, um *nobreak* e serviços de provedor de internet, além do *mikrotik*

routerboard 750 que custa em média R\$ 300,00. O custo pode variar de empresa para empresa, dependendo de quão bem estruturada está a sua rede de computadores antes da implantação de uma política de segurança.

Neste capítulo foram detalhados os métodos e processos utilizados para possibilitar que a empresa alcançasse a segurança da informação.

No capítulo 3 estão descritos os resultados obtidos durante o estudo.

3. RESULTADOS

Neste capítulo serão apresentados os resultados alcançados com o desenvolvimento deste trabalho. Primeiramente, vão ser descritos os pontos que estão em conformidade com as recomendações da ABNT NBR ISO/IEC 27001. As seções de 3.1.1 a 3.1.12 estão descritas no documento oficial da norma a partir da página 13. Após a apresentação das conformidades com algumas das recomendações da norma em questão, serão detalhados alguns testes de invasão realizados na rede de computadores da concessionária.

Estes testes têm como objetivo apresentar o quanto ficou eficiente a segurança da rede de computadores após a aceitação e execução das mudanças físicas e lógicas. Por fim, ocorrerá a apresentação dos resultados obtidos com a aplicação de um questionário sobre a segurança da informação na empresa.

A participação e comprometimento de todos os funcionários da organização foi de grande importância para a divulgação da política de segurança da informação, sendo possível conhecer a opinião de cada usuário.

3.1 RECOMENDAÇÕES DA ABNT NBR ISO/IEC 27001

3.1.1 Política de Segurança da Informação

O objetivo é prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio. A norma orienta que um documento da política de segurança deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes (ABNT NBR ISO/IEC 27001, 2006, p. 14).

Para atender a este quesito da norma, foi realizada uma reunião com o diretor da empresa que ocorreu em junho de 2016. Neste encontro foi explanado sobre o objetivo do trabalho e que haveria a necessidade da participação de todos os funcionários. Em primeira instância, o propósito era conhecer a opinião do membro de maior hierarquia da organização com relação ao presente trabalho. Após a exposição dos objetivos, o diretor demonstrou

interesse e autorizou a divulgação e orientações da política de segurança na concessionária. Com a autorização do diretor, todos os outros funcionários ficaram sabendo sobre o desenvolvimento deste trabalho, havendo também o apoio de todos os gerentes.

O documento da política de segurança da informação ficou pronto em outubro de 2016 e foi disponibilizado para o diretor e os gerentes com a finalidade de sua aprovação (Anexo 2). Com a aprovação da política de segurança, foi encaminhado uma cópia do documento para cada usuário. O departamento de Recursos Humanos também possui uma cópia da política de segurança, que será disponibilizada a novos funcionários juntamente com o termo de responsabilidade de uso de recursos de Tecnologia da Informação (Anexo 3).

No dia 26 de outubro de 2016 foi realizada uma reunião com todos os funcionários, com intuito de explicar cada ponto da política de segurança e concluir a divulgação da mesma.

3.1.2 Comprometimento da Direção com a Segurança da Informação

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 (ABNT NBR ISO/IEC 27001, 2006, p. 14).

Conforme exigido por esta seção da norma, a política de segurança da informação foi estabelecida pelo departamento de TI, mas todas as regras e recomendações contidas no documento são de conhecimento do diretor da organização. Com o reconhecimento do diretor, logo vem a importância que a segurança da informação representa para toda a empresa. Nos encontros com os usuários, sempre foram salientados os interesses e a importância que a empresa atribui a segurança da informação. A Política de Segurança da Informação da Minasvel se tornou uma norma interna que deve ser seguida por todos os funcionários.

3.1.3 Atribuição de responsabilidades para a segurança da informação

Todas as responsabilidades pela segurança da informação devem estar claramente definidas (ABNT NBR ISO/IEC 27001, 2006, p. 15).

Conforme exigido por esta seção, a política de segurança da Minasvel fala sobre as responsabilidades que os usuários devem ter com os recursos de Tecnologia da Informação. Esse quesito é descrito mais especificamente nos tópicos 2.1 e 5 no documento da política de segurança (Anexo 2).

3.1.4 Identificação dos riscos relacionados com partes externas

Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas. 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 (ABNT NBR ISO/IEC 27001, 2006, p. 15).

A concessionária conta com vendedores externos que vão até os clientes em outros municípios para realizar um atendimento ou venda de veículos. Estes vendedores fazem uso do mesmo sistema utilizado (Fiatnet) pelos consultores de vendas internos. O Fiatnet faz todo o controle de permissão de acesso a informação que determinado usuário possui.

A inclusão e configuração dos usuários no sistema e de responsabilidade do departamento de TI, onde são determinados quais os módulos do sistema um usuário pode acessar, quais relatórios tem permissão para visualizar e até mesmo restringir acesso a menus e botões de determinadas janelas.

Toda a capacidade de manipulação das permissões de acesso as informações do banco de dados que o Fiatnet possui, seria em vão se não existisse um meio seguro de acessá-lo remotamente. O *Mikrotik RouterOS* foi determinante neste quesito, com a configuração de uma VPN que possibilitou o acesso seguro entre a concessionária e os usuários externos. Detalhes sobre a configuração da rede privada virtual podem ser visualizados no capítulo 2,

subcapítulo 2.3.8.

3.1.5 Inventário dos ativos

Alcançar e manter a proteção adequada dos ativos da organização. Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido (ABNT NBR ISO/IEC 27001, 2006, p. 16).

Em dezembro de 2015 a concessionária passou por uma auditoria da *Microsoft* para comprovação das licenças de uso dos sistemas *Windows*, *Microsoft Office*, *SQL Server* e outros. Com intuito de comprovação das licenças é exigido o preenchimento de um inventário disponibilizado pela *Microsoft*, assim a fornecedora dos sistemas tem noção das licenças fornecidas.

Como a concessionária já possuía o inventário disponibilizado para a *Microsoft*, o mesmo foi atualizado e mantido até os dias atuais (Anexo 4).

O documento original do inventario possui todos os *softwares* comercializados pela *Microsoft*, como era muito extenso foi modificado de modo que atendesse a concessionária. Além deste inventário, a empresa também possui um registro de ativos imobilizados, que inclui ativos de Tecnologia da Informação. Esses registros são utilizados pela contabilidade para realização da depreciação dos ativos da organização.

3.1.6 Antes da Contratação de Colaboradores

Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos (ABNT NBR ISO/IEC 27001, 2006, p. 16).

Atualmente a empresa possui uma Política de Segurança da Informação documentada, que fica disponível no departamento de Recursos Humanos, juntamente com o termo de responsabilidade de uso recursos de Tecnologia da Informação (Anexos 2 e 3). Esta seção da norma foi atendida conforme a execução desta ação.

3.1.7 Conscientização, Educação e Treinamento em Segurança da Informação

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 (ABNT NBR ISO/IEC 27001, 2006, p. 17).

Todos os funcionários da concessionária, principalmente os recém contratados são orientados tomarem a conhecimento da Política de Segurança da empresa. Dentro dos recursos utilizados por cada usuário, são transmitidos conhecimentos sobre as melhores práticas de segurança na utilização da internet, e-mail, usuários do sistema, equipamentos e detalhes técnicos de cada departamento. Logo no início de suas atividades na empresa, cada usuário passa a ter conhecimento sobre as regras internas para utilizar recursos de tecnologia.

3.1.8 Retirada de Direitos de Acesso

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 NBR ISO/IEC 27001, 2006, p. 18).

O departamento de Recursos Humanos ficou responsável por comunicar para o administrador da rede de computadores, os funcionários que por ventura, serão desligados da empresa. Após a notificação, antes do funcionário sair da organização seu usuário do sistema e e-mail são desativados. Dependendo da função que era exercida pelo o usuário, o direito de acesso a outras ferramentas também é retirado. Por fim, é verificado se todos os equipamentos utilizados pelo funcionário foram devolvidos corretamente.

3.1.9 Controles de Entrada Física

As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso (ABNT NBR ISO/IEC 27001, 2006, p. 18).

A concessionária possui os departamentos bem divididos e organizados. Nos departamentos de maior segurança existem regras que determinam quem pode ter acesso a determinada instalação. As instalações dos departamentos de TI, contabilidade, financeiro, caixa e a sala do diretor são áreas que só podem ser acessadas por pessoas autorizadas.

Cada funcionário é responsável por deixar sua sala trancada e segura nos momentos em que estiver ausente. A empresa também conta com sistema de câmeras de segurança instaladas em quase todos os departamentos, ajudando a desencorajar ações que coloquem em risco os ativos da organização. Além disso, a Minasvel ainda conta com vigias que são responsáveis por manter a segurança e organização nos horários após o encerramento de expediente.

3.1.10 Utilidades

Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades (ABNT NBR ISO/IEC 27001, 2006, p. 19).

Conforme descrito no capítulo 2 deste trabalho, os servidores, modem, roteadores e o computador com as mídias externas de *backups*, são protegidos contra falhas no fornecimento de energia elétrica por dois *nobreaks* com autonomia eficiente da bateria. Esses *nobreaks* são testados frequentemente pelo administrador da rede e pelo menos uma vez a cada 18 meses é realizada a manutenção dos mesmos.

3.1.11 Documentação dos Procedimentos de Operação

Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem (ABNT NBR ISO/IEC 27001, 2006, p. 19).

A Minasvel utiliza o sistema de gestão de concessionárias Fiatnet. Esse sistema é desenvolvido e mantido pela Dealernet Ação Informática. O fiatnet é utilizado por quase todas as concessionárias de bandeira Fiat e para disponibilizar a documentação do sistema, notas técnicas, melhorias e novidades, a Dealernet desenvolveu o Dealernet *Wiki*, um portal onde são mantidos todos os procedimentos do sistema Fiatnet. Para acessar esse portal as concessionárias devem possuir um *login* e senha fornecido pela Dealernet, após realizar o acesso o usuário pode pesquisar pelo assunto de seu interesse. As documentações possuem procedimentos descritos em detalhes das funcionalidades do sistema, além das regras de negócios e detalhamento de cálculos executados pelo Fiatnet (DEALERNET, 2016).

3.1.12 Controle Contra Códigos Maliciosos

Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários (ABNT NBR ISO/IEC 27001, 2006, p. 20).

Para a proteção contra *softwares* maliciosos a concessionária possui o *Avast for Business*, um sistema que gerencia todos os computadores da rede que possuem seu cliente antivírus instalado. Quando qualquer tipo de ameaça é detectada um alerta é exibido no painel de controle do sistema, com essa medida as ações a serem tomadas são executadas com maior agilidade. Os detalhes sobre o *Avast for Business* podem ser vistos no capítulo 2 deste trabalho.

As execuções de *backups* dos sistemas seguros da empresa, possibilitam que a recuperação dos mesmos, seja executada caso algum inconveniente venha a acontecer. Os arquivos dos *backups* realizados são salvos em uma mídia externa para aumentar ainda mais a segurança. A política de *backups* da organização está descrita no capítulo 2.

Essas foram as seções retiradas da ABNT NBR ISO/IEC 27001 para aplicação neste trabalho. Os próximos resultados vão demonstrar a eficácia do *Firewall* configurado no *Mikrotik RouterOS* através de teste de invasão executados pelo próprio autor. Os métodos de invasão que serão demonstrados foram retirados do livro *Backtrack Linux* dos autores Silvio Giavaroto e Gerson Santos. O livro especifica métodos de auditoria e teste de invasão em rede de computadores (GIAVAROTO; SANTOS, 2013).

3.2 TESTES DE INVASÃO

Os testes de invasão que são apresentados, baseiam-se primeiramente em reconhecimento do alvo, onde são extraídas informações como portas ativas, serviços ativos, versões de aplicações ativas e sistemas operacionais em execução. Essas informações são promissoras para o invasor, pois fornecem dados de versões de serviços com vulnerabilidades ou dados sobre um serviço executando em determinada porta. Assim é possível determinar uma metodologia eficiente de ataque.

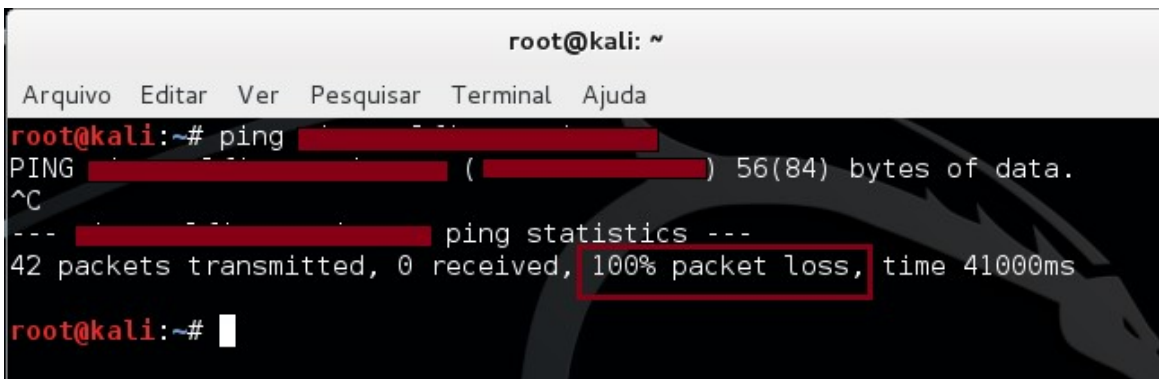
A utilização de engenharia pessoal para a coleta de dados relevantes para uma invasão também é muito utilizada. Com este método pode-se conseguir informações como nome de usuários do sistema, informações pessoais, informações da empresa, dados sobre sistemas em execução, e-mails entre outros. Em posse de determinadas informações, um invasor pode por exemplo, planejar métodos de ataques utilizando *word list* com palavras chaves coletadas. As *words lists* podem ser utilizadas para a descoberta de nomes de usuários e também para descobrir senhas (GIAVAROTO; SANTOS, 2013).

Vale destacar que os teste efetuados são do tipo de Testes de Caixa Branca, onde o autor das tentativas de invasão possui total conhecimento da estrutura do sistema alvo. O sistema operacional utilizado para os testes de intrusão foi o *Kali Linux* versão 1.1.0 (moto) 64-bit, *Kernel Linux* 3.18.0-kali3-amd64 e *GNOME* 3.4.2.

3.2.1 Ping

O primeiro teste executado foi o *ping*, onde conseguimos identificar se existe algum *host* ativo.

Neste caso, para maior segurança da rede interna da empresa, é desejável que não se tenha respostas na execução de uma simples requisição de *ping*. Nota-se os retornos da ferramenta após efetuar o *ping*.



```

root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# ping [REDACTED]
PING [REDACTED] ([REDACTED]) 56(84) bytes of data.
^C
--- [REDACTED] ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 41000ms
root@kali:~#

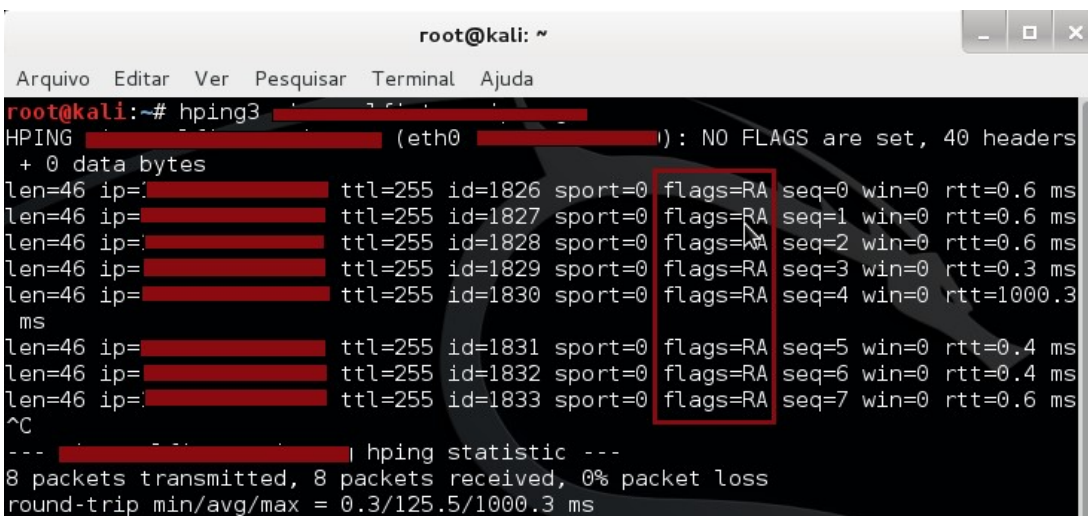
```

Figura 19. Execução da ferramenta *PING*

Fonte: Próprio autor

Como pode ser observado na figura anterior, não houve respostas do *host* testado.

O próximo teste também é baseado no *ping*, porém trata-se de uma ferramenta ainda mais poderosa, o *HPING3*. Nota-se a saída da ferramenta após a execução do *HPING3* contra o *host* alvo.



```

root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# hping3 [REDACTED]
HPING [REDACTED] (eth0 [REDACTED]): NO FLAGS are set, 40 headers
+ 0 data bytes
len=46 ip=[REDACTED] ttl=255 id=1826 sport=0 flags=RA seq=0 win=0 rtt=0.6 ms
len=46 ip=[REDACTED] ttl=255 id=1827 sport=0 flags=RA seq=1 win=0 rtt=0.6 ms
len=46 ip=[REDACTED] ttl=255 id=1828 sport=0 flags=RA seq=2 win=0 rtt=0.6 ms
len=46 ip=[REDACTED] ttl=255 id=1829 sport=0 flags=RA seq=3 win=0 rtt=0.3 ms
len=46 ip=[REDACTED] ttl=255 id=1830 sport=0 flags=RA seq=4 win=0 rtt=1000.3
ms
len=46 ip=[REDACTED] ttl=255 id=1831 sport=0 flags=RA seq=5 win=0 rtt=0.4 ms
len=46 ip=[REDACTED] ttl=255 id=1832 sport=0 flags=RA seq=6 win=0 rtt=0.4 ms
len=46 ip=[REDACTED] ttl=255 id=1833 sport=0 flags=RA seq=7 win=0 rtt=0.6 ms
^C
--- [REDACTED] hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0.3/125.5/1000.3 ms

```

Figura 20. Execução da ferramenta *HPING3*

Fonte: Próprio autor

Observando a figura anterior, nota-se que houve comunicação com o *host* de destino. Mas deve-se analisar detalhadamente os dados retornados, como *flags* e o valor que possui. Os valores informados nos *flags* determinam se o sistema está disponível para conexão ou não. Flag=SA disponível, flag=RA indisponível. Com os dados obtidos observa-se que o *Firewall* está filtrando comunicações ICMP.

O próximo método a ser demonstrado tenta recuperar informações do alvo através de configurações sobre o DNS (*Domain Name System*). A ferramenta escolhida para esse teste foi o DNSMAP, também disponível no *Kali Linux*.

3.2.2 DNSMAP

O DNSMAP pode descobrir informações de subdomínios relacionados com *host* alvo. Se na rede da empresa as configurações de domínio permitem transferências de zonas para servidores não autorizados, o invasor poderá conseguir facilmente dados para executar um determinado tipo de ataque.

A figura a seguir exibi o resultado da execução do DNSMAP contra a rede da empresa. Neste teste foi utilizada a própria *word list* da ferramenta na realização das buscas.

```

root@kali:~# cd /tmp/
root@kali:/tmp# dnsmap [REDACTED] -r ./teste.txt
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for [REDACTED] using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

[+] 0 (sub)domains and 0 IP address(es) found
[+] regular-format results can be found on ./teste.txt
[+] completion time: 823 second(s)
root@kali:/tmp#

```

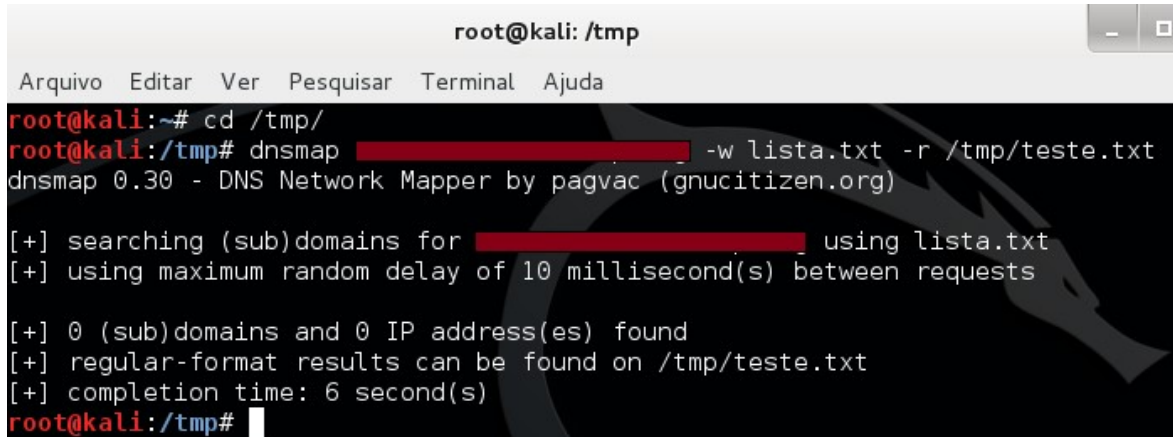
Figura 21. Execução da ferramenta DNSMAP

Fonte: Próprio autor

Como pode ser observado a execução da ferramenta levou 823 segundos e não retornou nenhum dado sobre a empresa.

O próximo teste demonstra o resultado da execução do dnsmap com uma *word list*

gerada pelo próprio invasor, contendo palavras chaves que podem facilitar a busca. A *word list* está identificada como “lista.txt” e o arquivo “teste.txt” é onde são gravados os resultados da busca.



```

root@kali: /tmp
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@kali:~# cd /tmp/
root@kali:/tmp# dnsmap [redacted] -w lista.txt -r /tmp/teste.txt
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for [redacted] using lista.txt
[+] using maximum random delay of 10 millisecond(s) between requests

[+] 0 (sub)domains and 0 IP address(es) found
[+] regular-format results can be found on /tmp/teste.txt
[+] completion time: 6 second(s)
root@kali:/tmp#

```

Figura 22. Execução da ferramenta DNSMAP com a *Word List* gerada

Fonte: Próprio autor

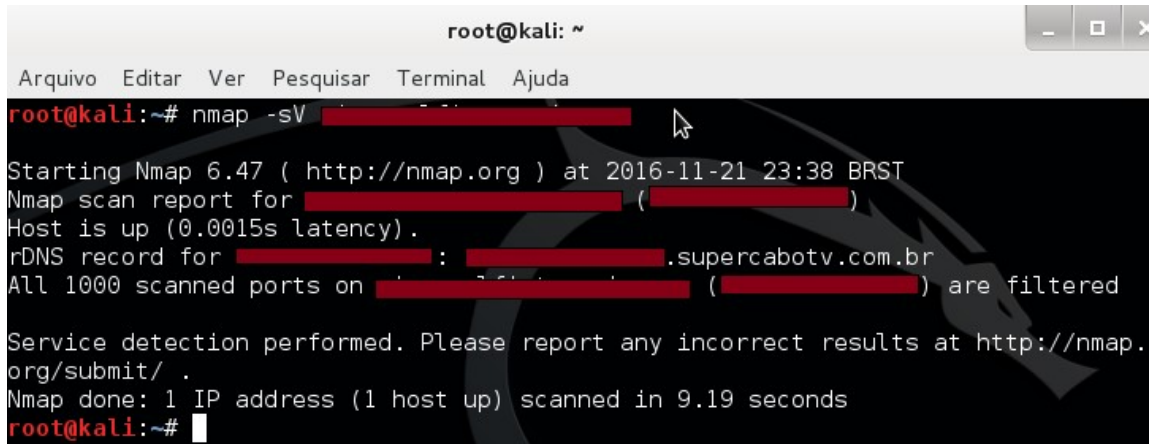
Mais uma vez não foi apresentado nenhum resultado relevante para o invasor. Nesta tentativa a ferramenta demorou apenas 6 segundos para concluir o processo aplicando a *word list* “lista.txt”.

Após algumas tentativas de reconhecimento por varreduras, será descrito a ferramenta NMAP. Com o NMAP é possível praticar tentativas mais invasivas com a possibilidade de obter nomes de computadores, usuários, serviços e versões.

3.2.3 NMAP

Com a execução da ferramenta NMAP contra o servidor, serão executadas tentativas de obtenção das portas disponíveis, serviços ou até mesmo versão do sistema operacional. Caso o invasor consiga as informações necessárias, tentativas de intrusões do tipo força bruta poderão ser aplicadas.

No seguinte teste aplicado contra o servidor, foi especificado a função `-sV` para a execução do NMAP, o “s” determina o *scan* e o “V” retorna as versões dos serviços ou sistemas, caso estejam disponíveis.



```

root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# nmap -sV [REDACTED]
Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-21 23:38 BRST
Nmap scan report for [REDACTED] ([REDACTED])
Host is up (0.0015s latency).
rDNS record for [REDACTED]: [REDACTED].supercabotv.com.br
All 1000 scanned ports on [REDACTED] ([REDACTED]) are filtered
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
root@kali:~#

```

Figura 23. Execução da ferramenta NMAP -sV

Fonte: Próprio autor

O teste com a ferramenta não obteve êxito. Analisando as informações retornadas, é possível notar que o NMAP detectou um *host* ativo, mas também informou que as portas do *Firewall* estão sendo filtradas.

Para finalizar as tentativas de coleta de informações sobre vulnerabilidades do alvo, executou-se o NMAP com as seguintes funções: `-T4 -A -v`, sendo que `-T4` executa varredura usando o *Three-Way Handshake* (cria uma conexão entre um cliente e servidor que passa por três etapas onde os *hosts* trocam pacote SYN e ACK), o “`-A`” define detecção de regras do *Firewall* e “`-v`” determina o modo verboso. O relatório retornado pela ferramenta pode ser visualizado no Anexo 5.

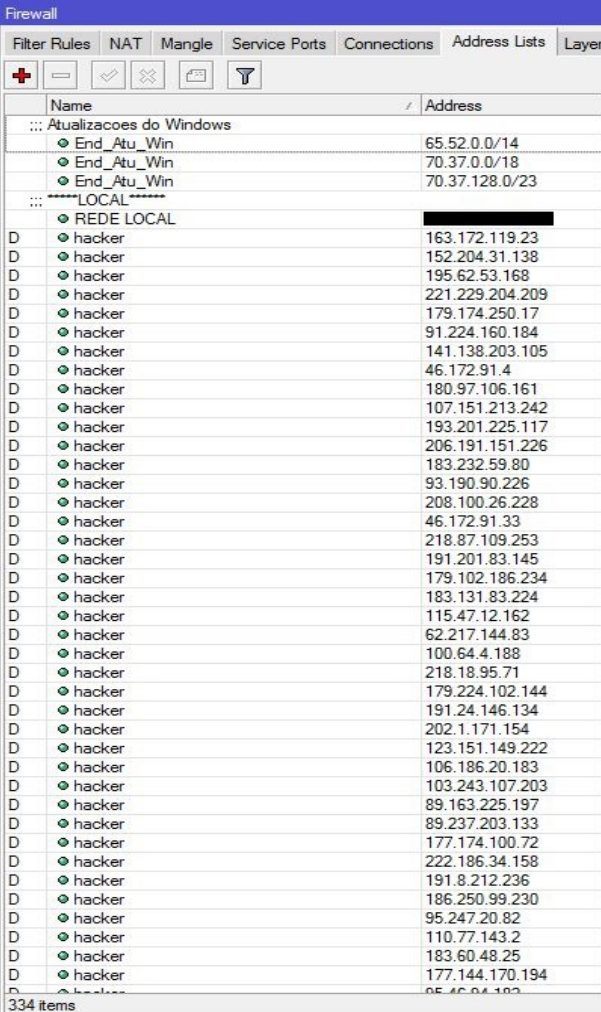
Com análise das informações alcançadas, nota-se que foram efetuados vários tipos de testes através do NMAP. Testes como *PING*, busca por DNS, scanner aplicando NYN, detecção de Sistema Operacional e até mesmo informações do caminho da rede entre os *hosts*. Vale destacar que mais uma vez a ferramenta informou que as portas do *Firewall* estão sendo filtradas (linha 25), ou seja, não foi possível detectar conexões disponíveis. Na linha 26 nota-se que o NMAP não conseguiu coletar informações sobre o Sistema Operacional.

A informação mais relevante coletada está na linha 29, sublinha 1, caso o endereço IP detectado pertencesse da rede interna da concessionária, poderia caracterizar uma vulnerabilidade crítica, pois houve conexão com algum equipamento disponível e neste caso uma metodologia de ataque poderia ser aplicada. O endereço IP 10.0.2.2 impresso no relatório não é da classe de IPs da rede interna, mas sim um *host* ativo na rede *Wireless* utilizada pelos clientes da empresa. Pelo horário da execução do NMAP (também disponível no relatório), provavelmente o dispositivo detectado, é um *Smartphone* de um dos vigias da concessionária.

3.2.4 Regra de Prevenção Contra os Ataques de Força Bruta

Foi possível notar nos testes demonstrados anteriormente que o *Firewall* configurado no *Mikrotik RouterOS* apresentou um comportamento que garante a segurança da rede de computadores da empresa. As informações coletadas com as ferramentas de testes de invasão durante suas execuções, não são de relevância para oferecer riscos a organização.

Vale destacar que a regra definida no *Firewall* para bloquear ataques do tipo força bruta, conforme orientado no manual da *Mikrotik*, foi de grande importância para a obtenção dos resultados apresentados (detalhes sobre a configuração da regra podem ser revistos no capítulo 2). De modo geral, a regra em questão adiciona os IPs de origem dos ataques em uma *black list*, onde é definido que os endereços IPs contidos na lista serão bloqueados para qualquer tipo de conexão durante 90 dias.



Name	Address
Atualizacoes do Windows	
End_Atu_Win	65.52.0.0/14
End_Atu_Win	70.37.0.0/18
End_Atu_Win	70.37.128.0/23
LOCAL	
REDE LOCAL	
D hacker	163.172.119.23
D hacker	152.204.31.138
D hacker	195.62.53.168
D hacker	221.229.204.209
D hacker	179.174.250.17
D hacker	91.224.160.184
D hacker	141.138.203.105
D hacker	46.172.91.4
D hacker	180.97.106.161
D hacker	107.151.213.242
D hacker	193.201.225.117
D hacker	206.191.151.226
D hacker	183.232.59.80
D hacker	93.190.90.226
D hacker	208.100.26.228
D hacker	46.172.91.33
D hacker	218.87.109.253
D hacker	191.201.83.145
D hacker	179.102.186.234
D hacker	183.131.83.224
D hacker	115.47.12.162
D hacker	62.217.144.83
D hacker	100.64.4.188
D hacker	218.18.95.71
D hacker	179.224.102.144
D hacker	191.24.146.134
D hacker	202.1.171.154
D hacker	123.151.149.222
D hacker	106.186.20.183
D hacker	103.243.107.203
D hacker	89.163.225.197
D hacker	89.237.203.133
D hacker	177.174.100.72
D hacker	222.186.34.158
D hacker	191.8.212.236
D hacker	186.250.99.230
D hacker	95.247.20.82
D hacker	110.77.143.2
D hacker	183.60.48.25
D hacker	177.144.170.194
D hacker	95.46.94.103

Figura 24. *Address Lists* do *Firewall*

Fonte: Próprio autor

A figura 24, na página anterior, mostra que 330 endereços IPs foram adicionados à lista *hacker*. Todos estes IPs foram filtrados em apenas 12 dias de execução do servidor *Mikrotik RouterOS*. Através destes números tem-se uma ideia da quantidade de ataques que são executados todos os dias contra a rede da empresa.

3.2.5 *xHydra*

O *xHydra* ou *Hydra-GTK*, é a versão que possui interface gráfica da ferramenta *Hydra* do *Kali Linux*. A função do *software* é realizar invasões através de quebra de senha *online*. Na interface gráfica pode-se definir o endereço IP ou nome DNS do alvo, lista (arquivo *.TXT* do tipo *word list*) com possíveis nomes de usuários, lista com caracteres alfanuméricos que será utilizada nas tentativas de quebra de senhas e a porta de conexão que será testada. É importante lembrar que neste teste o invasor já executou as tarefas de reconhecimento e coleta de dados sobre o alvo. No caso o autor possui total conhecimento sobre os usuários e senhas cadastrados no servidor, o que ajudou a definir os dados para o ataque. Nos serviços do *Mikrotik RouterOS* é possível definir o número da porta utilizada para conexão via *winbox* (também existem outros serviços que podem ter suas portas padrão alteradas como *ssh*, *www*, *telnet* e outros), o foco deste teste foi na porta de conexão remota do *Mikrotik RouterOS*. O número da porta em questão não será exibido por motivos de segurança da empresa. Como o sistema de roteamento é o ponto forte da segurança para a organização, foi de grande importância o teste feito com a porta utilizada para conexões remotas no servidor.

Na inicialização dos testes, após definir as configurações no *xHydra*, tais como: o endereço do servidor, a porta de destino e os arquivos *.txt* de geração de usuários e senhas, deu-se início aos ataques. A primeira tentativa de quebra de senha iniciou-se no dia 23/11/2016 as 21 horas e 45 minutos e a última tentativa do ataque foi finalizada no dia 24/11/2016 as 14 horas e 03 minutos.

Como pode ser observado no Anexo 6, no *log* de saída do *xHydra*, foi gerado através da ferramenta 117 tentativas de *login* com os arquivos *users.txt* e *senha.txt* informados nas configurações do *software*. No final do Anexo 6 na área destacada, pode ser visto que a tentativa de invasão obteve respostas negativas, ou seja, não houve a possibilidade de conseguir senhas válidas.

O *log* do *xHydra* disponível neste trabalho é apenas um pequeno trecho de todas as informações retornadas pela ferramenta. A cada tentativa de *login* malsucedida, o *software* iniciava automaticamente outra execução com novas informações de acesso. Todas as tentativas efetuadas falharam na obtenção do usuário e senha de acesso ao sistema.

Com o resultado apresentado através das ferramentas utilizadas no sistema operacional *Kali Linux*, é possível notar a eficiência das regras definidas no *Firewall* do *Mikrotik RouterOS*. Vale salientar que apesar dos bons resultados ocorridos não se deve baixar a guarda quando se fala em Segurança da Informação. Conforme cita Giavaroto e Santos (2013), deve-se sempre buscar informações que sejam relevantes, pois não existe um sistema totalmente seguro.

3.3 QUESTIONÁRIO REFERENTE A SEGURANÇA DA INFORMAÇÃO

Durante a coleta de dados realizada após a adequação da Política de Segurança da Informação na empresa, não poderia faltar a opinião dos usuários sobre as mudanças realizadas. A ABNT ISO/IEC 27001 descreve muitas vezes em suas diretrizes sobre a importância da conscientização dos usuários sobre a Política de Segurança. Com intuito de conhecer o ponto de vista dos usuários com relação a segurança da rede de computadores, foi aplicado um questionário para a obtenção dos dados na empresa.

O questionário aplicado coleta informação sobre as mudanças executadas na rede de computadores referente a segurança, qualidade, organização e facilidade de acesso a informação. Foram considerados os aspectos físicos e lógicos das mudanças. Também foram reunidas informações sobre a importância e comprometimento da empresa e usuários com a segurança da informação.

Para aplicar o questionário aos usuários foi utilizada uma ferramenta *online*, o Formulários Google disponível no Google Drive. Após incluir todas as perguntas no formulário da Google, o questionário foi enviado por e-mail aos funcionários. Foram obtidas 29 respostas de um total de 40 funcionários da organização, nos 3 dias em que o questionário esteve *online*.

As demonstrações dos resultados obtidos através das respostas do questionário serão apresentadas em forma de gráficos. A primeira fase de perguntas é avaliada pelo o usuário em

uma escala entre PÉSSIMO e ÓTIMO.

Na segunda parte os usuários avaliaram cada questão informando se a mesma possui importância pequena (NENHUM), até muito importante (MUITO).

As primeiras perguntas são referentes as mudanças na rede de computadores. O gráfico a seguir expõe a opinião dos usuários sobre a questão da organização atual dos dispositivos.

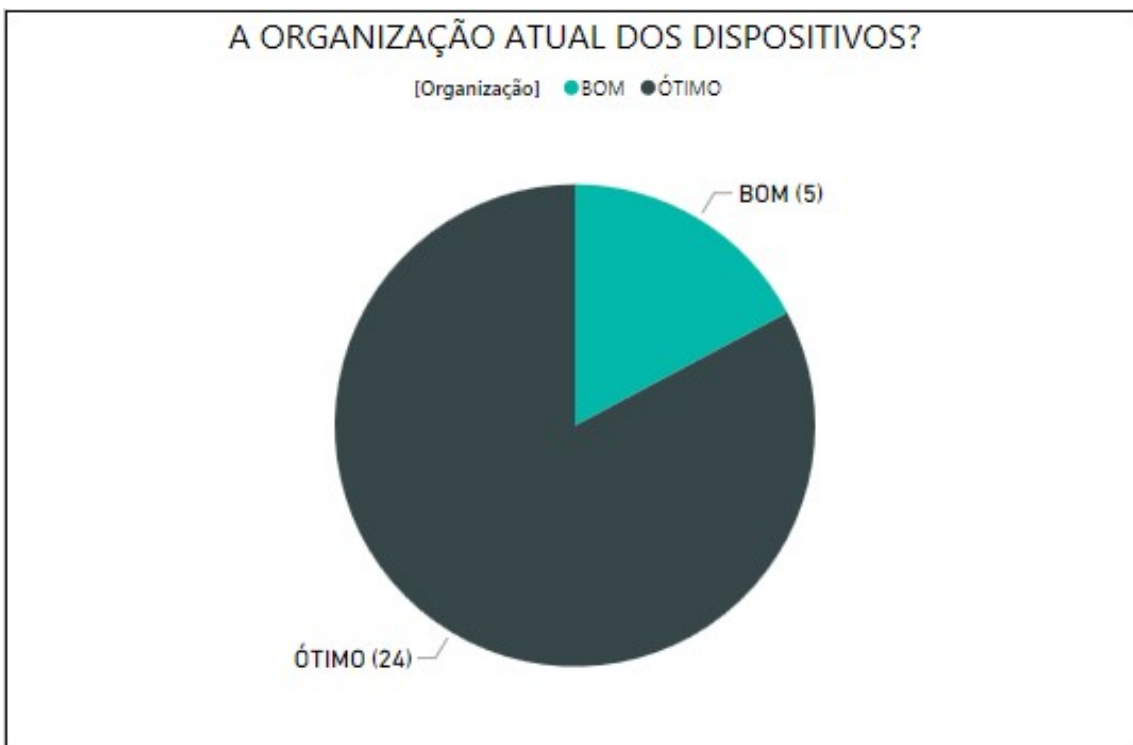


Gráfico 1. Organização atual dos dispositivos

Fonte: Próprio autor

O resultado do gráfico 1, demonstra que 24 funcionários entrevistados consideraram ótima a organização dos dispositivos na rede de computadores e 5 disseram que ficou bom.

O segundo gráfico mostra os dados obtidos sobre a qualidade da rede de computadores.

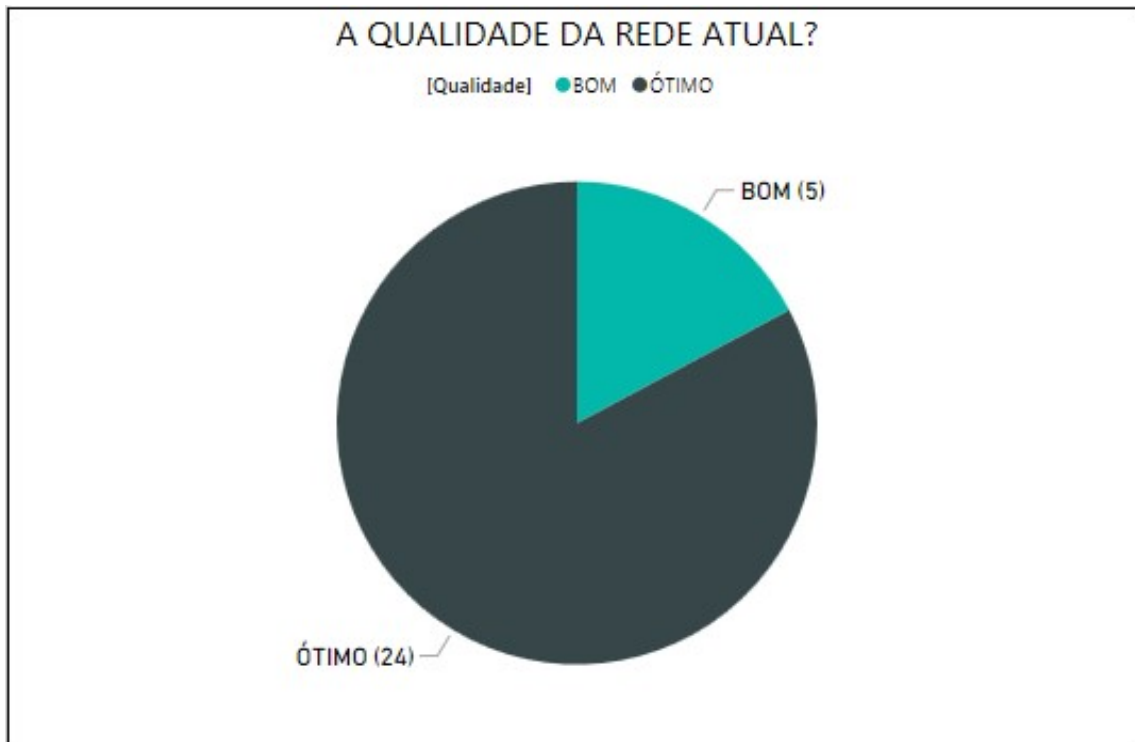


Gráfico 2. Qualidade da rede atual

Fonte: Próprio autor

O objetivo da segunda pergunta foi verificar se após as alterações na rede de computadores e substituição de equipamentos, houve melhoria significativa de desempenho na transmissão e compartilhamento dos dados. Conforme o gráfico 2, 24 funcionários disseram que a qualidade da rede é ótima e 5 consideraram que a qualidade é boa.

O gráfico 3 obtém o resultado referente ao acesso a *softwares* utilizados em rede.

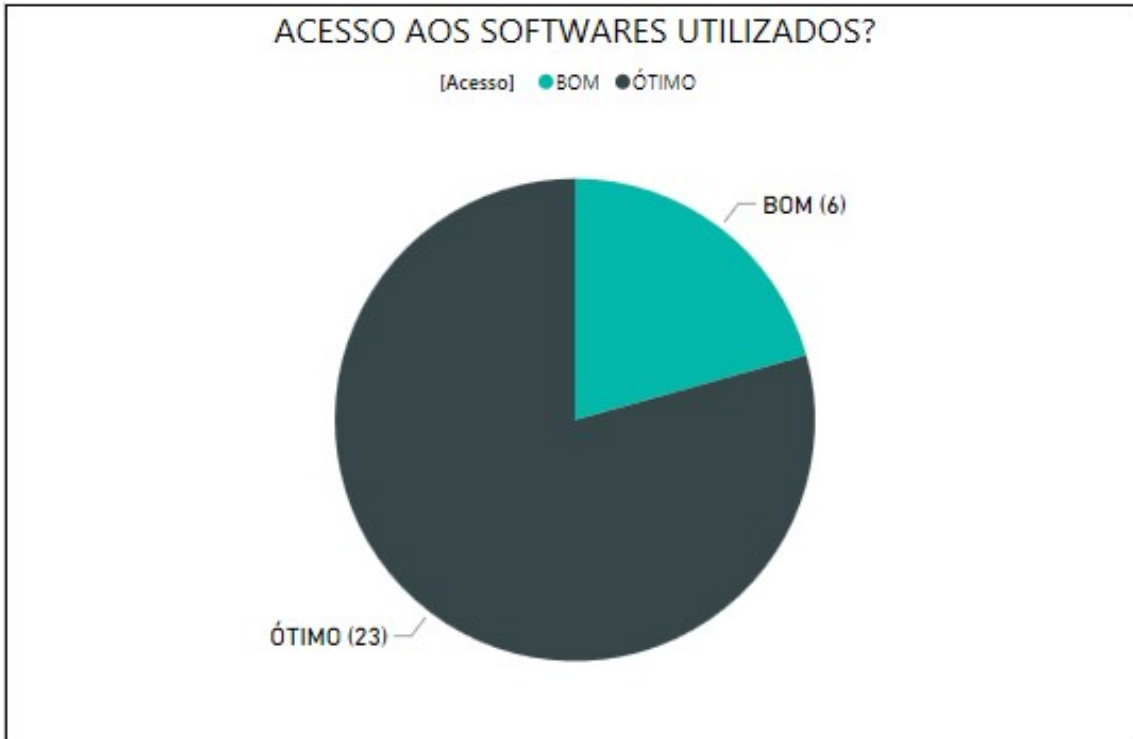


Gráfico 3. Acesso aos *softwares* utilizados

Fonte: Próprio autor

A terceira pergunta teve o propósito de avaliar os sistemas que são executados e utilizados em rede pelos usuários da empresa. Nesta questão, 23 funcionários responderam que é ótimo o acesso aos *softwares* e 6 disseram que é bom.

A próxima pergunta avalia o nível da segurança dos dados que trafegam na rede.

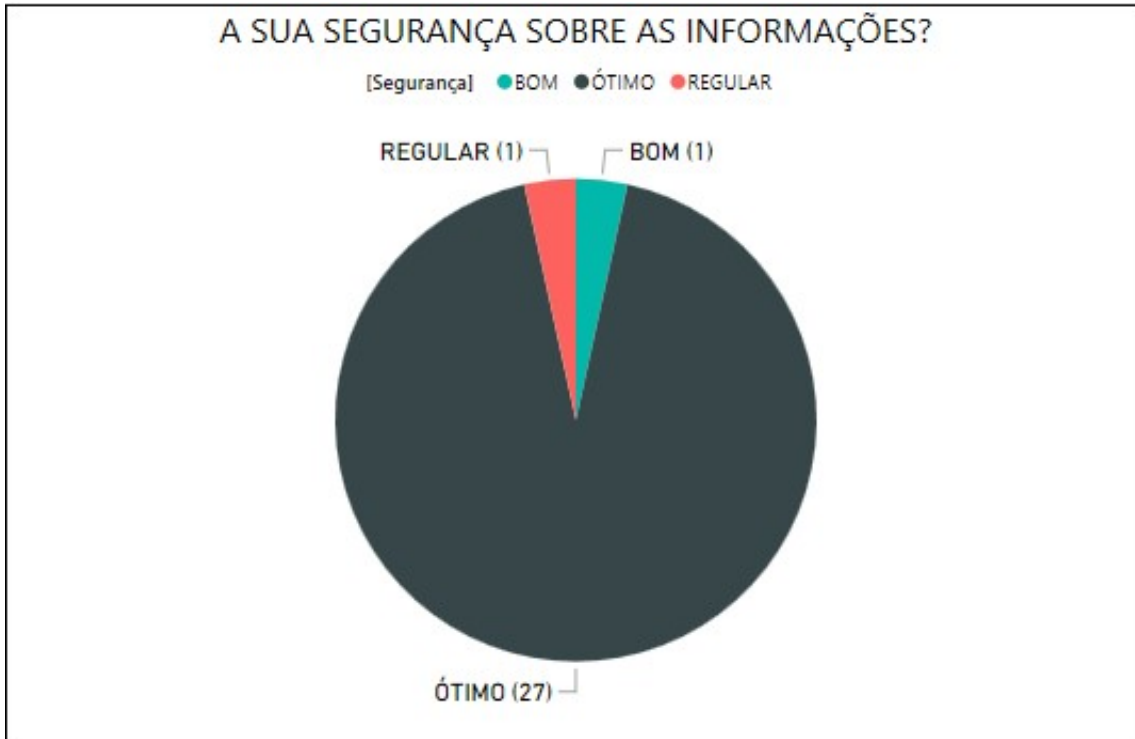


Gráfico 4. Sua segurança sobre as informações

Fonte: Próprio autor

Esta questão avalia o ponto de vista de cada funcionário considerando o quanto as informações da organização estão seguras. Das 29 respostas obtidas, 27 avaliaram a segurança como ótima, 1 usuário considerou bom e 1 usuário disse que a segurança é regular.

A quinta pergunta avalia a praticidade de acesso as informações.

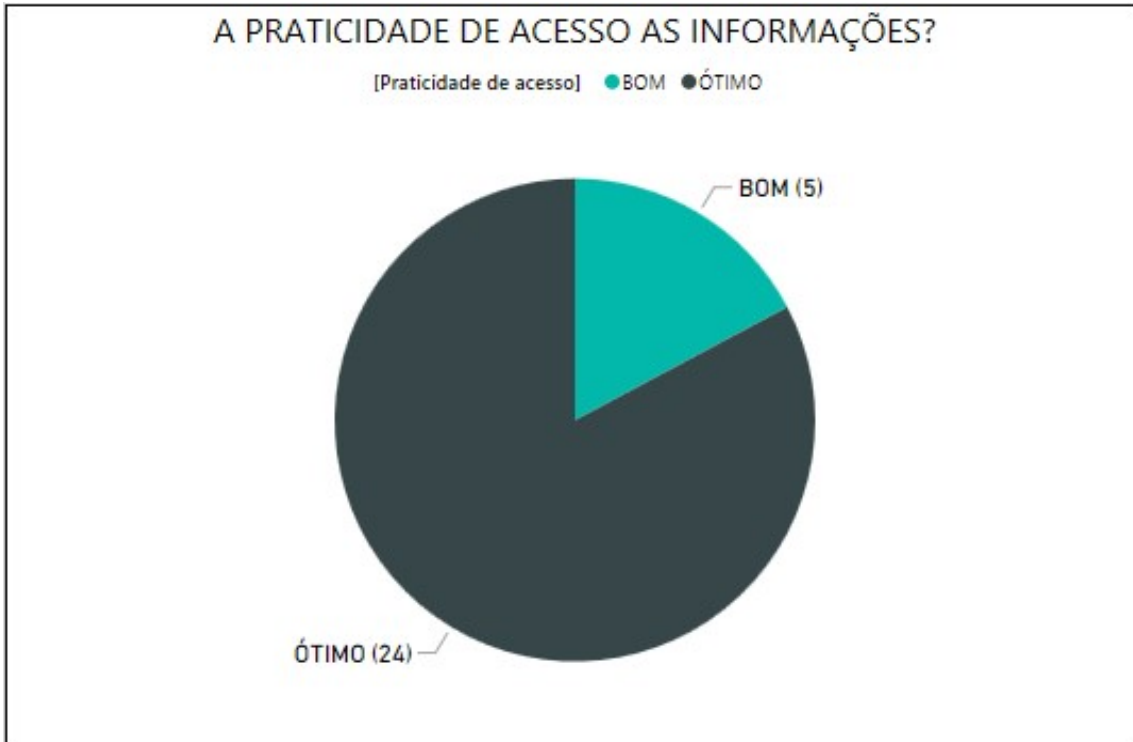


Gráfico 5. Praticidade de acesso as informações

Fonte: Próprio autor

A pergunta 5 avalia se após as alterações realizadas na rede de computadores houve alguma melhoria nos meios de acesso a informação. Conforme o gráfico 5, 24 usuários responderam que é ótima a praticidade de acesso as informações e 5 avaliaram como bom.

A sexta pergunta é referente a recuperação de serviços após falhas.

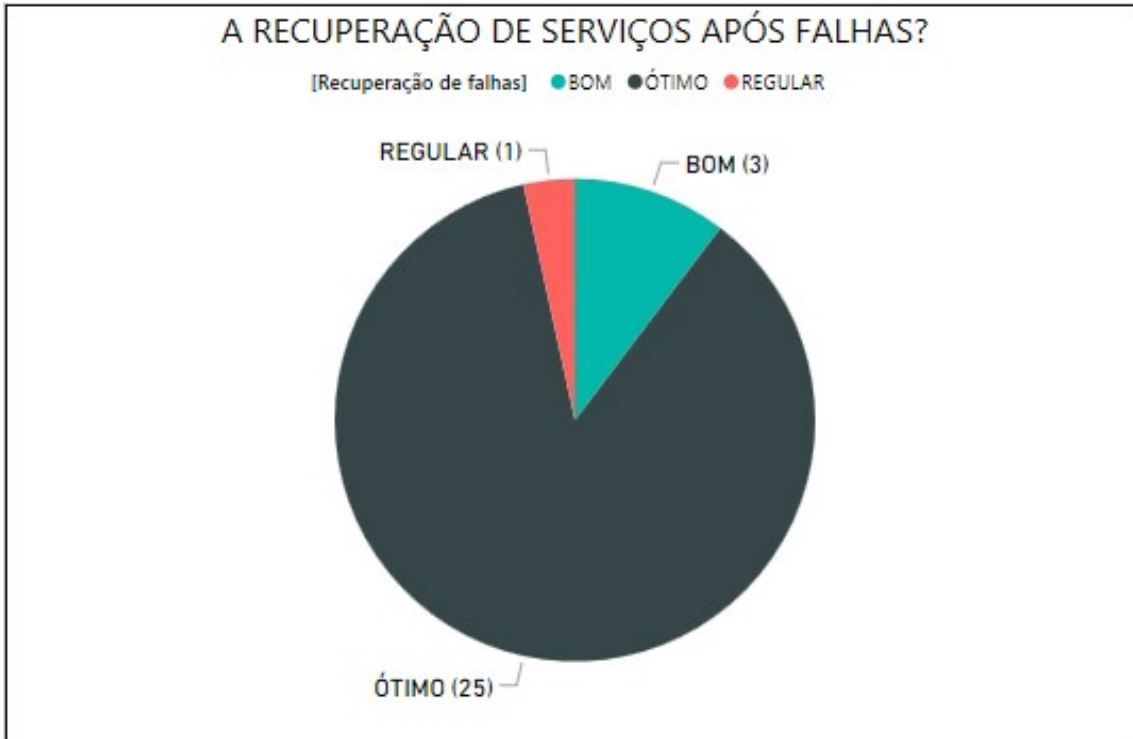


Gráfico 6. Recuperação de serviços após falhas

Fonte: Próprio autor

Neste quesito, os usuários avaliaram a recuperação dos sistemas utilizados na rede após a ocorrência de falhas. O gráfico 6 mostra que, 25 funcionários consideraram ótima a recuperação de serviços após falhas, 3 funcionários qualificaram como bom e 1 funcionário respondeu que é regular.

O gráfico 7 exibe o resultado obtido sobre a utilização das redes *wireless* da organização.

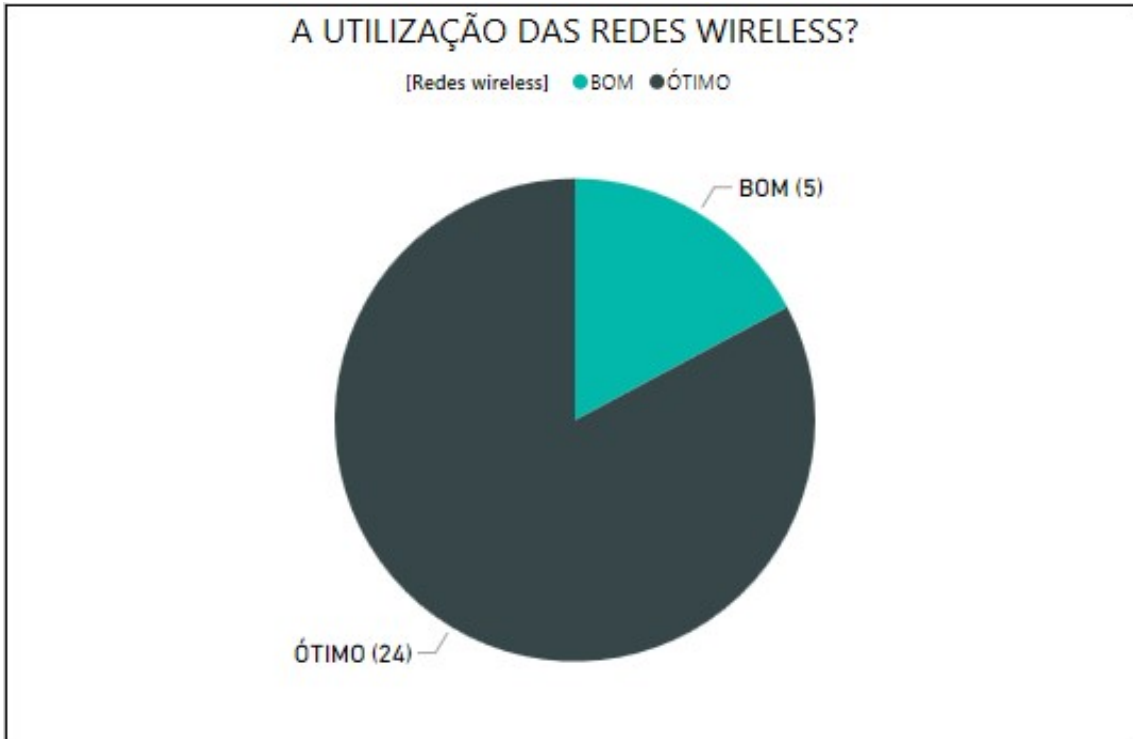


Gráfico 7. Utilização das redes *wireless*

Fonte: Próprio autor

Como pode ser observado no gráfico 7, dos 29 usuários que responderam o questionário, 24 qualificaram como ótima a utilização das redes *wireless* e 5 usuários classificaram como boa.

Os 7 gráficos apresentados anteriormente, compreendem a primeira parte do questionário. Os próximos gráficos que serão apresentados, expõem o ponto de vista dos entrevistados com relação a importância e comprometimento da empresa e usuários com a segurança da informação.

O próximo ponto avaliado é a importância da segurança da informação para a empresa.



Gráfico 8. Importância da segurança para a empresa

Fonte: Próprio autor

O objetivo da oitava pergunta foi avaliar de acordo com os usuários, o quanto a organização considera importante manter seus dados seguros. Através do gráfico 8, é possível observar que 100 % dos entrevistados responderam que a empresa considera muito importante a segurança.

O gráfico abaixo trata sobre o nível de importância da segurança para cada funcionário.



Gráfico 9. Importância que você atribui a segurança da informação

Fonte: Próprio autor

A questão acima teve o objetivo de avaliar o quanto é importante a segurança da informação de acordo com cada funcionário. O gráfico 9 mostra que todos os usuários responderam como muito importante a segurança da informação.

O decimo gráfico obtém os resultados sobre as atitudes da empresa para proporcionar a segurança da informação.

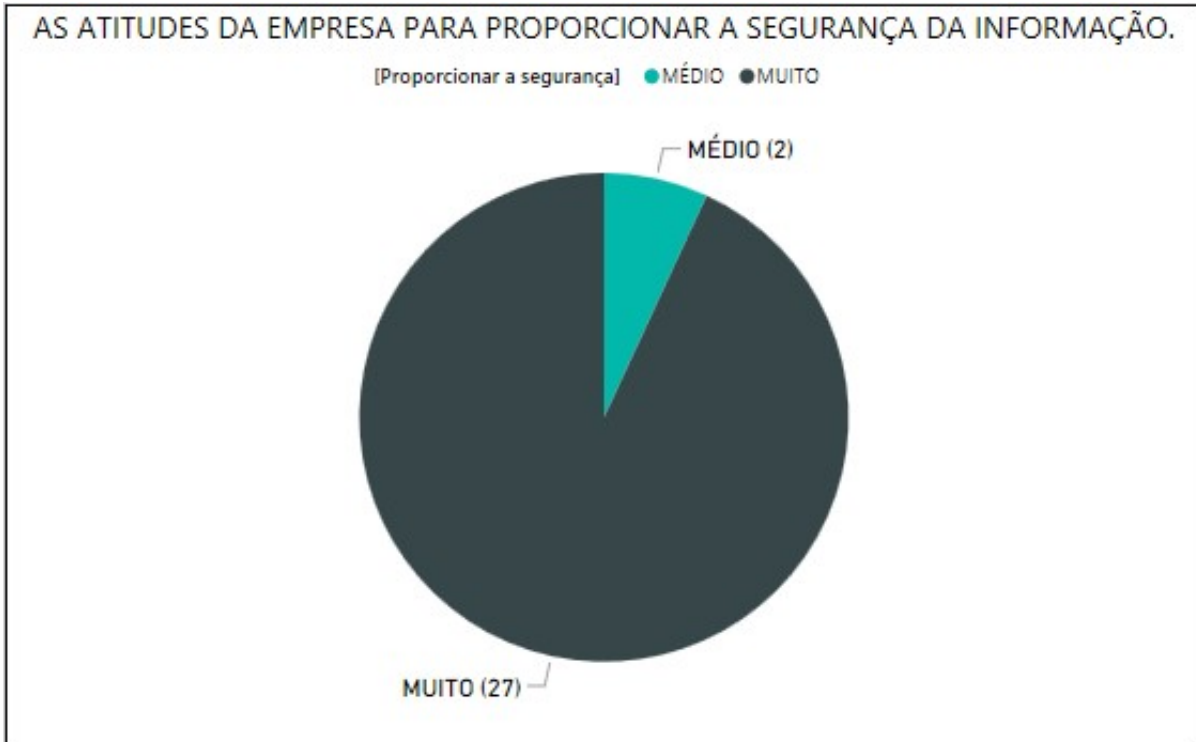


Gráfico 10. Atitudes da empresa para proporcionar a segurança da informação

Fonte: Próprio autor

O propósito desta questão foi avaliar acordo com os funcionários, como a organização tem agido para proporcionar maior segurança as informações. Conforme o gráfico 10, 27 usuários responderam que são muitas as ações realizadas para proporcionar maior segurança e 2 usuários consideraram medianas as ações.

O próximo assunto trata as atitudes de cada funcionário para proporcionar a segurança da informação.

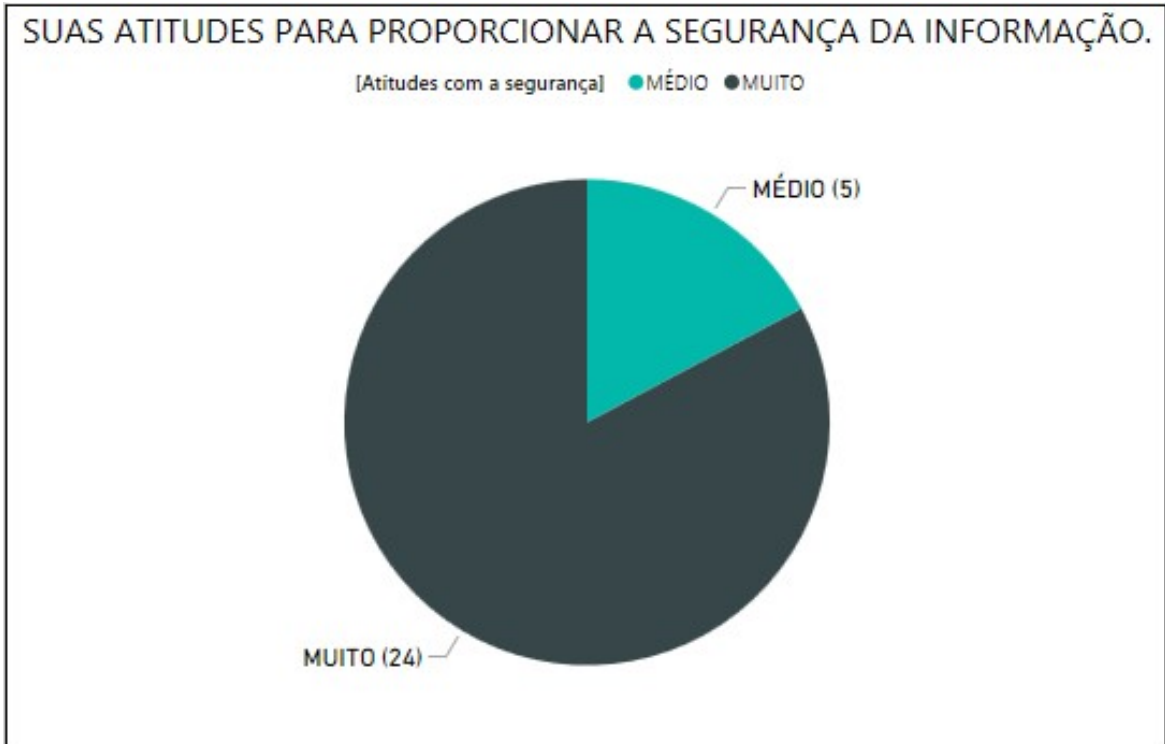


Gráfico 11. Suas atitudes para proporcionar a segurança da informação

Fonte: Próprio autor

Dos 29 usuários entrevistados, 24 responderam que são muitas as suas atitudes para proporcionar a segurança da informação e 5 classificaram como medianas suas ações. Podem ser consideradas ações que proporcionam a segurança, obter conhecimento da política de segurança e cumprir as regras estabelecidas.

A questão a seguir avalia como cada funcionário se comporta em relação a segurança da informação.

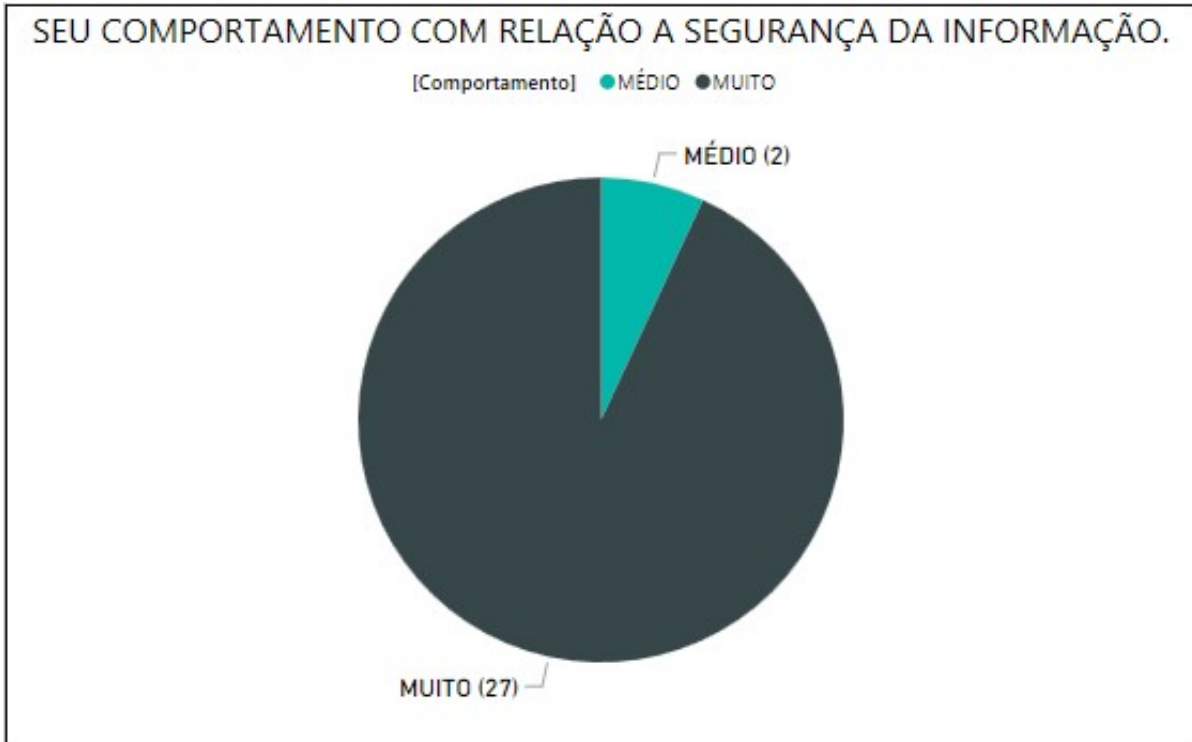


Gráfico 12. Seu comportamento com relação a segurança da informação

Fonte: Próprio autor

De acordo com o gráfico 12, 27 usuários responderam que é muito importante ter um comportamento que ajude a proporcionar maior segurança, enquanto 2 usuários classificaram como média a importância do comportamento. Essa avaliação demonstra como os usuários consideram a Política de Segurança.

A próxima questão visa demonstrar de acordo com os usuários, o quanto a organização investe em segurança da informação.

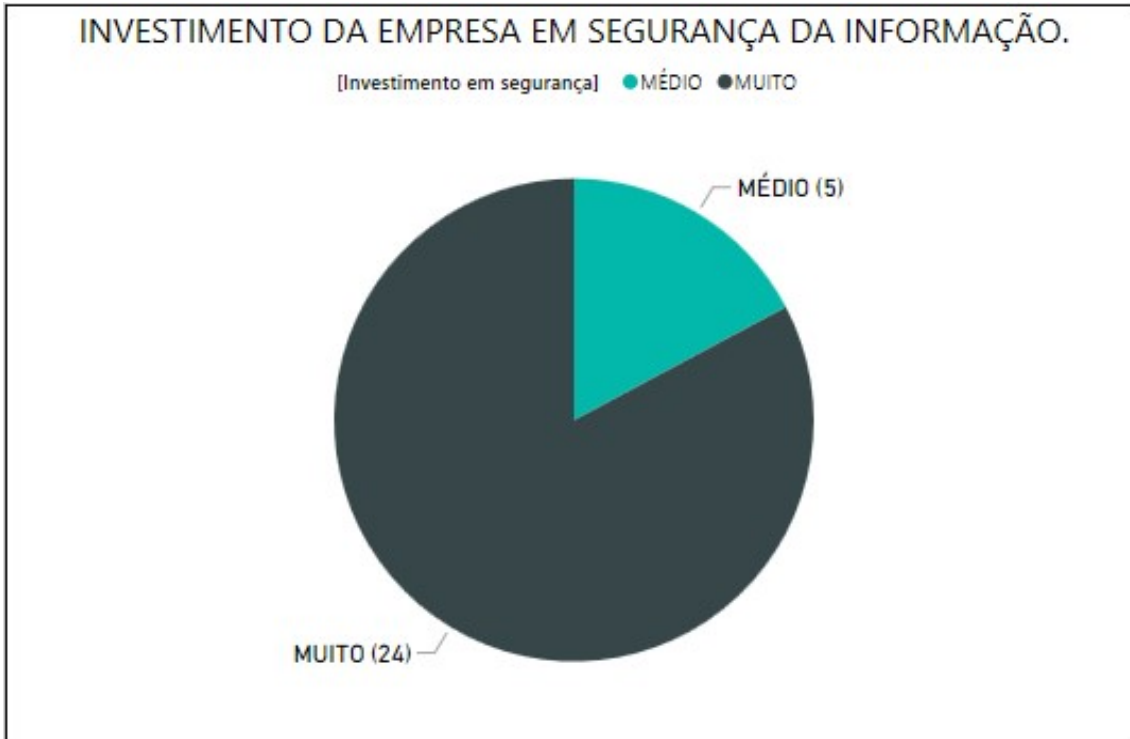


Gráfico 13. Investimento da empresa em segurança da informação

Fonte: Próprio autor

Como demonstrado no gráfico 13, 24 usuários disseram que são muitos os investimentos da empresa em segurança da informação e 5 classificaram como mediano os investimentos em segurança.

Do ponto de vista dos funcionários, essa questão avalia os serviços prestados referente a segurança da informação.

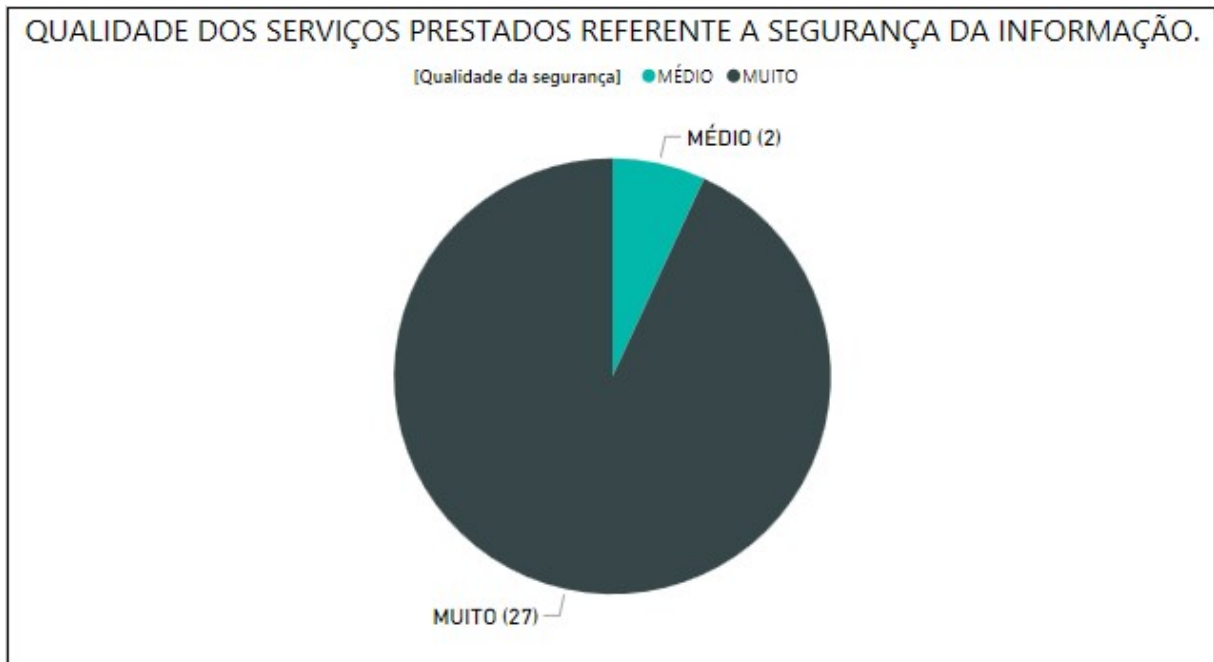


Gráfico 14. Qualidade dos serviços prestados referente a segurança da informação

Fonte: Próprio autor

O gráfico acima mostra a avaliação dos usuários sobre os serviços prestados pelo departamento de Tecnologia da Informação da empresa. Como pode ser visto no gráfico 14, 27 usuários responderam como muito a qualidade dos serviços prestados e 2 classificaram como mediana a qualidade.

De acordo com os usuários, a próxima questão classifica a importância das orientações sobre as práticas para maior segurança da informação.

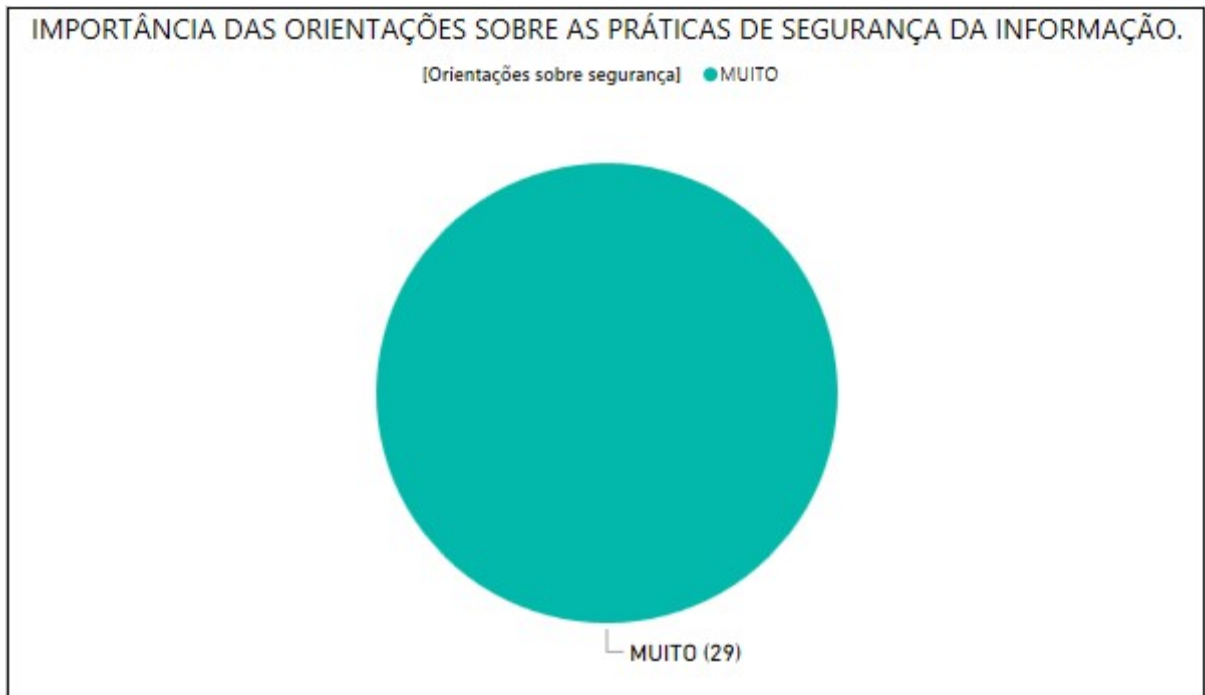


Gráfico 15. Importância das orientações sobre as práticas de segurança da informação

Fonte: Próprio autor

O objetivo deste ponto, é saber como os usuários consideram as instruções que tem o propósito de promover maior segurança na rede de computadores. O gráfico 15 mostra que 100% dos usuários que responderam o questionário, classificaram como muito importante as orientações de segurança da informação.

Através dos resultados apresentados, pode-se dizer que o objetivo de promover a segurança da informação a rede de computadores da empresa foi alcançado. A segurança da informação foi visada desde os aspectos tecnológicos até os fatores de ambiente de trabalho da organização.

No próximo capítulo poderá ser visto a conclusão obtida com a realização deste trabalho.

4. CONCLUSÃO

O desenvolvimento do presente trabalho, possibilitou a análise e aplicação de elementos para promover a segurança da informação em um ambiente de rede de computadores empresarial, utilizando o *Mikrotik RouterOS* com base nas diretrizes na ABNT NBR ISO/IEC 27001. A demonstração das ferramentas e metodologias apresentadas neste estudo, podem ser de grande valia para organizações que possuem dificuldades em manter seus dados seguros. Além disso, o estudo foi realizado utilizando-se várias referências bibliográficas, apresentando como os recursos podem ajudar a promover a segurança da informação.

Como pôde ser observado no desenvolvimento e resultados, a norma utilizada propõe métodos que envolvem recursos tecnológicos, ambiente e pessoas, atribuindo maior segurança aos dados de uma empresa. A utilização do *Mikrotik RouterOS* apoiado as instruções da ABNT NBR ISO/IEC 27001 e uma Política de Segurança da Informação documentada, tiveram resultados satisfatórios, comprovando a segurança das informações da organização.

Os testes foram realizados com ferramentas que são aplicadas em auditorias de redes de computadores. Como apresentado nos resultados, as execuções dos testes de intrusão contra a rede de computadores da concessionária não obtiveram êxito, mostrando que o *Mikrotik* é um sistema que possui métodos eficazes para promover a segurança da informação em ambiente de redes corporativas.

Além dos testes que foram executados, a empresa aderiu a uma Política de Segurança da Informação documentada que foi divulgada para todos os funcionários. Com essa ação, todos os usuários obtiveram conhecimento da importância que a organização atribui a segurança dos seus dados. Após a divulgação da política de segurança, foi aplicado um questionário onde os funcionários avaliaram o ambiente de tecnologia em relação as mudanças realizadas. Os resultados do questionário apresentados em gráficos, demonstram como os funcionários aprovaram a Política de Segurança da Informação.

Para a realização desse trabalho, utilizou-se a ABNT NBR ISO/IEC 27001, que fornece quesitos para promover a segurança da informação, onde doze de suas diretrizes foram atendidas. Sendo assim, o presente estudo pode contribuir com outros trabalhos que se apoiam em uma ISO voltada a segurança da informação.

O objetivo geral do trabalho, foi promover a segurança da informação em uma

organização onde não havia um processo padronizado com este propósito. Mediante os resultados obtidos, pode-se afirmar que o objetivo foi alcançado, comprovando que um ambiente de redes de computadores bem estruturado e que utiliza uma Política de Segurança da Informação interna, possuem seus dados protegidos.

4.1 TRABALHOS FUTUROS

O *Mikrotik RouterOS* permite a configuração de um servidor PPTP ou cliente PPTP, conforme pode ser revisto no capítulo 2. Essa configuração possibilita que duas empresas, sendo uma a matriz e a outra filial, com localizações geograficamente distantes, trabalhem interligadas por uma conexão segura.

Sendo assim, uma forma de trabalho futuro seria utilizar o *Mikrotik RouterOS* nas duas empresas, com o intuito de interligá-las por conexão PPTP (VPN). Também poderiam ser aplicadas outras diretrizes da ABNT NBR ISO/IEC 27001, além das apresentadas neste trabalho.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**. Rio de Janeiro: 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**. Rio de Janeiro: 2006.

ABNT. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. Disponível em: <<http://www.abntcatalogo.com.br/norma.aspx?ID=306582>>. Acesso em 27 abr. 2016.

AKAMAI. **Akamai's [state of the internet] / security Q3 2016 report**. Disponível em: <<https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf>>. Acesso em 21 de outubro de 2016.

AVAST. **Avast For Business**. Disponível em: <<https://www.avast.com/pt-br/avast-for-business>>. Acesso em 16 de novembro de 2016.

CARVALHO, Luciano Gonçalves de. **Segurança de Redes**. 1. Ed. Rio de Janeiro: Editora Ciência Moderna, 2005.

DANTAS, Marcelo Leal. **Segurança da Informação**. 1. Ed. Olinda: Livro Rápido – Elógica, 2011.

DEALERNET AUTOMOTIVE ECOSYSTEM. **Dealernet Wiki**. Disponível em: <<http://www.dealernet.com.br/>>. Acesso em 8 de outubro de 2016.

FERNANDES, Jorge Henrique Cabral. **Gestão da Segurança da Informação e Comunicações**. Volume 1. Universidade de Brasília, Brasília, 2010.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação: Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações**. 1. Ed. Rio de Janeiro: Editora Brasport, 2012.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3. Ed. São Paulo: Bookman, 2006.

GIAVAROTO, Sílvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtrack Linux – Auditoria e Teste de Invasão em Redes de Computadores**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2013.

GOOGLE. **Google Drive**. 2016. Disponível em < <https://drive.google.com/drive/my-drive>>. Acesso em 2 de outubro de 2016.

KALI LINUX TOOLS. **DNSMAP**. 2014. Disponível em < <http://tools.kali.org/information-gathering/dnsmap>>. Acesso em 9 de outubro de 2016.

KALI LINUX OFFICIAL DOCUMENTATION. 2016. **What is Kali Linux?**. Disponível em: <<http://docs.kali.org/introduction/what-is-kali-linux>>. Acesso em 7 de outubro de 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 5. Ed. São Paulo, 2009.

LOPES, Rafael Carlos. **Você conhece o RouterOS Mikrotik?** 2011. Disponível em: <<https://www.vivaolinux.com.br/artigo/Voce-conhece-o-RouterOS-Mikrotik?pagina=1>>. Acesso em 24 set. 2016.

MIKROTIK DOCUMENTATION. **Mikrotik Manual Winbox**. Disponível em: <http://wiki.Mikrotik.com/wiki/Manual:Winbox#Starting_the_Winbox>. Acesso em 30 de outubro de 2016.

MÓDULO. **9a Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro: Módulo Security Solutions S.A., 2003.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos**. 7. Ed São Paulo: Novatec Editora, 2007.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. 2. Ed. Rio de Janeiro: Elsevier Editora, 2014.

SILVA, Anderson Marques. **Mikrotik RouterOS**. 2012. Disponível em: <<http://187.7.106.14/rafael/Unidades%20Curriculares/Artigos/Anderson%20Silva%20-%20Revisado.pdf>>. Acesso em 24 set. 2016.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. Ed. Campus, 2003.

TEAMVIEWER. **Informações do TeamViewer**. Disponível em: <www.teamviewer.com/pt/>. Acesso em 30 outubro de 2016.

TORRES, Gabriel. **Redes de Computadores: Curso Completo**. 1. Ed. Rio de Janeiro: Axcel Books do Brasil Editora, 2001.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas Práticas de Segurança da Informação**. 4. Ed. Brasília, 2012.

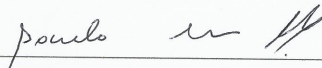
ANEXO 1 – AUTORIZAÇÃO PARA REDAÇÃO DE ESTUDO DE CASO

FORMULÁRIO DE LIBERAÇÃO PARA REDAÇÃO DE ESTUDO DE CASO

Pela presente, em nome da MINASVEL MINAS VEICULOS LTDA, a qual represento neste ato, autorizo Matheus Phillipe de Oliveira Ribeiro a iniciar um estudo de caso para fins acadêmicos para a FACULDADES INTEGRADAS DE CARATINGA (FIC), autorizo o uso do nome empresarial para a redação, podendo distribuí-lo e publicá-lo em sites, revistas, livros e coletâneas de casos que venham a ser organizados pela citada escola, sem nenhum ônus, cedendo todos os direitos inerentes a propriedade intelectual do caso à FIC.

Data: 21/06/2016

Assinatura: _____



Nome completo do representante legal: Paulo Cezar Alves

Empresa: Minasvel Minas Veículos Ltda

CNPJ: 20.811.105/0001-38

Endereço: Av. Presidente Tancredo Neves nº 2225, Centro, Caratinga MG

Telefone: (33) 3329-4250

ANEXO 2 – DOCUMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO MINASVEL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Segundo a ISO/IEC 27002:2005, a informação é um ativo que como qualquer outro ativo é importante, é essencial para os negócios de uma organização e deve ser adequadamente protegida. A informação é encarada, atualmente, como um dos recursos mais importantes de uma organização, contribuindo decisivamente para a uma maior ou menor competitividade.

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

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. MINASVEL E A POLÍTICA DE SEGURANÇA

As normas aqui listadas foram analisadas e aprovadas pela diretoria das empresas Minasvel e PCA Filho. Todos os funcionários, parceiros ou prestadores de serviços devem seguir com cautela 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 na internet ou na rede interna podem estar sendo monitorados.

1.2. NÃO CONFORMIDADE COM A POLÍTICA DE SEGURANÇA

O não cumprimento das orientações ou normas desta política de segurança acarretará em sanções administrativas em primeira instância, podendo ocorrer o desligamento do funcionário dependendo do nível ou gravidade do ocorrido.

2. AUTENTICAÇÃO

O meio de autenticação nos sistemas informatizados será baseado por uma senha. Este tipo de autenticação é o mais utilizado atualmente devido ao seu baixo custo e a facilidade de manutenção. Outros tipos como autenticação por biometria ou token são mais seguros, mas possuem custo elevado, além de uma implantação mais complexa.

A utilização de senhas que contenham nome de usuário, combinações simples (abcd1234), substantivos (casa, caneta, cadeira), datas (12091999) são fáceis de descobrir. No próximo tópico será demonstrado de maneira simples como criar senhas fortes e mais fáceis de memorizar.

2.1. POLÍTICA DE SENHAS

Uma senha para ser considerada segura deverá conter no mínimo 6 caracteres alfanuméricos e utilizando-se sempre caixas diferentes. Para aumentar ainda mais a força da senha pode-se utilizar um caractere em caixa alta ou até mesmo inserir um símbolo especial (^, !, /). Facilitando a memorização podemos usar palavras ou trechos de palavras que lidamos no dia-a-dia na formação das senhas.

Exemplo: Veic#8, 08test* ou 017@Toro

As senhas terão um tempo de validade determinado pelo departamento de TI, após o vencimento deste prazo a senha irá expirar e para ter acesso novamente ao sistema o usuário deverá criar uma nova senha. Não será permitido a renovação de senhas que já foram utilizadas anteriormente.

O usuário será responsável por tudo que for executado com a sua senha, por isso é de grande importância mantê-la secreta.

3. E-MAIL

Os tópicos a seguir possuem detalhes para a utilização de e-mail empresarial de forma segura. Deixar de seguir uma destas orientações pode colocar em risco todos os sistemas que estão conectados na rede de computadores interna.

- Não abra anexos com as extensões .bat, .exe, .src, .lnk, .HTML e .com se não tiver certeza absoluta de que solicitou esse e-mail;
- Não abra anexos de e-mails com assuntos estranhos, onde no campo remetente e destinatário está informando o mesmo endereço de e-mail.
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc;
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc;
- Não utilize o e-mail da empresa para assuntos pessoais;
- Não mande e-mails para um grande número de pessoas de uma única vez (to, cc, cco)
- Evite anexos muito grandes;
- Utilize sempre sua assinatura para enviar e-mails;
- Em caso de dúvida sobre algum link ou anexo em um e-mail procurar o departamento de TI antes de tentar visualizar o conteúdo.

MINASVEL

4. ACESSO A INTERNET

- O uso recreativo da internet não poderá acontecer durante o horário de expediente.
- Somente a navegação em sites ou sistemas online relacionados com o trabalho são permitidos. A utilização de protocolos específicos deve ser solicitada ao departamento de TI, com a previa autorização do gerente responsável.
- O acesso a conteúdo na internet é bloqueado, somente sites relacionados com o trabalho tem acesso livre. Caso haja a necessidade de liberação de algum site ou serviço online, a solicitação deve ser passada para o departamento de TI.
- Não é permitido a utilização de programas ou ferramentas que utilizam o protocolo P2P para realizar downloads.
- O uso da internet para o envio de mensagens instantâneas somente estará permitido para funcionários autorizados por seus gerentes.

5. USO DAS ESTAÇÕES DE TRABALHO

Todos os equipamentos da rede de computadores possuem um endereço IP tornando possível a sua identificação. Cada usuário 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 a causa de determinados problemas.

- Não é permitida a instalação de softwares/programas nos computadores. Caso haja a necessidade a equipe de TI deverá ser consultada.
- Não tenha em seu computador arquivos MP3, filmes, softwares/programas com direitos autorais. Além de colocar em risco os sistemas internos, empresa pode ser autuada por pirataria.
- A utilização de mídias removíveis (pen drive, CD, DVD) somente é permitida com a autorização do gerente do departamento.

6. POLÍTICA SOCIAL

Independente de sistemas computacionais, software ou hardware utilizado, o elemento mais vulnerável de sistemas de segurança da informação é o ser humano (NAKAMURA, 2007). Sem perceber podemos estar passando informações relevantes a pessoas mal-intencionadas que podem colocar em riscos os dados da empresa.

- Não fale ou mande sua senha de forma alguma para outras pessoas.
- Não utilize seu usuário e senha em máquinas de terceiros, principalmente se for fora da empresa.
- Não aceite ajuda técnica de pessoas que não sejam da equipe de TI da empresa.
- Nunca execute procedimentos técnicos que tenham chegado por e-mail antes de consultar a equipe de TI.
- Relate para o departamento de TI pedidos internos ou externos que venham a discordar dos procedimentos anteriores.
- Não comente com ninguém sobre detalhes técnicos do seu trabalho, principalmente se for externo da empresa.

7. UTILIZAÇÃO DE REDES SEM FIO (WIFI)

A Minasvel possui redes Wireless distinta, para uso dos funcionários em suas tarefas relacionadas com o trabalho e para os clientes onde o acesso à internet é liberado. A rede sem fio acessada pelos funcionários durante o expediente possui as mesmas políticas de segurança que a rede cabeada. Para garantir que pessoas não autorizadas acessem a rede, a senha não é disponibilizada para os funcionários. Para maior segurança a senha é configurada diretamente no dispositivo por um responsável do departamento de TI.

Os clientes têm acesso a internet sem fio por meio de uma placa que fica na sala vip da concessionária, com o nome e a senha da rede wifi. Essa rede wireless não tem comunicação com a rede interna da Minasvel, evitando que os dados da empresa sejam acessados ou danificados por agentes externos.

As regras abaixo devem ser seguidas para o uso das redes wireless:

- A rede wifi destinada para os clientes poderá ser utilizada por funcionários no horário de expediente somente com autorização do gerente.
- Os computadores da empresa estão configurados para não acessarem a rede wifi destinada para os clientes.
- A senha da rede sem fio destinada para os clientes poderá ser alterada por determinação do administrador da rede ou a pedido da diretoria.
- Nenhum dispositivo pessoal (smartphones, tablets, notebooks) poderá ser conectado nas redes wireless exclusivo para o trabalho na Minasvel.
- A política de acesso a conteúdo na internet utilizando o wifi exclusivo para o trabalho é idêntica à política da rede cabeada.
- O acesso a qualquer uma das redes sem fio poderá ser bloqueado utilizando o endereço físico do dispositivo, por determinação do administrador da rede ou diretoria.

Alf Cluemen Ricardo
Mauricio
Douza
B. Pachus magela
Dan
A. L. d. S. S. S. S.
Daniel
Karina
Daniel

ANEXO 3 – TERMOS DE RESPONSABILIDADE NO USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

TERMOS DE RESPONSABILIDADE NO USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

1. (Nome do Funcionário, RG: (0000000000), CPF: 000.000.000-00, Matrícula 0000000, colaborador da (Nome da Empresa), na função (do funcionário), declaro para os devidos fins que recebi desta empresa todas as informações referentes à Política de Segurança da Informação com as regras que disciplinam a utilização de soluções e recursos de Tecnologia da Informação (TI) e colocados à minha disposição para exercício de minhas atividades laborais, sendo responsável por:

a) receber as senhas vinculadas ao meu código de usuário, destinadas ao acesso às ferramentas (softwares e hardwares) de TI disponíveis na (Nome da Empresa), são de meu uso pessoal e intransferíveis, sendo meu dever garantir sua proteção, sigilo e assumir a responsabilidade por todas as transações efetuadas sob esse código de identificação;

b) cumprir as normas e regras da Política de Segurança da Informação para utilização dos recursos e soluções de TI fornecidas pela (Nome da Empresa), em todo acesso obtido por meio do meu código de usuário e da senha a ele vinculado, inclusive nos casos em que o acesso seja realizado a partir de equipamentos e canais de comunicação não pertencentes a (Nome empresa);

c) manter sigilo sobre todas as informações técnicas, comerciais e de negócio recebidas ou acessadas nos meios fornecidos pela (Nome da empresa), bem como de todas as informações obtidas em razão de meu acesso aos sistemas desta empresa, constituindo infração grave a divulgação de dados sigilosos da empresa;

d) responder pelo uso indevido ou fraudulento de recursos e soluções da TI, bem como a sua utilização para quaisquer outros fins que não sejam estritamente para as atividades e serviços realizados a (nome da empresa), sujeitando por perdas e danos, lucros cessantes que decorrer de tal ato, sem prejuízo das sanções penais cabíveis, só podendo divulgá-las com expressa autorização desta empresa;

Declaro, ainda:

a) estar ciente que a (Nome da Empresa) se resguarda o direito de suspender o meu acesso a sistemas de informação, correio eletrônico, internet e outras soluções e recursos de TI a qualquer momento, sem prévia comunicação e que a empresa efetua o monitoramento dos correios eletrônicos corporativos.

b) estar ciente que a (Nome da Empresa) poderá introduzir modificações nas normas e regras que disciplinam a utilização de soluções de TI a qualquer tempo, divulgando-as aos usuários por meio de comunicação escrita ou eletrônica, sendo tais modificações consideradas aceitas automaticamente quando de meu subsequente acesso a tais soluções.

(Cidade), (Dia) de (Mês) de (Ano).

(Matrícula) - (Nome do Funcionário)

(Nome Da Empresa ou Gestor de T.I.)

ANEXO 4 – INVENTÁRIO DOS ATIVOS

PUA - POSIÇÃO DE UTILIZAÇÃO ATUAL

Estou de acordo com as informações declaradas corretamente neste inventário

SIM	DATA DO INVENTÁRIO	06/10/2016
------------	---------------------------	-------------------

RAZÃO SOCIAL	
MINASVEL MINAS VEICULOS LTDA	
ENDEREÇO	
AV. PRESIDENTE TANCREDO NEVES - Nº 2235 - ZACARIAS - CARATINGA	
CONTATOS	
TELEFONE	(33) 33296250 / (33) 399508519
E-MAIL	Informatica@satminasvel.com.br
TOTAL DE UNIDADES (MATRIZ/ FILIAIS)	
1	

Total de Servidores Físicos:	2
Total de Servidores Virtuais:	0
Total de PC's/Notebooks:	38
Total de Thin Clients:	38
Total de dispositivos móveis com acesso à rede	7
Qual é o CRM que utiliza?	CLINK
Qual o Banco de Dados utilizado pelo CRM?	SQL Server 2008
Quanto usuários acessam informação do CRM?	11
Qual é o ERP que utiliza?	FlatNet
Qual o Banco de Dados utilizado pelo ERP?	SQL Server 2008
Quanto usuários acessam informação do ERP?	24

ESTAÇÕES DE TRABALHO (DESKTOPS E/OU NOTEBOOKS)					
PRODUTO	VERSÃO	EDIÇÃO	TOTAL INSTALADO	LOCAL	HOSPEDADO
Windows	Anterior (95/98)		0	0	0
	2000	Me	0	0	0
		Professional	0	0	0
	XP	Starter Edition	0	0	0
		Home Edition	1	1	0
	VISTA	Professional	4	4	0
		Starter Edition	0	0	0
		Home Basic	0	0	0
		Home Premium	0	0	0
		Business	0	0	0
	7	Ultimate	0	0	0
		Starter Edition	0	0	0
		Home Basic	0	0	0
		Home Premium	1	1	0
		Professional	0	0	0
	8	Ultimate	26	26	0
		Enterprise	0	0	0
		Single Language	6	6	0
	8.1	Professional	0	0	0
		Enterprise	0	0	0

SERVIDORES							
PRODUTO	VERSÃO	EDIÇÃO	TOTAL INSTALADO	VIRTUAIS	LOCAL	HOSPEDADO	
Windows Server	Standard Edition		2	0	2	0	
	Enterprise Edition		0	0	0	0	
	Datacenter Edition		0	0	0	0	
	HPC Server		0	0	0	0	
	Web Server		0	0	0	0	
	Storage Server		0	0	0	0	
	Foundation		0	0	0	0	
	Essentials Business		0	0	0	0	
	Small Business	Standard		0	0	0	0
		Premium Add-on		0	0	0	0
	Standard Edition		0	0	0	0	
	Web Server		0	0	0	0	
	HPC Server		0	0	0	0	
	Enterprise Edition		0	0	0	0	
	Datacenter Edition		0	0	0	0	
	Itanium		0	0	0	0	
	Foundation		0	0	0	0	
	Small Business	Standard		0	0	0	0
		Premium Add-on		0	0	0	0
	Standard		0	0	0	0	
	Datacenter		0	0	0	0	
	Foundation		0	0	0	0	
	Essentials		0	0	0	0	
	Standard		0	0	0	0	
	Datacenter		0	0	0	0	
	Foundation		0	0	0	0	
	Essentials		0	0	0	0	

CAL5	Device	2000	0	0	0		
		2003	0	0	0		
		2008	0	0	0		
	User	2000	0	0	0		
		2003	0	0	0		
		2008	4	4	0		
	Terminal Service	2000	0	0	0		
		2003	0	0	0		
	Remote Desktop Service (RDS)	2008	0	0	0		
		2012	0	0	0		
	Small Business	2000	0	0	0		
	Small Business Premium	2000	0	0	0		
	Small Business	2003	0	0	0		
	Small Business Premium	2003	0	0	0		
	Small Business	2008	0	0	0		
	Small Business Premium	2008	0	0	0		
	Small Business	2011	0	0	0		
	Small Business Premium	2011	0	0	0		
	External connector	-	0	0	0		
Rights Mgmt Service Device	-	0	0	0			
COMUNICAÇÃO UNIFICADA							
PRODUTO	VERSÃO	EDIÇÃO	TOTAL INSTALADO	LOCAL	HOSPEDADO		
Lync	Server	Standard	2010	0	0	0	
		Enterprise	2010	0	0	0	
		Standard	2013	0	0	0	
		Enterprise	2013	0	0	0	
	Client instalado máquina usuário		2010	1	1	0	
		2013	0	0	0		
Utiliza o Exchange integrado com o sistema de telefonia? (Selecionar SIM ou NÃO)				NÃO			
Utiliza o Lync integrado com o sistema de telefonia? (Selecionar SIM ou NÃO)				NÃO			
BANCO DE DADOS							
PRODUTO	VERSÃO	EDIÇÃO	TOTAL INSTALADO	VIRTUAIS	LOCAL	HOSPEDADO	
SQL Server	Standard	2008	1	0	1	0	
	Enterprise		0	0	0	0	
	Workgroup		0	0	0	0	
	Web	2008 R2	0	0	0	0	
	Standard		0	0	0	0	
	Enterprise		0	0	0	0	
	Workgroup	2012	0	0	0	0	
	Web		0	0	0	0	
	Standard		0	0	0	0	
	Enterprise	2014	0	0	0	0	
	Business Intelligence		0	0	0	0	
	Standard		0	0	0	0	
	Enterprise	2016	0	0	0	0	
	Business Intelligence		0	0	0	0	
	Standard		0	0	0	0	
	CAL		2000	0	0	0	0
			2005	0	0	0	0
			2008	1	0	1	0
			2008 R2	0	0	0	0
2012			0	0	0	0	
		2014	0	0	0	0	
Existe acesso externo ao SQL? (Selecionar SIM ou NÃO)			NÃO		QUANTOS?		
Para mais informações, acesse: Antipirataria Microsoft							

ANEXO 5 – RETORNO DA EXECUÇÃO DO NMAP COM AS FUNÇÕES -T4 -A -s

```
root@kali:~# nmap -T4 -A -v [REDACTED]
```

1. Starting Nmap 6.47 (<http://nmap.org>) at 2016-11-22 22:03 BRST
2. NSE: Loaded 118 scripts for scanning.
3. NSE: Script Pre-scanning.
4. Initiating Ping Scan at 22:03
5. Scanning [REDACTED] ([REDACTED]) [4 ports]
6. Completed Ping Scan at 22:03, 0.01s elapsed (1 total hosts)
7. Initiating Parallel DNS resolution of 1 host. at 22:03
8. Completed Parallel DNS resolution of 1 host. at 22:03, 0.28s elapsed
9. Initiating SYN Stealth Scan at 22:03
10. Scanning [REDACTED] ([REDACTED]) [1000 ports]
11. Completed SYN Stealth Scan at 22:03, 4.03s elapsed (1000 total ports)
12. Initiating Service scan at 22:03
13. Initiating OS detection (try #1) against [REDACTED] ([REDACTED])
14. Retrying OS detection (try #2) against [REDACTED] ([REDACTED])
15. Initiating Traceroute at 22:03
16. Completed Traceroute at 22:03, 0.02s elapsed
17. Initiating Parallel DNS resolution of 2 hosts. at 22:03
18. Completed Parallel DNS resolution of 2 hosts. at 22:03, 0.12s elapsed
19. NSE: Script scanning [REDACTED].
20. Initiating NSE at 22:03
21. Completed NSE at 22:03, 0.00s elapsed
22. Nmap scan report for [REDACTED] ([REDACTED])
23. Host is up (0.0036s latency).
24. rDNS record for [REDACTED]: [REDACTED].supercabotv.com.br
25. All 1000 scanned ports on [REDACTED] ([REDACTED]) are filtered
26. Too many fingerprints match this host to give specific OS details
27. Network Distance: 2 hops

28. TRACEROUTE (using port 80/tcp)

29. HOP RTT ADDRESS

1 2.85 ms 10.0.2.2

2 2.99 ms [REDACTED].supercabotv.com.br ([REDACTED])

30. NSE: Script Post-scanning.

31. Read data files from: /usr/bin/./share/nmap

32. OS and Service detection performed. Please report any incorrect results at
<http://nmap.org/submit/>.

33. Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds

34. Raw packets sent: 2053 (94.624KB) | Rcvd: 18 (736B)

ANEXO 6 – LOG DO ATAQUE COM XHYDRA

```

root@kali:~# hydra -R
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2016-11-24 13:49:09
[DATA] max 16 tasks per 1 server, overall 64 tasks, 117 login tries (l:9/p:13), ~0 tries per task
[DATA] attacking service asterisk on port ██████████
*** glibc detected *** hydra: double free or corruption (out): 0x00007f02a8ac5d80 ***
===== Backtrace: =====
/lib/x86_64-linux-gnu/libc.so.6(+0x75bb6)[0x7f02a6047bb6]
/lib/x86_64-linux-gnu/libc.so.6(cfree+0x6c)[0x7f02a604c95c]
hydra(+0x1032b)[0x7f02a83c32b]
hydra(main+0x1f3b)[0x7f02a83c486b]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xfd)[0x7f02a5ff0ead]
hydra(+0xc0b5)[0x7f02a83c80b5]
===== Memory map: =====
7f029c000000-7f029c021000 rw-p 00000000 00:00 0
7f029c021000-7f02a0000000 ---p 00000000 00:00 0
7f02a2b1e000-7f02a2b23000 r-xp 00000000 08:01 677594 /lib/x86_64-linux-gnu/libnss_dns-2.13.so
7f02a2b23000-7f02a2d22000 ---p 00005000 08:01 677594 /lib/x86_64-linux-gnu/libnss_dns-2.13.so
7f02a2d23000-7f02a2d24000 rw-p 00005000 08:01 677594 /lib/x86_64-linux-gnu/libnss_dns-2.13.so
7f02a2f26000-7f02a2f31000 r-xp 00000000 08:01 677595 /lib/x86_64-linux-
7f02a3135000-7f02a3334000 ---p 00003000 08:01 653808 /lib/x86_64-linux-gnu/libgpg-error.so.0.8.0
7f02a3334000-7f02a3335000 rw-p 00002000 08:01 653808 /lib/x86_64-linux-gnu/libgpg-error.so.0.8.0
7f02a3335000-7f02a3346000 r-xp 00000000 08:01 143438 /usr/lib/x86_64-linux-gnu/libp11-kit.so.0.0.0
7f02a3346000-7f02a3545000 ---p 00011000 08:01 143438 /usr/lib/x86_64-linux-gnu/libp11-kit.so.0.0.0
7f02a3545000-7f02a3546000 r-p 00010000 08:01 143438 /usr/lib/x86_64-linux-gnu/libp11-kit.so.0.0.0
7f02a3546000-7f02a3547000 rw-p 00011000 08:01 143438 /usr/lib/x86_64-linux-gnu/libp11-kit.so.0.0.0
7f02a3547000-7f02a3557000 r-xp 00000000 08:01 138468 /usr/lib/x86_64-linux-gnu/libtasn1.so.3.1.16
7f02a3758000-7f02a37d3000 r-xp 00000000 08:01 654190 /lib/x86_64-linux-gnu/libgcrypt.so.11.7.0
7f02a37d3000-7f02a39d3000 ---p 0007b000 08:01 654190 /lib/x86_64-linux-
f02a4fa0000 ---p 00003000 08:01 653785 /lib/x86_64-linux-gnu/libcom_err.so.2.1
7f02a4fa0000-7f02a4fa1000 r-p 00002000 08:01 653785 /lib/x86_64-linux-gnu/libcom_err.so.2.1
7f02a4fa1000-7f02a4fa2000 rw-p 00003000 08:01 653785 /lib/x86_64-linux-
gnu/libcom_err.so.2.1[STATUS] attack finished for ██████████ (waiting for children to finish) ...
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-11-24 14:03:15

```

ANEXO 7 – QUESTIONÁRIO SOBRE A SEGURANÇA DA INFORMAÇÃO NA EMPRESA

Questionária de Trabalho de Conclusão de Curso - Segurança da Informação
--

Informações Iniciais

NOME DO FUNCIONARIO (A):
CARGO:
GRAU DE ESCOLARIDADE:

Mudanças na rede de computadores.

Após as mudanças realizadas na rede de computadores da Minasvel, como você classificaria?	PÉSSIMO	RUIM	REGULAR	BOM	ÓTIMO
A organização atual dos dispositivos?					
A qualidade da rede atual?					
O acesso aos softwares utilizados?					
A sua segurança sobre as informações?					
A praticidade de acesso as informações?					
A recuperação de serviços após falhas?					
A utilização das redes wireless?					

Responsabilidade com a segurança da informação.

Sobre a segurança da informação atual na organização, avalie:	NENHUM	POUCO	MÉDIO	MUITO
A importância da segurança para a empresa.				
A importância que você atribui a segurança da informação.				
As atitudes da empresa para proporcionar a segurança da informação.				
Suas atitudes para proporcionar a segurança da informação.				
Seu comportamento com relação a segurança da informação.				
Investimento da empresa em segurança da informação.				
Qualidade dos serviços prestados referente a segurança da informação.				
Importância das orientações sobre as práticas de segurança da informação.				

Deixe sua opinião sobre o que pode ser melhorado referente a tecnologia e segurança da informação na empresa Minasvel.	
--	--