UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

MAIARA MIRANDA BARDINI

DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

CRICIÚMA
2015

MAIARA MIRANDA BARDINI

DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

Trabalho de Conclusão do Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Rogério Antônio Casagrande

Coorientador: Prof. MSc. Kristian Madeira

CRICIÚMA

2015

MAIARA MIRANDA BARDINI

DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em redes de computadores.

Criciúma, 26 de novembro de 2015.

BANCA EXAMINADORA

Prof. Rogério Antônio Casagrande - MSc - (UNESC) - Orientador

Prof. Kristian Madeira - MSc - (UNESC) - Coorientador

Prof. Paulo João Martins -MSc - (UNESC)

Prof. Valter Blauth Junior - Esp - (UNESC)

Dedico este trabalho primeiramente a Deus, aos meus pais Judinei, Anadir e ao meu irmão Alan por estarem sempre ao meu lado nas horas mais difíceis.

AGRADECIMENTOS

Eu agradeço primeiramente a Deus, por me dar forças para seguir em frente e não desistir nunca dos meus sonhos.

Aos meus pais, Judinei, Anadir e ao meu irmão Alan, pelo apoio, compreensão, amor, carinho, e por me ensinar o significado de família. AMO VOCÊS!

Tenho a agradecer a todos meus familiares, principalmente aos meus primos Cassiano, Thaís Biz, Karen, Thaís Bardini, Renata, Marina, Francine, Franciele e Elaine pelo apoio nos momentos que mais precisei.

A todos os colegas de faculdade, principalmente as minhas amigas Jéssica, Morgana, Maitê e ao meu amigo Maicon, por estarem sempre ao meu lado em momentos bons e ruins e por terem muita paciência comigo.

Ao meu Patrão Ivanor Maragno (*in memoriam*), por me apoiar em momentos da minha vida que pensei em desistir, pelo seu jeito calmo e atencioso.

Tenho muito a agradecer a Gisele e a Margarete, pelo apoio, conselhos, por me acalmar em minhas crises de choros e por muitas risadas.

A todos os professores do curso de Ciência da Computação, ao professor Paulo e a professora Merisandra pela ajuda em meu trabalho e por todo carinho.

Ao meu Orientador Rogério Antônio Casagrande e meu Coorientador Kristian Madeira por me auxiliarem na elaboração deste trabalho. Agradeço carinhosamente vocês dois pelos conselhos, dicas, por me fazer rir nos momentos bons e ruins.

Ao meu namorado Andrei, por me compreender nos momentos mais difíceis, pela paciência, amor e carinho.

Enfim, por todos que de uma maneira ou outra me ajudaram durante o curso!

“Um homem que não se alimenta de seus sonhos, envelhece cedo.”

William Shakespeare

RESUMO

A expansão tecnológica trouxe facilidade em acessar a Internet, mas junto com ela surgiram também vários problemas quanto à segurança. No presente trabalho de conclusão de curso objetivou explorar a segurança das redes sem fio domésticas, por meio de uma análise dos procedimentos de segurança adotados. Para tanto, foi realizada uma pesquisa por amostragem aplicada aos acadêmicos do Curso de Ciência da Computação regulamente matriculados no segundo semestre do ano de 2015. Deste modo, notou-se que muitas falhas de segurança nas redes Wi-Fi são causadas pelo desconhecimento ou por falta de preocupação dos próprios usuários, porquanto sequer conhecem políticas de segurança ou, aqueles que possuem algum conhecimento, não demonstram a preocupação sobre a importância destes procedimentos básicos. O grande problema se encontra nas redes mal configuradas, e no desinteresse dos usuários com a segurança, sendo assim sujeitas a invasões. Assim, ao identificar as vulnerabilidades contidas nas redes, foi proposto um cenário para aplicação prática de uma política de segurança mínima para demostrar os métodos utilizados no experimento como, por exemplo, o uso de senhas complexas, criptografia, verificar a lista de DHCP, filtros de MAC, entre outros, para minimizar os problemas encontrados.

Palavras – chave: Redes sem fio. Política de Segurança. Práticas seguras.

ABSTRACT

The technological expansion brought facility in accessing the Internet, but it brought together also a number of problems regarding security. This work aimed to explore the security of domestic wireless networks through an analysis of the adopted security procedures. For this purpose, a sample survey was applied to the students of the Computer Science course regularly enrolled in the second semester of 2015. In this way, it was noticed that many security flaws in Wi-Fi networks are caused by the lack of knowledge or lack of concern of the users, because they do not even know the security policies, or those who have some knowledge do not show concern about the importance of these basic procedures. The biggest problem is related to the misconfiguration of the networks and the lack of interest of users with security, therefore subject to invasions. Thus, when the vulnerabilities in networks were identified, it was proposed a scenario for practical application of minimal security policies to demonstrate the methods used in the experiment, such as the use of complex passwords, encryption, checking the DHCP list, MAC's filters, among others, to minimize the problems encountered.

Keywords: Wireless networks. Security policy. Safe practices.

LISTA DE ILUSTRAÇÕES

Figura 1 - Topologia em barramento 19
Figura 2 - Topologia em anel 20
Figura 3 - Topologia em estrela 21
Figura 4 - Topologia sem fio (Wireless) 26
Figura 5 - Topologia estrela - estendida 27
Figura 6 - Topologia malha (mesh) 28
Figura 7 - Placa de rede 29
Figura 8 - Access Point (AP) 29
Figura 9 - Taxonomia 35

LISTA DE TABELAS

Tabela 1 - Plano de amostragem 45
Tabela 2 – Idade e Sexo 46
Tabela 3 – Q1, Q2, Q3, Q4 47
Tabela 4 - Q5, Q6.....49
Tabela 5 – Q7.....50
Tabela 6 – Q7.....51
Tabela 7 – Q7.....52
Tabela 8 – Q8.....53
Tabela 9 – Q9, Q10.....54
Tabela 10 – Q11, Q12, Q13 55
Tabela 11 – Q14.....56
Tabela 12 – Q15, Q16.....57
Tabela 13 – Q17.....58
Tabela 14 – Q18.....59
Tabela 15 – Q19.....60
Tabela 16 - Cruzamento questão Q3 x Q7.....61
Tabela 17 - Cruzamento questão Q3 x Q7.....62
Tabela 18 - Cruzamento questão Q3 x Q8 e Q3 x Q9 63
Tabela 19 - Cruzamento questão Q3 x Q10, Q3 x Q12 e Q3 x Q13 64
Tabela 20 - Cruzamento questão Q3 x Q14.....66

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
Bps	Bits por Segundo
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
GHz	Gigahertz
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
Mbps	Megabit por segundo
MIMO	Multiple-Input, Multiple-Output
Ms	Milissegundos
PMC	Prefeitura Municipal de Criciúma
PSK	Pre Shared Key
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
WAN	Wide Area Network
WEP	Wired Equivalente Privacy
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access2

SUMÁRIO

1 INTRODUÇÃO 14
1.1 OBJETIVO GERAL 15
1.2 OBJETIVOS ESPECÍFICOS 15
1.3 JUSTIFICATIVA 15
2 REDES DE COMPUTADORES 17
2.1 COMPONENTES FÍSICOS DE UMA REDE 17
2.1.1 Hubs 17
2.1.2 Bridges (Pontes) 18
2.1.3 Comutadores (Switch) 18
2.1.4 Router (Roteadores) 18
2.1.5 Gateways 19
2.2 TOPOLOGIAS DE REDES 19
2.2.1 Topologia em barramento 19
2.2.2 Topologia em anel 20
2.2.3 Topologia em estrela 20
3 REDES SEM FIO 22
3.1 PADRÕES DE REDES SEM FIO 22
3.1.1 Padrão IEEE 802.11b 22
3.1.2 Padrão IEEE 802.11a 23
3.1.3 Padrão IEEE 802.11g 23
3.1.4 Padrão IEEE 802.11n 23
3.2 CRIPTOGRAFIAS PARA SEGURANÇA 24
3.2.1 Protocolos Wired Equivalente Privacy (WEP) 24
3.2.2 Protocolos Wi-Fi Protected Access (WPA) 24
3.2.3 Protocolos Wi-Fi Protected Access 2 (WPA2) 25
3.3 TOPOLOGIA SEM FIO (WIRELESS) 26
3.3.1 Topologia estrela - estendida 26
3.3.2 Topologia malha (mesh) 27
3.4 REDES SEM FIO DOMÉSTICAS 28
3.4.1 Funcionalidades de equipamentos de redes sem fio domésticas 28
3.4.2 Placas de redes sem fio 28
3.4.3 Access Point (AP) 29

3.4.4 Antenas 30
3.5 TIPOS DE REDES SEM FIO DOMÉSTICAS 30
3.5.1 Banda larga móvel 30
3.5.2 Bluetooth 31
3.5.3 Infravermelho 31
3.5.4 Wi-Fi 32
4 SEGURANÇA DE REDES SEM FIO 33
4.1 POLÍTICA DE SEGURANÇA 33
4.2 PILARES DA SEGURANÇA 34
4.3 ENDEREÇOS MAC 34
4.4 MÉTODOS DE ATAQUES CONTRA REDES SEM FIO 35
4.5 VULNERABILIDADES 36
4.6 CONTRAMEDIDAS DE SEGURANÇA 36
4.6.1 Falsificando o IP/ sequestro de sessão 36
4.6.2 Ataques de negação de serviço (dos – denial of service) 37
4.6.3 Varredura (scanning) 37
4.6.4 Sniffers (farejadores) 38
4.6.5 Força Bruta (Brute Force) 38
5 TRABALHOS CORRELATOS 39
5.1 VULNERABILIDADE E SEGURANÇA EM REDES SEM FIO 39
5.2 SEGURANÇA EM REDE SEM FIO 39
5.3 EVOLUÇÃO DA SEGURANÇA EM REDES SEM FIO 40
5.4 UMA ABORDAGEM SEGURANÇA EM REDES WIRELESS 40
5.5 A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA 41
5.6 ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES 41
6 SEGURANÇA EM REDES SEM FIO DOMÉSTICAS 42
6.1 METODOLOGIA 42
6.1.1 Caracterização do ambiente da pesquisa 43
6.1.2 População e amostra 43
6.1.3 Plano de amostragem 44
6.1.4 Utensílios de coleta de dados 45
6.2 RESULTADOS OBTIDOS 45

6.2.1 Avaliação dos Resultados: Fases x Conhecimento.....46
6.2.2 Avaliação dos resultados: Cruzamento 60
7 APLICAÇÃO PRÁTICA DE UMA POLÍTICA DE SEGURANÇA MÍNIMA 68
8 CONCLUSÃO 71
REFERÊNCIAS.....73
APÊNDICE (S).....80
APÊNDICE A - QUESTIONÁRIO DE DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS 81
APÊNDICE B – ARTIGO.....84

1 INTRODUÇÃO

Com a evolução tecnológica a acessibilidade às redes sem fio se tornou um grande avanço em termos de facilidade e rapidez.

Esta expansão tecnológica trouxe para a sociedade moderna a inclusão digital, pois passou a dar mais mobilidade para seus usuários, permitindo que qualquer pessoa a qualquer hora, desde que se tenha um ponto de acesso a Wi-Fi, possa navegar pelo mundo da Internet.

De acordo com Teixeira e Silva (2012), as redes sem fio nada mais são que transmissões de informações por ondas de rádio, sem a utilização de cabos, o que justifica a acessibilidade e a facilidade do uso da Internet.

Com a grande expansão das redes sem fio domésticas é relevante destacar os problemas referentes à vulnerabilidade de segurança, sendo disponibilizadas por erros nas configurações de seus serviços (FIGUEIREDO; PINHEIRO; MELLO, 2011).

As invasões de redes têm sido um problema constante, pois se o intruso conseguir ter acesso à rede também terá a possibilidade de acesso aos dados existentes nela, podendo provocar sérios danos à mesma. Assim, com base de estudo da utilização das redes sem fio, pretendeu-se explorar as formas de segurança das redes sem fio domésticas.

No presente trabalho de conclusão de curso foi realizada uma pesquisa por meio de um questionário, aplicado com os acadêmicos do Curso de Ciência da Computação sobre a aplicação da segurança nas redes sem fio domésticas.

No cenário da aplicação prática sobre as políticas de segurança, foi proposto demonstrar formas básicas de proteção da rede, como por exemplo, o uso de senhas complexas, filtros de MAC, criptografia, entre outros.

O presente trabalho foi dividido em várias etapas, sendo que o primeiro capítulo analisa as redes de computadores juntamente com os componentes físicos de uma rede e as topologias de redes.

O segundo capítulo contém um estudo sobre as redes sem fio, dando ênfase nos padrões de redes e nas criptografias de segurança, bem como das redes sem fio domésticas e as funcionalidades dos seus equipamentos de redes.

O terceiro e o quarto capítulo abordam as formas mais comuns de segurança das redes sem fio e as contramedidas de segurança; no quinto capítulo

sobre a aplicação prática de uma política de segurança mínima. Já no sexto capítulo sobre os trabalhos correlatos e seus objetivos, sendo após apresentado o trabalho desenvolvido com sua análise e resultado.

Por fim, as etapas metodológicas e o tipo de pesquisa utilizada, caracterização do ambiente da pesquisa, população amostral, plano de amostragem e utensílios de coleta de dados e análise dos resultados obtidos, sendo posteriormente proposta uma política mínima de segurança.

1.1 OBJETIVO GERAL

Avaliar a utilização de redes sem fio domésticas com vistas às condições de usos e procedimentos de segurança da informação.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender o conceito de redes sem fio domésticas;
b) estudar políticas de segurança;
c) realizar uma pesquisa com os usuários sobre a segurança de redes sem fio domésticas;
d) avaliar resultados e propor uma política de segurança mínima para redes sem fio domésticas.

1.3 JUSTIFICATIVA

O mundo da tecnologia vem crescendo a cada dia, uma vez que o uso da Internet permitiu um avanço em termos de acessibilidade para toda a população. A facilidade do acesso à Internet é um dos maiores exemplos de expansão tecnológica.

O crescimento acelerado das redes sem fio juntamente com a expansão e a facilidade do acesso mostra-se evidente, pois no mercado atual elas vêm sendo mais divulgadas. Todavia, com esse crescimento surgem diversos problemas quanto à segurança tecnológica (DUARTE, 2010).

Diariamente, dados pessoais dos usuários são exibidos em suas redes domésticas, como senhas de banco, redes sociais, conversas particulares, entre outros, redes estas que muitas vezes não possuem a segurança adequada.

Tendo isso em vista, é fundamental conscientizar as pessoas da importância de manter suas redes domésticas seguras, para impedir o fácil acesso às informações e recursos compartilhados na rede.

Isso porque estes podem comprometer a rede, pois existem diversas formas de ataques na abrangência da mesma que podem ocorrer, trazendo insegurança para aqueles que a utilizam (PINZON, 2009).

A prevenção é umas das medidas excelentes, uma vez que é o conjunto mínimo que dificulta a exploração de possíveis falhas no sistema que possam ocorrer bem como a proteção que busca inibir possíveis tentativas de ataques que o sistema pode sofrer (BOF, 2010).

Este trabalho demonstra métodos e ações que podem ser utilizados para assegurar condições mínimas de segurança das redes sem fio domésticas, de modo que proporcione conhecimentos básicos acerca desta necessidade de implementação de níveis de segurança. Permitiu-se analisar as redes Wi-Fi, descrevendo as vulnerabilidades e as falhas contidas nas mesmas, a fim de diagnosticar e apresentar simples soluções para os problemas mais comuns enfrentados pelos usuários em suas redes domésticas.

2 REDES DE COMPUTADORES

As redes de computadores referem-se a vários computadores conectados por um dispositivo de comunicação, ou seja, são conexões entre dois ou mais computadores quando há troca de informações (TANENBAUM, 2003).

De acordo Martinez (sd, p. 1) explica que:

> As **redes de computadores** possibilitam que indivíduos possam trabalhar em equipes, compartilhando informações, melhorando o desempenho da realização de tarefas, e estão presentes no dia-a-dia de todos nós. São estruturas sofisticadas e complexas, que mantém os dados e as informações ao alcance de seus usuários.

2.1 COMPONENTES FÍSICOS DE UMA REDE

São interfaces de redes, adaptadores internos ou externos que permitem interconexão entre computadores, de maneira que a sua função é controlar as entradas e saídas de dados de uma rede. Os cabeamentos ou comunicação sem fio podem ser utilizados para levar informações para computadores por meio de protocolos (MENDES, 2007).

Abaixo tem-se os principais equipamentos de interconexão de redes: *Hubs*, *bridges* (pontes), comutadores (*switch*), *router* (roteadores) e *gateways*.

2.1.1 Hubs

Os *Hubs* são equipamentos que possuem diversas portas de entrada. Os pacotes de dados que chegam a uma dessas portas são emitidos para as demais portas em *broadcast*. Durante o procedimento de envio dos pacotes de dados, se dois pacotes chegarem juntos ocorrerá uma colisão entre eles. O *hub* em si forma um domínio de colisão, e todas as ligações trabalham na mesma velocidade (portas) (TANENBAUM, 2003).

2.1.2 Bridges (Pontes)

Os *bridges* são dispositivos utilizados para conexão de duas ou mais redes, onde vários computadores comunicam-se entre si e podem compartilhar informações (MORIMOTO, 2005).

De acordo com Carissimi, Rochol e Granville (2009, p.197):

> À medida que equipamentos vão sendo interligados em uma rede estruturada com Hubs, aumenta a probabilidade de ocorrência de colisão, o que consequentemente afeta o desempenho da rede. As pontes surgem como uma primeira solução para esse problema, definindo diferentes domínios de colisão em uma rede. O ato de dividir uma rede em vários domínios de colisão é denominado segmentação da rede. Uma ponte serve para interconectar duas ou mais redes físicas, mantendo a abstração de uma única rede composta pelos equipamentos dessas redes físicas. Entretanto, cada rede física possui um domínio de colisão próprio.

2.1.3 Comutadores (Switch)

Os comutadores possuem comportamento similar a uma ponte. Este dispositivo além de fazer conexão entre equipamentos possui diversas portas, permitindo que várias máquinas possam se conectar a cada porta do *Switch* ou qualquer outro dispositivo de conexão entre equipamentos, criando diversos domínios de colisão, o que beneficia o uso da rede. Logo, quaisquer destas portas possuem um exclusivo segmento conectado a um computador ou outros equipamentos criando novos segmentos de rede (CARISSIMI; ROCHOL; GRANVILLE, 2009).

2.1.4 Router (Roteadores)

Os roteadores são equipamentos muito importantes para o acesso à Internet, eles são responsáveis por todos os dados trafegados na rede. Esses equipamentos proporcionam a conectividade com várias redes diferentes, enviando informações para outros computadores em outras redes (MORIMOTO, 2011).

De acordo com Morimoto (2011, p. 1), um roteador wireless tem em regra três funções:

> Compartilhar a conexão com a web, que pode chegar através de um modem ADSL, cable modem ou mesmo de um modem 3G. Oferecer acesso wireless para notebooks, tablets, smartphones e outros dispositivos, bem

como PCs com adaptadores sem fio. Oferecer algumas portas ethernet para a conexão de PCs e outros dispositivos cabeados.

2.1.5 Gateways

Os *gateways* possuem a funcionalidade de converter protocolos, através deste dispositivo pode-se transmitir informações entre diferentes redes. Portanto, ao conectá-los em duas máquinas distintas ambas comunicam-se entre si (SOUSA, 1999).

2.2 TOPOLOGIAS DE REDES

As topologias de redes são parâmetros que descrevem o meio de conexão dos dispositivos na rede, isto é, como eles estão conectados (ZACKER; DOYLE, 2000).

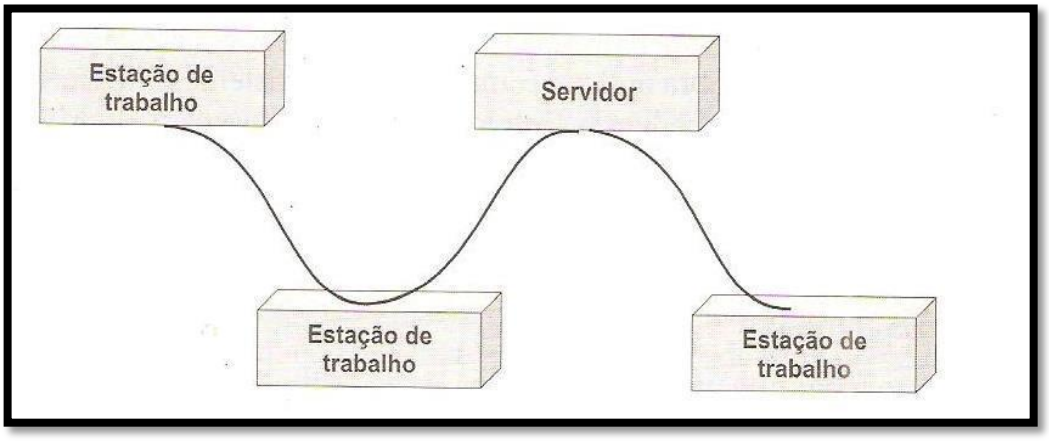
A seguir serão abordados os tipos mais comuns de topologias de redes.

2.2.1 Topologia em barramento

Topologia em barramento são conexões feitas por um só cabo coaxial onde os computadores são conectados. Esse tipo de topologia é utilizada em redes LAN, e consegue alcançar 10 Mbps. Com o avanço tecnológico as redes LAN expandiram, com isso, prevalece sua arquitetura de rede, assim chamada de Ethernet (AMARAL, 2012).

Essa topologia pode ser visualizada na figura 1:

Figura 1 - Topologia em barramento



Fonte: Zacker, Doyle (2000).

2.2.2 Topologia em anel

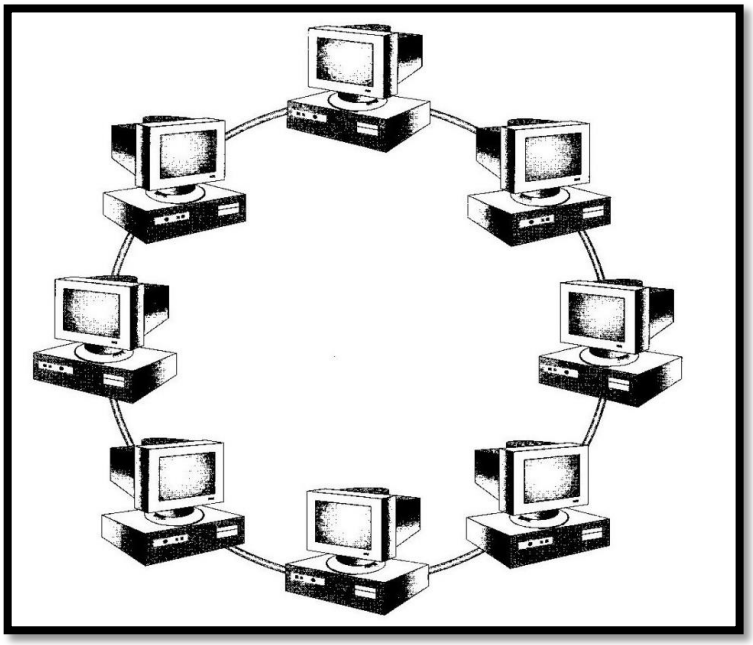
Topologia anel são conexões de cabos em forma de círculo, cada ponto se comunica com o ponto seguinte até chegar à direção informada (THOMAS, 1997).

Para Furgeri (sd, p. 5) a topologia em anel:

> Consiste de estações conectadas através de um caminho fechado, usando ligações ponto a ponto. Possui repetidores para aumentar a confiabilidade, podem receber e transmitir dados em qualquer direção, no entanto o mais comum é unidirecional.

Essa topologia pode ser visualizada na figura 2:

Figura 2 - Topologia em anel



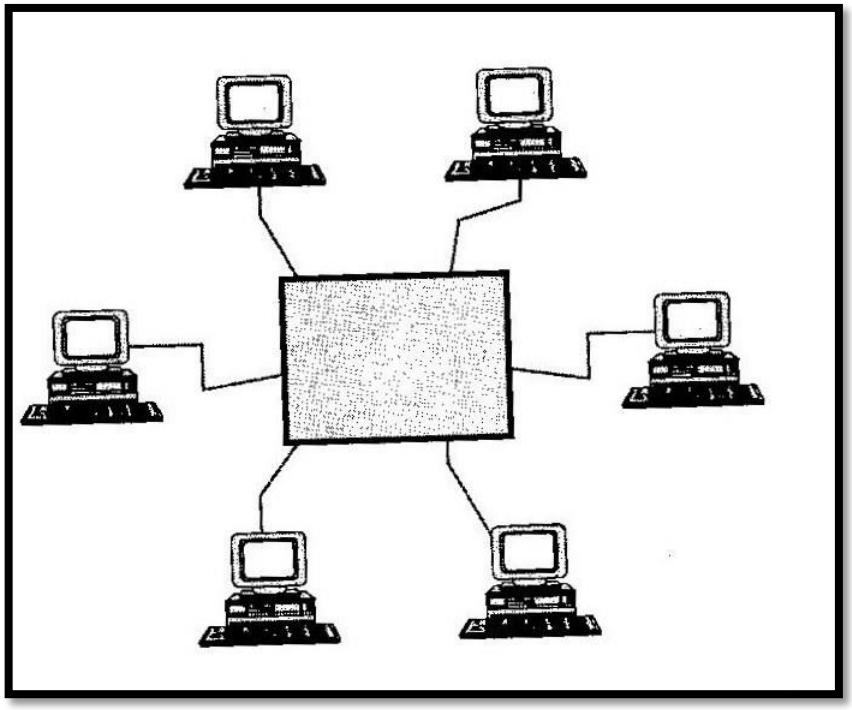
Fonte: Thomas (1997).

2.2.3 Topologia em estrela

Topologia em estrela ocorre pela conexão de computadores ligados por meio de cabos, sendo que todas as comunicações que circulam na rede são direcionadas ao nó central (SOARES; LEMOS; COLCHER, 1995).

Essa topologia pode ser visualizada na figura 3:

Figura 3 - Topologia em estrela



Fonte: Soares, Lemos e Colcher (1995).

3 REDES SEM FIO

Nos últimos anos a tecnologia de redes sem fio vem sendo cada vez mais utilizada, pois o acesso à Internet em casa se tornou mais rápido de fácil. Com todo esse crescimento, inúmeros estabelecimentos da área da tecnologia oferecem aos seus clientes diversos computadores com dispositivos Wi-Fi, e outros equipamentos como antenas e roteadores (PINZON, 2009).

Para Ferreira (2013), as redes sem fio são a passagem de dados entre dois ou mais mecanismos, através de ondas de rádio, portanto essa comunicação é feita sem o uso de cabos. Os sinais como os de televisão ou rádio FM, possuem os procedimentos do mesmo modo que as ondas de rádio são encaminhadas.

3.1 PADRÕES DE REDES SEM FIO

A diferença das redes sem fio para as redes cabeadas são os métodos de realização da troca de dados, nesse caso foi criado em 1990 pela IEEE um protocolo para este tipo de rede, assim em 1997 o protocolo foi aprovado e recebeu o nome de 802.11 (SANTOS; RIBEIRO, 2004).

A seguir serão abordados os tipos de padrões de redes sem fio mais utilizados.

3.1.1 Padrão IEEE 802.11b

“IEEE 802.11b é o padrão mais lento e barato. Transmite a 2,4 GHz e pode transmitir até 11 Mbps de dados” (CUTRIM, 2013, p. 9).

Ferreira (2013) mostra que: de maneira inicial o padrão IEEE 802.11b conseguem sustentar 32 usuários em cada rede Wi-Fi. Possui vantagens, como por exemplo, um preço acessível dos dispositivos, e a velocidade de conexão é gratuita. Por outro lado, possui alta interferência em transmissões e recepções de sinais, dificultando a rede e deixando-a mais lenta.

3.1.2 Padrão IEEE 802.11a

O padrão IEEE 802.11a, atinge uma velocidade de 54 Mbps, e faz uma transmissão com frequência de 5 GHz, nos padrões da IEEE os fabricantes que não possuem padrões é de 72 a 108 Mbps, a principio esse padrão sustenta 64 usuários por ponto de acesso e atinge área de pequena distância (FARIA, 2007).

De acordo com Cunha Neto (2011), o padrão IEEE 802.11a, surgiu depois do padrão IEEE 802.11b, com o objetivo de solucionar problemas existentes no padrão IEEE 802.11b.

3.1.3 Padrão IEEE 802.11g

Cunha Neto (2011) mostra que o padrão IEEE 802.11g consegue operar na mesma frequência do padrão IEEE 802.11b, enquanto opera com uma velocidade de 54Mbps, ou seja, ele permite que equipamentos que sigam os dois padrões sejam interoperáveis, assim como utiliza a mesma velocidade do padrão IEEE 802.11a.

Conclui-se então que este padrão utiliza os aspectos positivos dos padrões IEEE 802.11a e IEEE 802.11b.

3.1.4 Padrão IEEE 802.11n

O padrão 802.11n abrange uma área de 70 metros e possui uma velocidade de transmissão de dados na rede de até 300 Mbps. Atua nas frequências 2,4GHz e 5GHz. Esse tipo de padrão utiliza diversas antenas para transmissão de dados de dados de uma área a outra, o qual possui uma nova tecnologia chamada *Multiple Input, Multiple Output* (MIMO). Sendo que possui uma ampla velocidade de transmissão e a distância que pode alcançar (FERREIRA, 2013).

O tema a seguir explica sobre os três protocolos de segurança de redes sem fio mais utilizados.

3.2 CRIPTOGRAFIAS PARA SEGURANÇA

Na conexão com a rede sem fio é necessário à utilização de algum protocolo para que ocorra a segurança da mesma. Onde se tem os principais protocolos de segurança: Protocolos Wired Equivalente Privacy (WEP), Protocolos Wi-Fi Protected Access (WPA) e Protocolos Wi-Fi Protected Acess 2 (WPA2).

3.2.1 Protocolos Wired Equivalente Privacy (WEP)

O protocolo WEP surgiu da preocupação que se tinha em dar garantia à segurança nas redes sem fio. Esse protocolo tem aparência de ser seguro para usuários que não se preocupam com a proteção de sua rede (BOF, 2010).

Conforme Cutrim (2013), a segurança do protocolo WEP é formada por uma chave estática e um componente dinâmico. A chave estática é utilizada para o acesso a todos os componentes da rede, enquanto os componentes dinâmicos, juntamente com a chave estática, formam uma chave utilizada na cifragem do tráfego.

Este protocolo torna-se inseguro em alguns casos quando a chave estática é distribuída. Então se houver necessidade de trocar a chave, o seu procedimento poderá ser mais complexo ou até mesmo não poder ser concluído. Geralmente, isso ocorre em ambientes públicos. Posteriormente, com a conexão estabelecida, a chave estatística será subordinada a cálculos matemáticos para produzir quatro novas chaves, tendo a função de criptografar dados percorridos pela rede. Sua troca será feita apenas se a chave estática original for modificada (FARIA, 2007).

3.2.2 Protocolos Wi-Fi Protected Access (WPA)

O WPA é um protocolo aperfeiçoado do WEP para proteger as redes sem fio tornando-as cada vez mais seguras (BOF, 2010).

Surgiu como alternativa ao WEP, proporcionando mais segurança de acesso. Cada usuário utiliza uma senha única para ativar o WPA e essa senha é alterada constantemente, ao contrário do WEP que utiliza uma única senha estática (DUARTE, 2010).

Além de este protocolo fornecer segurança a redes sem fio, ele também analisa pacotes no qual reconhece a ocorrência de devidas mudanças e ataques nas redes (DEMARTINI, 2013).

3.2.3 Protocolos Wi-Fi Protected Access 2 (WPA2)

De acordo com Duarte (2010), o protocolo WPA resolveu diversos erros do WEP, mas ainda possuía insegurança no desempenho desse protocolo. Então para resolver essas vulnerabilidades ainda existentes no WPA, surgiu o protocolo WPA2 com o compromisso de solucionar segurança as redes sem fio.

O protocolo WPA2 possui um método de funcionamento com senhas e algoritmos, com isso ele consegue restringir as possibilidades de ataques. Deste modo o WPA2 vem sendo atualmente o mais seguro, este protocolo é mais utilizado para que não ocorra eventual invasão (DEMARTINI, 2013).

Conforme Guimarães (2009), o protocolo WPA2 está sendo o mais utilizado por realizar uma criptografia mais elaborada que o WPA, sendo que o padrão 802.11i trabalha a parte de autenticação que não ocorre diferença entre os protocolos, mas sendo o que diferencia o WPA2 dos outros protocolos são as autenticações que ainda não conseguiram decifrar os códigos para a descoberta das senhas da rede.

De acordo com Ferreira (2013), também o que diferencia os protocolos WPA e WPA2, é que o WPA usa chave de criptografia *Temporal Key Integrity Protocol* (TKIP) na web. Já o WPA2 usa a chave de criptografia *Advanced Encryption Standard* (AES), sendo esta chave considerada a mais segura.

Ferreira (2013, p. 22) mostra que:

> **WPA-PSK** (Pre Shared Key) de maneira simples WPA-PSK é uma criptografia forte em que as chaves de criptografia (TKIP) e frequentemente mudada o que garante mais segurança protegendo de ataques hackers, muito utilizado por usuários domésticos. **WPA2-PSK** e ainda mais seguro que o WPA-PSK onde sua criptografia (AES) e extremamente forte e resistência a ataques, adotado como padrão de criptografia do governo americano.

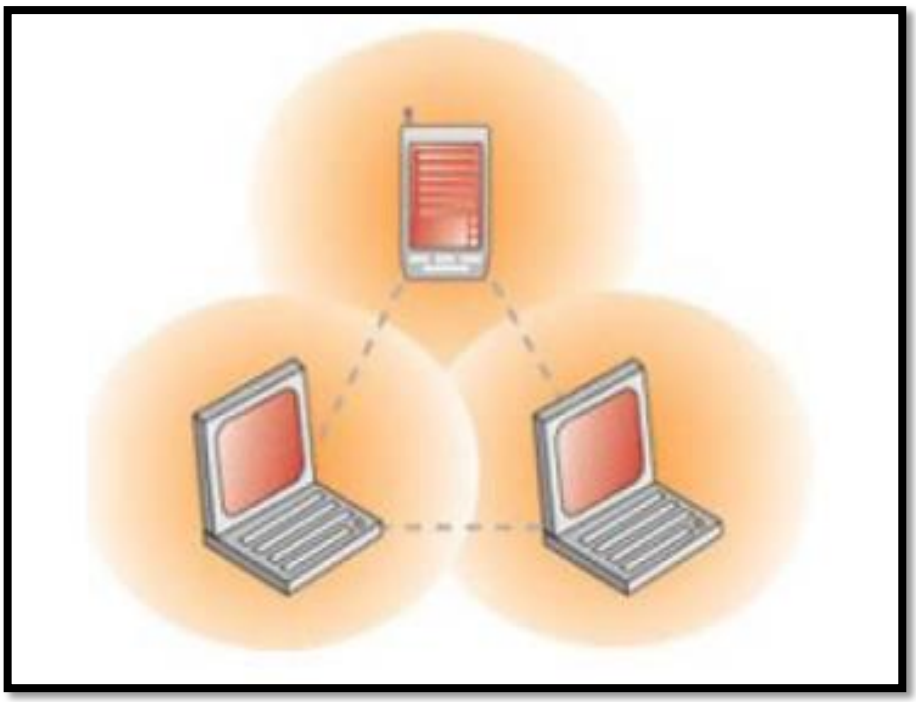
O tema a seguir explica sobre as topologias sem fio Wireless mais utilizadas.

3.3 TOPOLOGIA SEM FIO (WIRELESS)

A topologia sem fio Wireless é para o uso de redes empresarias e redes domésticas. Esse tipo de rede é utilizada quando dois ou mais dispositivos emissores e receptores Wireless estão próximos, os mesmos emitem sinais de um para o outro, assim reconhecem a presença de outro dispositivo para comunicarem entre si (PINHEIRO, sd).

Essa topologia pode ser visualizada na figura 4:

Figura 4 - Topologia sem fio Wireless



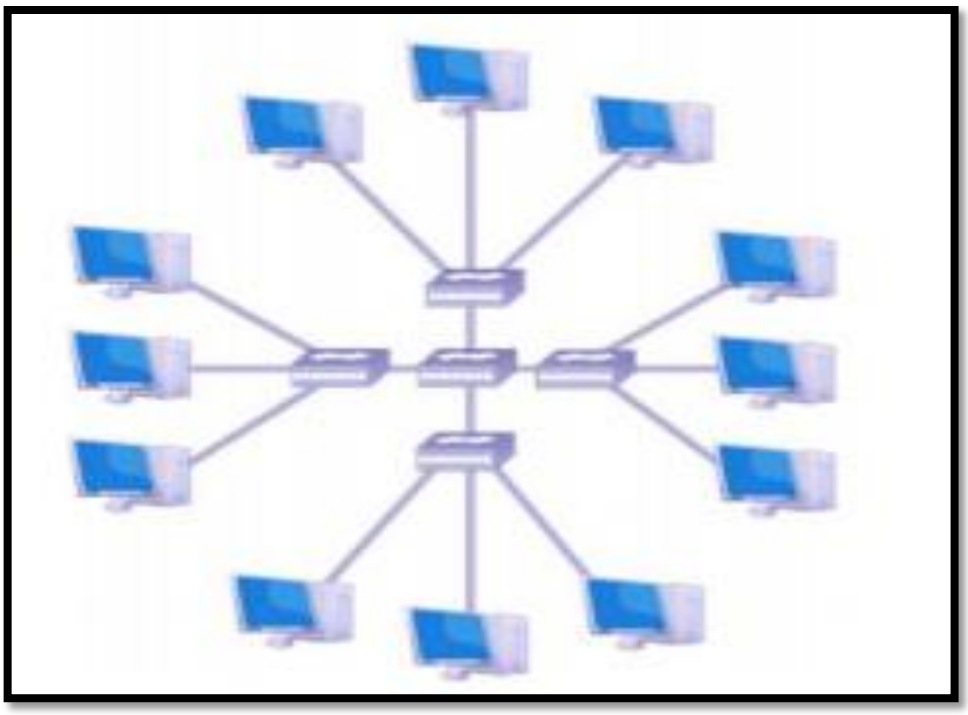
Fonte: Pinheiro (sd).

3.3.1 Topologia estrela - estendida

A topologia de estrela estendida une redes de estrelas individuas em outra estrela, utilizando os equipamentos como: switches, hubs e concentradores. Isso estenderá o tamanho e comprimento da rede. A diferença com a topologia de estrela é que esta entende os domínios de colisão e broadcast. Se uma rede pequena precisar ser conectada, a mesma possui uma vantagem de que a sua manutenção é simples de utilizar. As suas desvantagens são que o domínio de colisão e de broadcast podem sobrecarregar e atrasar o desempenho da rede, podendo até não ocorrer comunicação entre as mesmas (SILVA, 2014).

Essa topologia pode ser visualizada na figura 5:

Figura 5 - Topologia estrela - estendida



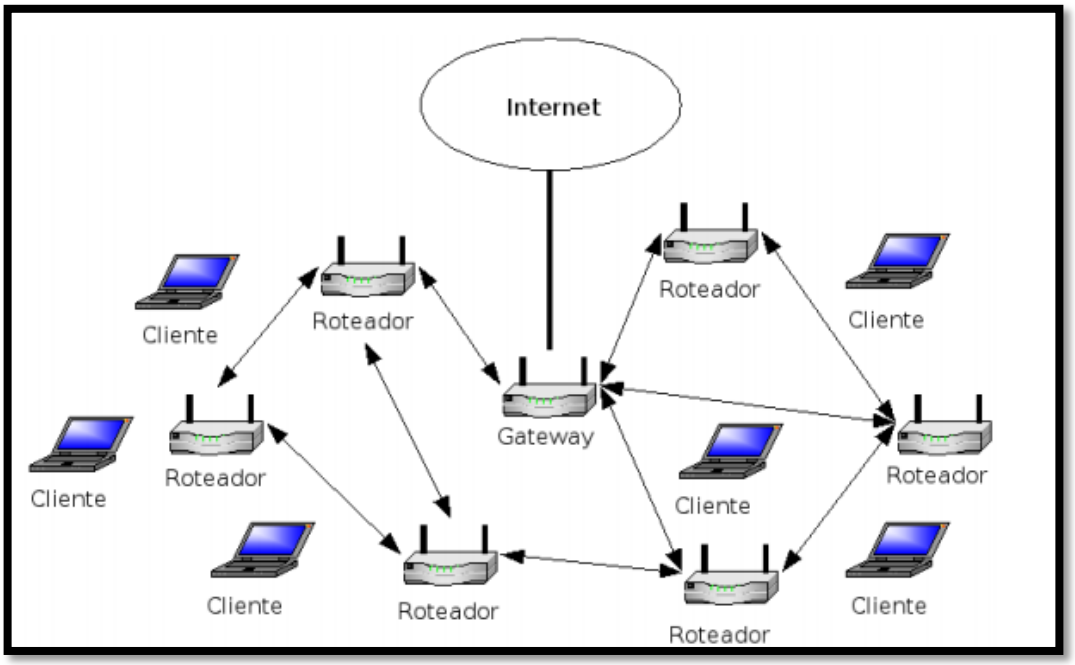
Fonte: Silva (2014).

3.3.2 Topologia malha (mesh)

A topologia em malha facilita a conexão com mais rapidez ao local destinado, também possuem diversas conexões que chegam ao mesmo lugar, logo será utilizando o melhor caminho por meio dos protocolos de roteamento para alcança-lo, dificilmente poderá ocorrer falha de conectividade se a rede é bem protegida. Também para ocorrer à comunicação as redes em malhas, as mesmas precisam apenas dos pontos de acesso (APs) para encontrar o local destinado ou gateway de Internet para utilizar o melhor caminho (MEGGER, 2011).

Essa topologia pode ser visualizada na figura 6:

Figura 6 - Topologia malha (mesh)



Fonte: Megger (2011).

3.4 REDES SEM FIO DOMÉSTICAS

A grande maioria da população está utilizando redes sem fio domésticas, devido à facilidade que se tem ao acesso da Internet. Para isso, basta possuir um roteador de redes sem fio que faça conexão com diversos computadores, sendo que cada um deles pode trocar informações entre si (TANENBAUM, 2003).

3.4.1 Funcionalidades de equipamentos de redes sem fio domésticas

Existem vários equipamentos de redes sem fio que são de extrema importância para transmitir sinal. A seguir serão mostrados os tipos e funcionalidades dos mesmos.

3.4.2 Placas de redes sem fio

As placas de redes são dispositivos que permitem a comunicação de diversos computadores de uma rede. Elas servem para emitir e receber informações da rede, assim para cada tipo de rede é preciso um modelo compatível de placa.

Caso contrário, não sendo compatível, não será possível possuir comunicação com as outras redes (MORIMOTO, 2002).

A figura 7, apresentada demostra um exemplo de placa de rede.

Figura 7 - Placa de rede

Fonte: Duarte (2010).

3.4.3 Access Point (AP)

O Access Point ou ponto de acesso, nada mais é do que um roteador para acessar as redes sem fio, sendo assim ele é quem faz o gerenciamento da comunicação entre os usuários (PINZON, 2009).

A figura 8, apresentada demostra um exemplo de roteador.

Figura 8 - Access Point (AP)

Fonte: Pinzon (2009).

3.4.4 Antenas

As antenas transmitem sinais para todos os lados, são conectadas ao ponto de acesso que permitem conexões à longa distância. Para o uso doméstico são utilizadas as antenas direcionais (ONO, 2004).

Conforme Duarte (2010), as antenas direcionais possuem irradiações e são destinadas a um local exclusivo, neste caso essas antenas emitem raios fortes enviados para uma ampla área. Sendo assim, as antenas direcionais são aquelas que enviam e recebem sinais com uma velocidade de transmissão de dados determinada pela estrutura da antena.

Reis (2012, p. 25) explica sobre antenas direcionais:

> Este tipo de antena também capta sinais em apenas uma direção, de uma forma mais concentrada, permitindo que seja atingida distâncias ainda maiores que outras antenas. Muitas antenas utilizam uma grade o que reduz o custo e evita que a antena seja deslocada do seu lugar original pelo vento. Esta antena trabalha na frequência 2.4 Ghz, com potência de 25dBi, ângulo vertical de 9º e horizontal de 8,5º.

3.5 TIPOS DE REDES SEM FIO DOMÉSTICAS

Os tipos de redes sem fio domésticas são classificados em Local Area Network (LAN) e Wide Area Network (WAN) (NÉRIO; RODRIGUES, 2003).

Abaixo tem-se os tipos mais comuns de tecnologias de acesso sem fio.

3.5.1 Banda larga móvel

Banda larga móvel ou redes WAN, transmitem informações de longa distância, fornecem acesso de alta velocidade à Internet (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Onde os dois tipos mais oferecidos ultimamente de conexão de Internet são: 3G e 4G, sendo assim chamada de tecnologia 3G por ser a terceira geração, consegue até 1 Megabit por segundo (Mbps), o segundo tipo assim chamado de tecnologia 4G abrange com velocidade de 5 Megabits por segundo (Mbps) (TAGIAROLI, 2014).

A conexão de Internet 3G aperfeiçoa a comunicação de dados e voz, sendo que essa tecnologia proporciona grande velocidade de conectividade como,

por exemplo, a comunicação de sinal de televisão e vídeo chamadas, entre outras utilidades (HAMMERSCHMIDT, 2008).

Já o 4G tem preferência em trafegar informações, uma vez que a rede tem mais velocidade e segurança, esta conexão atua mediante a tecnologia *Long Term Evolution* (LTE) que permite prioridade de transmissão de dados da Internet e também a probabilidade de tráfego de voz (GRASEL, 2014).

De acordo com Tagiaroli (2014), essas duas tecnologias podem ser utilizadas em qualquer local que possua um limite de acesso e cobertura, ressalta-se depois de fazer o uso de uma quantidade de informações dessa tecnologia ela diminui a velocidade.

3.5.2 Bluetooth

O Bluetooth é uma inovação tecnológica que admite a conexão ágil sem a utilização de cabos que facilita o manuseio dos dispositivos, pois é necessário somente que os mesmos fiquem próximos uns dos outros, para ocorrer a troca de informações entre os equipamentos móveis. As informações do Bluetooth são conduzidas através de radiofrequência, sendo que cada dispositivo identifica sua colocação (ALECRIM, 2013).

3.5.3 Infravermelho

O infravermelho é uma tecnologia utilizada para a troca de informações de pequena distância. Portanto, seu funcionamento é de alta frequência e suas comunicações entre os dados são realizadas sem que ocorra qualquer impedimento entre envio e recebimento de informações. O infravermelho possui uma taxa de transmissão que submete as mudanças entre 9.600 bits por segundo (bps) até um máximo de 4 megabits por segundo (Mbps), porém à extensão é de pequena distância (ALVES, 2009).

Nério e Rodrigues (2003, p. 4) explicam as principais transmissões de informações por infravermelho:

> Ondas infravermelhas não atravessam objetos sólidos. Assumem comportamento parecido com o da luz, quando se desloca do rádio de onda longa e vai em direção à luz visível, perdendo as características de rádio.

> Um sistema infravermelho num ambiente fechado, não interfere em outro, instalado em numa sala ao lado, por esse motivo não precisa de autorização do governo para operar. Em ambientes abertos a comunicação infravermelha é inviável devido o sol enviar radiação infravermelha.

3.5.4 Wi-Fi

A Wi-Fi refere-se a conexões de redes sem fio, que utilizam o padrão IEEE 802.11, o mesmo estabelece conexão entre dois ou mais dispositivos sem fio (CARAÇA; PENNA, 2009).

Com a avanço tecnológico as redes Wi-Fi vendo sendo mais utilizadas pelos usuários, devido a sua praticidade de instalação e a facilidade de acesso em vários ambientes diferentes. Por conta disso existem diversos riscos a serem analisados, como por exemplo: por sua transmissão ser via ondas de rádio, não precisa necessariamente acessar uma rede fisicamente, como acontece com as redes cabeadas. Portanto os dados que são enviados por os usuários autênticos podem ser interceptados por usuários próximos com o mínimo de equipamentos. As redes Wi-Fi são fáceis de serem instaladas o que leva a maioria das pessoas instalarem por si próprias, sem se preocupar com o mínimo de proteção. Em ambientes públicos os dados que não possuem criptografia estão sujeitos a roubos por intrusos, devido aos dados estarem sendo transmitidos em texto limpo. Existem ainda algumas redes Wi-Fi abertas que de propósito são falsas, utilizadas como estratégias de intrusos, para ter acesso aos dados dos usuários que acessam a mesma (CERT, 2012).

4 SEGURANÇA DE REDES SEM FIO

Com o avanço da tecnológica computacional e por decorrência do crescimento da utilização da rede sem fio, observa-se que alguns cuidados com a segurança da rede precisam se tomados. Isso porque a maioria da população tem o costume de instalar uma rede sem fio em casa sem tomar os devidos cuidados com a segurança sem saber os riscos que está correndo, e abrindo caminhos a possíveis invasões, como por exemplo, roubos de dados (TORRES, 2009).

Deste modo, para dar mais eficiência às redes sem fio é necessário à aplicação de políticas de segurança capazes de barrar possíveis invasores (SOARES; LEMOS; COLCHER, 1995).

4.1 POLÍTICA DE SEGURANÇA

As políticas de segurança consistem em normas que determinam se os dados de uma rede possuem segurança ou não. Neste entendimento, referem-se a um sistema de segurança estruturado para a proteção de dados obtidos na rede (SOARES; LEMOS; COLCHER, 1995).

De acordo com Ormond (2006), as políticas de segurança não são necessariamente apenas para guardar informações ou modificações, por isso requerem um excelente conhecimento de segurança.

Soares, Lemos e Colcher (1995), explicam que um conjunto de normas consiste em uma política de segurança que pode possuir dois tipos:

a) **política de segurança baseada em regras:** confia em dados sobre sensibilidade. Entretanto, para possuir a segurança de um sistema, é sugerido que seu nível de sensibilidade seja marcado com rótulos[1] de segurança. Os procedimentos que atuam sob o controle de usuários possuem os rótulos de segurança adequados, que indicam se possui controle no nível de autorização do usuário. As normas usam os rótulos e procedimentos que originam o modo de acessibilidade que devem ser realizados. Os mecanismos que programam os canais de comunicação

[1] São utilizados pelas ocorrências de vulnerabilidades em redes de computadores, assim utilizadas nas politicas de segurança que são normas para segurança, podem ser utilizadas em diversos dispositivos. (BRASIL ESCOLA, 2009).

em redes de computadores possuem rótulos de segurança. Então, as normas que determinam a política de segurança e que definem quando as informações podem se comunicar por canais, ou seja, só podem se comunicar quando o nível de segurança estiver apropriado (SOARES; LEMOS; COLCHER, 1995);

b) **Políticas de segurança baseadas em identidade:** são os controles de acesso mais comuns nos computadores. Essa determinada segurança, baseia-se em controlar o acesso que permita apontar o que cada usuário possa fazer, ou seja, interpretar, alterar ou utilizar (SOARES; LEMOS; COLCHER, 1995).

4.2 PILARES DA SEGURANÇA

É constituído por três pilares, sendo que o primeiro pilar é a Confidencialidade, que é uma forma de cuidar dos dados para que usuários que não possuam permissão aos dados os utilizem; o segundo pilar é a Integridade dos dados que consiste em uma forma de cuidar dos dados para que não ocorra nenhuma alteração sem autorização do usuário autêntico e, por fim, o terceiro pilar é a Disponibilidade que garante que os dados sempre estejam disponíveis a usuários autênticos (FERREIRA, 2009).

4.3 ENDEREÇOS MAC

Os endereços MAC são endereços físicos, exclusivos compostos por 12 números hexadecimais, fazendo com que eles sejam reconhecidos na rede. Assim, com filtragem destes endereços é possível que apenas as máquinas com os endereços de MAC cadastrados tenham acesso à rede (BOF, 2010).

De acordo com Faria (2007, p. 22) que relata:

> Para melhorar ainda mais a segurança utilizando o endereço MAC é necessário substituir a entrega de endereços IP via DHCP por IP fixos, que trabalhando em conjunto dificultaria um possível ataque. Alguns programas também permitem associar o endereço MAC do cliente com o endereço MAC do concentrador, permitindo assim a autenticação em um concentrador correto e não por engano, com um concentrador errado de maior potência ou de um atacante, dificultando um possível ataque.

4.4 MÉTODOS DE ATAQUES CONTRA REDES SEM FIO

Conforme Verissimo (2002) existem quatros tipos de ataques, sendo que os intrusos possuem maneiras diferentes para encaminhar mensagens. Os tipos são:

a) **Interrupção:** os intrusos conseguem parar as movimentações de informações do ponto de origem, no qual impedem que as informações cheguem às direções desejadas;

b) **Interceptação:** “as informações são interceptadas durante a transmissão, comprometendo a confidencialidade da mensagem.” (LIMA, 2005, p. 6).

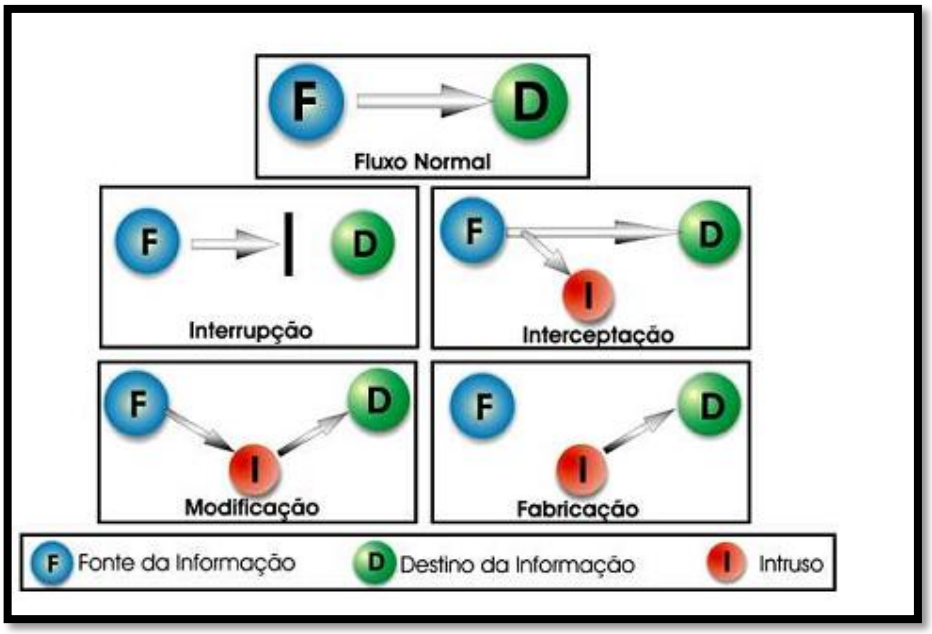
Os outros dois tipos de acordo com Schweitzer et al. (2005) são:

c) **Modificação:** esse ataque consta como o mais moderno, pois o intruso não possui só acesso às informações, portanto ele consegue alterar os dados assim prejudicando as informações existentes;

d) **Fabricação:** esse tipo de ataque acontece quando o intruso produz informações como se fossem de pontos autorizados, esse tipo de falha ocorre quando há mudanças no sistema e usuários.

A figura 9, apresentada demostra a Taxonomia baseada em ações:

Figura 9 - Taxonomia



Fonte: Lima (2005)

4.5 VULNERABILIDADES

As vulnerabilidades são falhas que ocorrem no sistema quando um programa é mal projetado, deixando-o suscetível às invasões. Caso isso ocorra, tanto os usuários que possuem permissão total do sistema, quanto os que não possuem podem executar alterações, colocando em risco os dados lá armazenados (QUEIROZ, 2007).

Com o avanço tecnológico, por mais que haja proteção em um sistema, necessariamente ele não estará livre de invasões, isso ocorre pelo surgimento de novas vulnerabilidades. Torna-se difícil para usuários que acham que investindo na implantação do sistema de segurança resolverá todos os problemas existentes (BOF, 2010).

Para contornar esse problema é necessária a aplicação de contramedidas de segurança.

4.6 CONTRAMEDIDAS DE SEGURANÇA

As contramedidas examinam as inseguranças de um sistema suscetível a ocorrer invasões, objetivando prevenir que algo malicioso venha a ocorrer (RODRIGUES, 2007).

Acerca desse tema, existem as ameaças que podem atingir a rede, neste caso serão abordadas algumas contramedidas de segurança para as ameaças mais comuns (TECNET, 2004).

4.6.1 Falsificando o IP/ sequestro de sessão

Conforme Thomas (2007), a falsificação de um IP é quando o intruso cria um pacote com endereço de IP falso para se infiltrar na rede. Com isso, o intruso terá acesso a todas as máquinas conectadas à rede. Então, para execução desse ataque, o intruso tem que descobrir a faixa de endereços de IP que essas máquinas conectadas a rede confiam, após isso ele poderá perpetrar o ataque desejado.

De acordo com a Microsoft (2004) as contramedidas:

> Utilize autenticação forte.
> Não armazene segredos (por exemplo, senhas) em texto puro.
> Não transmita credenciais em texto puro por linha.
> Proteja os cookies de autenticação com Secure Sockets Layer (SSL).

4.6.2 Ataques de negação de serviço (dos – denial of service)

O ataque de negação de serviço (DoS), são tentativas de usuários mal-intencionados para investigar as características dos protocolos de Internet e descobrir falhas, com o propósito de impedir que os usuários legítimos acessem os serviços de rede (GOMES,2000).

Segundo Laufer et al. (sd) algumas medidas adequadas para impedir ou diminuir riscos ocasionados por ataques de negação de serviço são:

a. **Medidas preventivas:** são feitas manutenções em todos os programas. Esses processos são utilizados para minimizar ataques à rede. Neste caso, a filtragem de pacotes é utilizada para impedir pacotes com endereço de IP não legítimos, que transitam na rede;

b. **Medidas reativas:** se a invasão não pode ser impedida, deve-se buscar dados sobre a originalidade do acesso. Portanto com o rastreamento de pacotes, se constata todo o caminho percorrido pelos mesmos tentando identificar a origem.

Para ataques distribuídos (DoS), a identificação da origem torna-se quase impossível devido ao ataque ser proveniente de diversas fontes simultaneamente, o que leva a uma grande dificuldade de se defender. Neste caso a prevenção é a melhor estratégia.

4.6.3 Varredura (scanning)

Para que se tenha um ataque à rede os intrusos precisam de informações da mesma e a conexão entre outros serviços que são utilizados. O intruso costuma coletar todos os dados possíveis, realizando assim uma varredura dos pontos de acesso das redes sem fio (KUROSE; ROSS, 2006).

Conforme Lima (2005), a contramedida utilizada para os ataques de varredura é a detecção de intrusão, pois: possuem diversos dispositivos para

proteção de dados, sendo alguns deles, tais como: o backup dos dados, filtros entre outros.

Ainda segundo Lima (2005, p. 10):

> Os IDS (*Intrusion Detection System*) são ferramentas complementares no processo de gestão de segurança da informação, pois apesar dos esforços empregados para automatizar a tarefa de detecção e respectivas respostas, é imprescindível a interação humana na análise dos filtros, alertas e relatórios gerados, objetivando medidas apropriadas dadas as circunstâncias envolvidas.

4.6.4 Sniffers (farejadores)

Os sniffers são ferramentas utilizadas para capturar pacotes de dados que vão ser enviados até máquinas conectadas a rede onde o sniffer está instalado. É utilizado o sniffer mais avançado de rede para poder decodificar informações em todo sistema, assim o intruso pode ter acesso a todos os dados da rede (GOMES, 2000).

De acordo com a Microsoft (2004):

> Contramedidas para ajudar a evitar sniffing incluem:
> Use forte segurança física e segmentação adequada da rede. Este é o primeiro passo para evitar que o tráfego seja coletado localmente. Faça a encriptação total das comunicações, incluindo a autenticação de credenciais. Isto evita que os pacotes de sniffing possam ser usados por um invasor.

4.6.5 Força Bruta (Brute Force)

Os ataques de força bruta são tentativas de quebra de senhas, realizadas por intrusos, para ter acesso ao sistema, como se fosse o próprio usuário da rede. Independente da máquina, componente de rede ou aparelho conectado a Internet, possuindo usuário e senha, sofrem riscos de ataques de força bruta. Até mesmo aparelhos com proteção de senha, estão sujeitos a ataques, se o intruso possuir o acesso físico na rede (CERT, 2012).

De acordo com a Microsoft (2004): Para ocorrer esse ataque de força bruta, depende muito da estrutura computacional, e procedimentos adotados. A contramedida para evitar ataques de força bruta é utilização de senhas complexas na rede, como por exemplo: senhas grandes, com letras maiúsculas e minúsculas seguidas de números, para dificultar a descoberta da mesma.

5 TRABALHOS CORRELATOS

O trabalho de diagnóstico de segurança em redes sem fio domésticas aqui proposto é a compreensão dos métodos de segurança e como utilizá-los. Deste modo, os trabalhos correlatos são estudos relacionados com o projeto de pesquisa, que seguem:

5.1 VULNERABILIDADE E SEGURANÇA EM REDES SEM FIO

O trabalho de conclusão de curso foi elaborado pelo acadêmico Alexandre Pinzon, no curso de Bacharel em Sistemas de Informação, na instituição do Centro Universitário Ritter Dos Reis, no ano de 2009.

Este trabalho explica de modo geral os pontos fracos referentes à segurança, e se um intruso obtiver informações de uma rede sem fio, ela estará sujeita a vários danos. Portanto, foram efetuados testes que identificam se a rede é mal configurada, sendo assim usadas ferramentas mais comuns para hackers, então é essencial tomar cuidados com a segurança para não ocorrer ataques avançados (PINZON, 2009).

5.2 SEGURANÇA EM REDE SEM FIO

O trabalho de conclusão de curso foi elaborado pelo acadêmico Felipe Zanatta Pereira, no curso de Sistemas de Informação (bacharelado), na Universidade Planalto Catarinense Departamento de Ciências Exatas e Tecnológicas, no ano de 2007.

Neste trabalho foram realizados estudos sobre ataques, vulnerabilidades e formas de prevenção, sejam no uso corporativo ou no uso doméstico. Com os conhecimentos adquiridos foram identificados esses pontos fracos na rede, através de ferramentas específicas ou não (PEREIRA, 2007).

5.3 EVOLUÇÃO DA SEGURANÇA EM REDES SEM FIO

O trabalho de conclusão de curso foi elaborado pelo acadêmico Marcos Antônio Costa Corrêa Júnior, no curso de Ciência da Computação, Universidade Federal de Pernambuco Centro de Informática, no ano de 2008.

Este trabalho mostra o padrão IEEE 802.11, o qual autoriza a interoperabilidade dos mecanismos e muitos fabricantes, sendo determinado um protocolo de segurança, o WEP. Neste passo, foi mencionado a questão que envolve o protocolo ser inseguro para redes sem fio. Com base nos estudos feitos do padrão IEEE 802.11i, foram aprimorados para o desenvolvimento do protocolo WPA, este foi idealizado com velocidade e ainda estudado para buscar novas formas de melhoramento a esse protocolo. Assim, na finalização do IEEE foi lançado o protocolo WPA2, este é o protocolo mais utilizado por ser muito seguro.

Portanto, a evolução da segurança das redes sem fio baseia-se em estudar as evoluções da segurança *WLAN*, neste caso, sendo assim constatadas umas de suas inseguranças, provavelmente com o tempo foram surgindo melhorias (CORRÊA JÚNIOR, 2008).

5.4 UMA ABORDAGEM SEGURANÇA EM REDES WIRELESS

O trabalho de conclusão de curso foi elaborado pelo acadêmico Rogério Pereira Diana Filho, no curso de Bacharelado em Ciência da Computação, na Universidade Presidente Antônio Carlos, no ano de 2003.

Este trabalho demostra as funcionalidades de redes wireless e seus métodos de segurança, onde as redes wireless devem ser tratadas com cuidado, desde a instalação do *Access Point (AP)* na rede para obter-se a segurança, além das políticas de segurança, protocolos de redes wireless.

Para que haja mais segurança as redes sem fio, conforme acima mencionado, é necessária a aplicação de uma política de segurança: quais equipamentos são aceitos, se é essencial utilizar o protocolo de segurança dentro de uma rede, enfim todos os métodos ligados à segurança, embora nesses métodos ainda existam falhas (DIANA FILHO, 2003).

5.5 A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA

O trabalho de conclusão de curso foi elaborado pelo acadêmico Carlos Anderson Andrade Duarte, no curso de Pós-graduação em Redes de Computadores, na Escola Superior Aberta do Brasil – ESAB, no ano 2010.

Este trabalho relata sobre a família de protocolos 802.11x, assim sendo alguns métodos de segurança, e protocolos de redes sem fio. O WEP, com o nível dos estudos realizados, indica as falhas e pontos fracos nesse protocolo e o WPA, sendo assim criado para corrigir falhas e pontos fracos existentes no WEP. E o protocolo WPA2 como foi estudado neste trabalho é de grande utilidade para proteger as redes sem fio, pois ainda não conseguiu quebrar sua criptografia (DUARTE, 2010).

5.6 ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES

O trabalho de conclusão de curso foi elaborado pelo acadêmico Lucas Da Silva Carlessi, no curso de bacharelado de Ciência da Computação, na Universidade do Extremo Sul Catarinense – UNESC, no ano 2011.

Este trabalho demostra vários métodos de segurança de redes sem fio, sendo que as mesmas ficam expostas devido seu meio de transmissão de informação ser por ondas de rádio. Para isso foi utilizado às ferramentas chamadas Kismet e Beholder para proteger e diminuir ataques às redes, e suas funcionalidades são monitorar e detectar ataques (CARLESSI, 2011).

6 SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

Neste trabalho de projeto de pesquisa, foram elaborados os estudos sobre segurança em redes sem fio domésticas. Foi aplicado um questionário com 172 usuários, alunos do curso de Ciência da Computação, regularmente matriculados no segundo semestre do ano de 2015, sobre a utilização de segurança de redes sem fio. Também foi realizado um experimento para verificar o melhoramento na segurança de redes sem fio domésticas por meio de um cenário de configuração básico.

6.1 METODOLOGIA

Para a realização deste trabalho as etapas metodológicas seguidas foram pesquisa bibliográfica, estudo sobre a segurança em redes sem fio domésticas e políticas de segurança. Na elaboração da pesquisa bibliográfica foi essencial ter um entendimento sobre o conteúdo abordado no projeto de pesquisa.

Segundo Gil (2002, p. 44) pesquisa bibliográfica:

> A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Boa parte dos estudos exploratórios pode ser definida como pesquisas bibliográficas. As pesquisas sobre ideologias, bem como aquelas que se propõem à análise das diversas posições acerca de um problema, também costumam ser desenvolvidas quase exclusivamente mediante fontes bibliográficas.

Após a construção do referencial teórico, foi realizada uma pesquisa com usuários de redes sem fio domésticas, por meio de um questionário apresentado no (apêndice A), caracterizando essa pesquisa como de abordagem predominantemente quantitativa. De acordo com Michel (2005, p. 33) a pesquisa quantitativa:

> [...] se realiza na busca de resultados precisos, exatos, comprovados através de medidas de variáveis preestabelecidas, na qual se procura verificar e explicar sua influência sobre outras variáveis, através da análise da frequência de incidências e correlações estatísticas.

Os dados coletados foram analisados por meio do software IBM *Statistical Package for the Social Sciencies* (SPSS) versão 21.0. As variáveis qualitativas foram expressas por meio de frequências e porcentagens. A idade foi expressa por meio de média e desvio padrão. As análises inferenciais foram realizadas com um nível de significância α = 0,05 e confiança de 95%. A distribuição da idade quanto à normalidade foi avaliada por meio da aplicação do teste de Shapiro-Wilk. A comparação das médias de idade entre as fases estudadas foi realizada por meio da aplicação do teste H de Kruskal-Wallis seguido *post hoc* teste de Dunn. A investigação da existência de associação entre as variáveis qualitativas foi avaliada por meio da aplicação do teste qui-quadrado de Peason (FIELD, 2009).

6.1.1 Caracterização do ambiente da pesquisa

Esta pesquisa foi realizada com usuários que possuem redes sem fio domésticas. Para a presente pesquisa foram entrevistados os acadêmicos do curso de Ciência da Computação da Universidade de Extremo Sul Catarinense – UNESC - Município de Criciúma/SC, regularmente matriculados no segundo semestre do ano de 2015.

Foi entregue um questionário para todos os entrevistados selecionados da 1ª à 9ª fase do curso de Ciência da Computação, a pesquisa foi realizada em sala de aula, onde o pesquisador aplicou o instrumento.

6.1.2 População e amostra

Foram considerados 307 acadêmicos matriculados no curso de Ciência da Computação. A partir dessa informação foi realizado o cálculo do tamanho mínimo da amostra, por meio da fórmula proposta por Barbetta, Reis e Bornia (2010, p. 193):

$$n_o = \frac{z_\gamma^2 p(1-p)}{E_o^2}$$

$$n_o = \frac{1{,}96^2 \times 0{,}5(1-0{,}1)}{0{,}05^2}$$

$$n_o = 385 \text{ acadêmicos}$$

Em que, “γ” refere-se ao nível de significância adotado, nesse caso, 0,05, “z” é a estatística padrão normal, que para γ =0,05 é 1,96, “P” é à proporção que maximiza o tamanho da amostra, 0,50, “E_0” é o erro amostral máximo tolerável, 0,05, e, “n_o”, trata-se da primeira aproximação para o tamanho mínimo da amostra, nesse caso 385 entrevistados.

O resultado da primeira aproximação para o cálculo do tamanho mínimo da amostra foi corrigido por meio da fórmula proposta por Barbetta, Reis e Bornia (2010, p.193):

$$n = \frac{N \times n_o}{N + n_o - 1}$$
$$n = \frac{307 \times 385}{307 + 385 - 1}$$
$$n = \frac{118195}{691}$$
$$n \cong 172 \text{ acadêmicos}$$

Em que “N” refere-se ao total de alunos do curso de Ciência da Computação da UNESC regularmente matriculados no ano/semestre 2015/02, e, “n” é o tamanho mínimo da amostra a ser pesquisada, que resultou em aproximadamente 172 entrevistados.

6.1.3 Plano de amostragem

Conforme dados disponíveis na tabela 1, foram entrevistados 15 alunos da primeira fase, 25 alunos da segunda fase, 21 alunos da terceira fase, 20 alunos da quarta fase, 15 alunos da quinta fase, 14 alunos da sexta fase, 10 alunos da sétima fase, 8 alunos da oitava fase e 44 alunos da nona fase. O processo de amostragem foi estratificado proporcionalmente, com amostragem aleatória simples dentro de cada estrato.

Tabela 1 - Plano de amostragem

Fase	N	%	n
1	27	8,79	15
2	45	14,66	25
3	38	12,38	21
4	36	11,73	20
5	26	8,47	15
6	25	8,14	14
7	18	5,86	10
8	13	4,23	8
9	79	25,73	44
∑	307	100,00	172

Fonte: Dados da pesquisa, 2015.

6.1.4 Utensílios de coleta de dados

Para a coleta de dados foi realizado um questionário sobre redes sem fio domésticas, elaborado pelo autor, e seu orientador. O questionário contém 19 perguntas, sendo dez delas descritivas (abertas) e nove de múltipla escolha, conforme no Apêndice A.

6.2 RESULTADOS OBTIDOS

Foram pesquisados 172 acadêmicos do curso de Ciência da Computação, predominantemente do sexo masculino (n = 154; 89,5%), com média de idade de 22,02 ± 3,73 anos, sendo o aluno mais jovem com 17 anos e o de mais idade com 40 anos. Demais resultados foram dispostos em tabelas com a respectiva descrição posterior às mesmas e apresentados a seguir.

6.2.1 Avaliação dos Resultados: Fases x Conhecimento

Tabela 2 – Idade e Sexo

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Idade (anos)	19,67±2,29	18,64±1,39	23,19±5,46	19,90±1,51	20,73±1,83	22,21±3,62	24,70±5,20	23,25±3,58	24,68±1,96	<0,001
Sexo										
Feminino	0(0,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	2(14,3)	1(10,0)	1(12,5)	8(18,2)	0,524
Masculino	15(100,0)	24(96,0)	18(85,7)	19(95,0)	14(93,3)	12(85,7)	9(90,0)	7(87,5)	36(81,8)	

Fonte: Dados da pesquisa, 2015.

Com relação ao questionamento Idade e Sexo, os alunos da segunda fase apresentaram, em média, idade significativamente menor que os alunos da sexta ($p = 0,013$), terceira ($p = 0,001$), oitava ($p = 0,007$), sétima ($p < 0,001$) e nona ($p < 0,001$) fases. Os alunos da primeira fase são significativamente mais jovens quando comparados aos alunos matriculados na sétima ($p = 0,027$) e nona ($p < 0,001$) fases. Os alunos matriculados na quarta fase são significativamente mais jovens que aqueles matriculados na sétima ($p = 0,036$) e nona ($p < 0,001$). Os alunos da quinta fase são significativamente mais novos que aqueles matriculados na nona fase ($p = 0,002$). Portanto, pode-se perceber bastante heterogeneidade quanto à idade, além de uma média elevada de idade na terceira, quinta, sexta, sétima, oitava e nona fases. A grande maioria dos alunos matriculados no curso é do sexo masculino, concentrando-se o maior número de indivíduos do sexo feminino na nona fase ($n = 8$; 18,2%), sendo que não se observou existência de associação entre gênero e fase ($p = 0,524$).

Tabela 3 – Q1, Q2, Q3, Q4

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q1										
Sim	15(100,0)	25(100,0)	21(100,0)	20(100,0)	15(100,0)	14(100,0)	10(100,0)	8(100,0)	44(100,0)	
Não	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	-
Q2										
Próprio	7(46,7)	12(48,0)	8(38,1)	16(80,0)	9(60,0)	9(64,3)	8(80,0)	6(75,0)	27(61,4)	
Técnico	7(46,7)	13(52,0)	11(52,4)	4(20,0)	6(40,0)	5(37,7)	2(20,0)	2(25,0)	16(36,4)	0,279
Amigo	1(6,7)	0(0,0)	2(9,5)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	
Q3										
Sim	11(73,3)	23(92,0)	13(61,9)	18(90,0)	11(73,3)	10(71,4)	9(90,0)	8(100,0)	36(81,8)	
Não	4(26,7)	2(8,0)	8(38,1)	2(10,0)	4(26,7)	4(28,6)	1(10,0)	0(0,0)	8(18,2)	0,138
Q4										
Sim	8(53,3)	12(48,0)	9(42,9)	13(65,0)	3(20,0)	8(57,1)	4(40,0)	3(37,5)	31(70,5)	
Não	6(40,0)	13(52,0)	12(57,1)	7(35,0)	12(80,0)	6(42,9)	6(60,0)	5(62,5)	12(27,3)	0,125
Não sei	1(6,7)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	
Proteção										
WEP	2(13,3)	0(0,0)	0(0,0)	4(20,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	3(6,8)	
WPA	2(20,0)	3(12,0)	4(19,0)	2(10,0)	0(0,0)	3(21,4)	1(10,0)	2(25,0)	13(29,5)	
WPA2	2(13,3)	7(28,0)	4(19,0)	4(20,0)	1(6,7)	4(28,6)	3(30,0)	0(0,0)	6(13,6)	
Controle por MAC	1(6,7)	2(8,0)	1(4,8)	1(5,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	4(9,1)	
Firewall	0(0,0)	0(0,0)	0(0,0)	2(10,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	0,096
Desabilitar o SSID	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	1(12,5)	2(4,5)	
Senha do administrador	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	3(6,8)	
Não se encaixa	7(46,7)	13(52,0)	12(57,1)	7(35,0)	12(80,0)	6(42,9)	6(60,0)	5(62,5)	13(29,5)	

Fonte: Dados da pesquisa, 2015.

Q1: Você sabe o que é uma rede Wireless (Sem Fio)?
Q2: Quem configurou o seu roteador Wi-Fi?
Q3: Você já acessou o console do seu roteador?
Q4: Você utiliza algum tipo de proteção no seu roteador? Se sim, qual?

Quando questionados se conheciam uma rede Wireless, todos os entrevistados afirmaram ter esse conhecimento. Embora exista uma tendência de o próprio aluno da quarta fase em diante configurar o seu roteador Wi-Fi, essa relação não se mostrou estatisticamente significativa (p = 0,279), provavelmente relacionada ao amadurecimento do aluno no curso, e, também a entrada no mercado de trabalho ou realização de estágios. Em todas as fases, percebe-se que a maioria dos alunos, já acessou o console do seu roteador (p = 0,138). Embora a maioria dos alunos utilize proteção no seu roteador, essa característica não foi observada na quinta, sétima e oitava fases, onde apenas 20,0% (n = 3), 40,0% (n = 4) e 37,5% (n = 3) respectivamente, utilizavam algum tipo de proteção (p = 0,125). Dos tipos de proteção mais utilizados, os mais frequentes, nas fases avaliadas, foram o WEP, WPA, WPA2 e controle por MAC, não havendo associação estatisticamente significativa (0,096).

Tabela 4 - Q5, Q6

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q5										
Sim	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	
Não	15(100,0)	24(96,0)	21(100,0)	20(100,0)	15(100,0)	13(92,9)	10(100,0)	8(100,0)	44(100,0)	0,466
Tipo de software para gerar senha										
LastPass	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	0,183
Não se encaixa	15(100,0)	25(100,0)	21(100,0)	20(100,0)	15(100,0)	13(92,9)	10(100,0)	8(100,0)	44(100,0)	
Q6										
1	1(6,7)	0(0,0)	1(4,8)	1(5,0)	0(0,0)	0(0,0)	1(10,0)	0(0,0)	1(2,3)	
2	3(20,0)	2(8,0)	2(9,5)	0(0,0)	5(33,3)	0(0,0)	0(0,0)	0(0,0)	4(9,1)	
3	5(33,3)	12(48,0)	7(33,3)	12(60,0)	5(33,3)	6(42,9)	2(20,0)	3(37,5)	13(29,5)	
4	0(0,0)	1(4,0)	2(9,5)	2(10,0)	3(20,0)	1(7,1)	0(0,0)	0(0,0)	6(13,6)	
5	2(13,3)	5(20,0)	1(4,8)	2(10,0)	1(6,7)	6(42,9)	1(10,0)	0(0,0)	6(13,6)	
6	0(0,0)	0(0,0)	2(9,5)	0(0,0)	0(0,0)	0(0,0)	1(10,0)	2(25,0)	3(6,8)	
7	0(0,0)	2(8,0)	1(4,8)	1(5,0)	0(0,0)	0(0,0)	1(10,0)	1(12,5)	3(6,8)	0,218
8	1(6,7)	1(4,0)	1(4,8)	0(0,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	2(4,5)	
9	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	
10	1(6,7)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(10,0)	1(12,5)	1(2,3)	
12	0(0,0)	0(0,0)	0(0,0)	1(5,0)	0(0,0)	0(0,0)	0(0,0)	1(12,5)	0(0,0)	
Não sei	2(13,3)	2(8,0)	4(19,0)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	

Fonte: Dados da pesquisa, 2015.

Q5 Você utiliza algum software para gerar senha? Se sim, qual?
Q6 Quantos dispositivos se conectam em sua rede? Se outros (especificar)?

Em todas as fases percebeu-se que a maioria dos alunos não utiliza algum tipo de software para gerar senha (p =0,446). Em relação aos tipos de software para gerar senha, essa característica foi observada na sexta fase onde apenas 7,1% (n=1), utiliza software para gerar senha, sendo este, o *LastPass*, não havendo associação estatisticamente significativa (p =

0,183). A respeito de quantos dispositivos se conectam na rede, a pesquisa apresentou que a maioria dos alunos tem em média três dispositivos conectados, estando este fato provavelmente relacionado à segurança, deixando acessar somente usuários confiáveis (p = 0,218).

Tabela 5 – Q7

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q7										
Sim	12(80,0)	24(96,0)	18(85,7)	19(95,0)	14(93,3)	14(100,0)	8(80,0)	8(100,0)	40(90,9)	0,429
Não	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	

Fonte: Dados da pesquisa, 2015.

Q7: Você sabe quais dispositivos se conectam no seu roteador?

Quando questionados se eles sabem quais dispositivos se conectam no seu roteador, a maioria dos alunos afirmou ter conhecimento sobre isso independentemente da fase em que estão matriculados (p = 0,429).

Tabela 6 – Q7

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q7										
Conecta-se ao roteador: Notebook										0,359
Sim	9(60,0)	16(64,0)	10(47,6)	12(60,0)	7(46,7)	7(50,0)	7(70,0)	4(50,0)	31(70,5)	
Não	3(20,0)	8(32,0)	8(38,1)	7(35,0)	7(46,7)	7(50,0)	1(10,0)	4(50,0)	9(20,5)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: Celular										
Sim	12(80,0)	17(68,0)	13(61,9)	16(80,0)	12(80,0)	10(71,4)	5(50,0)	6(75,0)	29(65,9)	0,557
Não	0(0,0)	7(28,0)	5(23,8)	3(15,0)	2(13,3)	4(28,6)	3(30,0)	2(25,0)	11(25,0)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: Smartphone										0,637
Sim	0(0,0)	3(12,0)	4(19,0)	1(5,0)	2(13,3)	3(21,4)	1(10,0)	1(12,5)	4(9,1)	
Não	12(80,0)	24(84,0)	14(66,7)	18(90,0)	12(80,0)	11(78,6)	7(70,0)	7(87,5)	36(81,8)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: Computador										0,187
Sim	4 (26,7)	15(60,0)	11(52,4)	11(55,0)	5(33,3)	9(64,3)	3(30,3)	6(75,0)	14(31,8)	
Não	8(53,3)	9(36,0)	7(33,3)	8(40,0)	9(60,0)	5(35,7)	5(50,0)	2(25,0)	26(59,1)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: SmartTv										
Sim	2(13,3)	4(16,0)	0(0,0)	2(10,0)	3(20,0)	1(7,1)	1(10,0)	2(25,0)	7(15,9)	0,617
Não	10(66,7)	20(80,0)	18(85,7)	17(85,0)	11(73,3)	13(92,9)	7(70,0)	6(75,0)	33(75,0)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: Tablet										
Sim	2(13,3)	3(12,0)	0(0,0)	5(25,0)	0(0,0)	1(7,1)	1(10,0)	4(50,0)	6(13,6)	0,057
Não	10(66,7)	21(84,0)	18(85,7)	14(70,0)	14(93,3)	13(92,09)	7(70,0)	4(50,0)	34(77,3)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	

Fonte: Dados da pesquisa, 2015.

Q7: Você sabe quais dispositivos se conectam no seu roteador? Se sim, quais?

Tabela 7 – Q7

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q7										
Conecta-se ao roteador: iPad										
Sim	0 (0,0)	2(8,0)	0(0,0)	1(5,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	0,603
Não	12(80,0)	22(88,0)	18(85,7)	18(90,0)	14(93,3)	14(100,0)	8(80,0)	8(100,0)	39(88,6)	
Não se encaixa	3(30,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	
Conecta-se ao roteador: Xbox										
Sim	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	3(21,4)	0(0,0)	1(12,5)	0(0,0)	0,015
Não	12(80,0)	23(92,0)	18(85,7)	19(95,0)	14(93,3)	11(78,6)	8(80,0)	7(87,5)	40(90,9)	
Não se encaixa	3(20,0)	1(4,0)	3(14,3)	1(5,0)	1(6,7)	0(0,0)	2(20,0)	0(0,0)	4(9,1)	

Fonte: Dados da pesquisa, 2015.
Q7: Você sabe quais dispositivos se conectam no seu roteador? Se sim, quais?

Em relação aos tipos de dispositivos que se conectam no roteador, mostrados nas tabelas 6 e 7, em todas a fases foi observado que os dispositivos menos utilizados pelos usuários foram Smartphone (p=0,637), SmartTv (p=0,617), Tablet (p=0,057), iPad (p= 0,603), Xbox (p=0,015). Dos tipos de dispositivos mais utilizados e conectados no roteador, os mais frequentes, nas fases avaliadas, foram notebook, celular e computador, provavelmente por serem dispositivos de uso comum em nossa região (p = 0,05).

Tabela 8 – Q8

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q8										
Sim	2(13,3)	4(16,0)	3(14,3)	3(15,0)	4(26,7)	0(0,0)	4(40,0)	3(37,5)	3(6,8)	0,002
Não	7(46,7)	17(68,0)	14(66,7)	16(80,0)	9(60,0)	14(100,0)	6(60,0)	5(62,5)	39(88,6)	
Não se encaixa	6(40,0)	4(16,0)	4(19,0)	1(5,0)	2(13,3)	0(0,0)	0(0,0)	0(0,0)	2(4,5)	
Tipo de restrição										
Senha	2(13,3)	1(4,0)	3(14,3)	0(0,0)	3(20,0)	0(0,0)	4(40,0)	3(37,5)	2(4,5)	0,034
Limite de Velocidade	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	
Controle por Mac	0(0,0)	2(8,0)	0(0,0)	3(15,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	2(4,5)	
Não se encaixa	13(86,7)	21(84,0)	18(85,7)	17(85,0)	11(73,3)	14(100,0)	6(60,0)	5(62,5)	40(90,9)	

Fonte: Dados da pesquisa, 2015.

Q8 Existe alguma restrição de acesso por dispositivo? Se sim, qual?

Quando se perguntou se existe alguma restrição por acesso ao dispositivo, esta foi mais percebida nos alunos da sétima e oitava fase, fato provavelmente relacionado com a sua entrada no mercado de trabalho (p=0,002). Dos tipos de restrição, observou-se que em todas as fases, a mais utilizada é restrição por senha. Provavelmente isso acontece, pois, esse tipo de restrição é um dos primeiros métodos a serem utilizados nas proteções de redes domésticas, para que ela não fique aberta para todos se conectarem.

Tabela 9 – Q9, Q10

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q9										
Sim	0(0,0)	1(4,0)	1(4,8)	1(5,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	0,107
Não	10(66,7)	23(92,0)	17(81,0)	19(95,0)	14(93,3)	14(100,0)	10(100,0)	8(100,0)	40(90,9)	
Não sei	5(33,3)	1(4,0)	3(14,3)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	3(6,8)	
Tipo de Limite de Velocidade										
Velocidade de Download	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0,856
Controle de Banda	0(0,0)	0(0,0)	0(0,0)	1(5,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(2,3)	
Não se encaixa	15(100,0)	24(96,0)	21(95,2)	19(95,0)	15(100,0)	14(100,0)	10(100,0)	8(100,0)	43(97,7)	
Q10										
1semana	1(6,7)	0(0,0)	0(0,0)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	
1 mês	2(13,3)	4(16,0)	2(9,5)	4(20,0)	0(0,0)	2(14,3)	0(0,0)	1(12,5)	6(13,6)	
3 meses	1(6,7)	1(4,0)	1(4,8)	0(0,0)	0(0,0)	0(0,0)	2(20,0)	0(0,0)	0(0,0)	0,088
4 meses	1(6,7)	0(0,0)	0(0,0)	1(5,0)	0(0,0)	2(14,3)	0(0,0)	0(0,0)	0(0,0)	
6 meses	1(6,7)	3(12,0)	1(4,8)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	1(12,5)	2(4,5)	
1 ano	2(13,3)	5(20,0)	4(19,0)	8(40,0)	5(33,3)	7(50,0)	1(10,0)	3(37,5)	19(43,2)	
Não se encaixa	7(46,7)	12(48,0)	13(61,9)	7(35,0)	8(53,3)	3(21,4)	7(70,0)	3(37,5)	17(38,6)	

Fonte: Dados da pesquisa, 2015.

Q9 Existe algum tipo de limitação de velocidade para alguns dos dispositivos? Se sim, quais?
Q10 Você tem o costume de trocar senha em quanto tempo?

Quando questionados se sabem se possuem algum tipo de limite de velocidade para alguns dos dispositivos, foi observado que na primeira, quinta, sexta, sétima e oitava fases os alunos não sabem (p=0,107). Foram observadas limitações quanto à velocidade de download, controle de banda, no entanto, esses foram relatos isolados (p = 0,856). O período mais frequente observado para troca de senhas foi o de 1 ano (p = 0,088).

Tabela 10 – Q11, Q12, Q13

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q11										
Sim	7(46,7)	13(52,0)	12(57,1)	14(70,0)	9(60,0)	8(57,1)	5(50,0)	4(50,0)	35(79,5)	0,242
Não	8(53,3)	12(48,0)	9(42,9)	6(30,0)	6(40,0)	6(42,9)	5(50,0)	4(50,0)	9(20,5)	
Q12										
Sim	1(6,7)	2(8,0)	0(0,0)	1(5,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	5(11,4)	0,003
Não	11(73,3)	23(92,0)	13(61,9)	19(95,0)	14(93,3)	14(100,0)	10(100,0)	8(100,0)	33(75,0)	
Não sei	3(20,0)	0(0,0)	8(38,1)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	6(13,6)	
Q13										
Sim	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0,266
Não	13(86,7)	25(100,0)	18(85,7)	20(100,0)	14(93,3)	14(100,0)	10(100,0)	8(100,0)	41(93,2)	
Não sei	2(13,3)	0(0,0)	3(14,3)	0(0,0)	1(6,7)	0(0,0)	0(0,0)	0(0,0)	3(6,8)	

Fonte: Dados da pesquisa, 2015.

Q11 Você tem costume de utilizar senhas complexas?
Q12 Existe algum tipo de filtro de conteúdo?
Q13 Existe algum controle por horário?

Quando questionados sobre a utilização de senhas complexas, observou-se que em todas as fases existem alunos que utilizam essa proteção, havendo predominância na nona fase (p=0,242). Já na utilização de filtro de conteúdo, a maioria dos alunos não utiliza essa proteção, sendo o seu uso mais frequente na nona fase (p = 0,003). Não foi observado a existência de controle por horário (p=0,266).

Tabela 11 – Q14

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q14										
Sim	0(0,0)	0(0,0)	0(0,0)	4(20,0)	0(0,0)	2(14,3)	1(10,0)	0(0,0)	5(11,4)	0,079
Não	15(100,0)	25(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7)	9(90,0)	8(100,0)	39(88,6)	
Presença de serviços: DNS										
Sim	0(0,0)	0(0,0)	0(0,0)	2(10,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	0,128
Não	0(0,0)	0(0,0)	0(0,0)	2(10,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	5(11,4)	
Não se encaixa	15(100,0)	2(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7)	9(90,0)	8(100,0)	39(88,6)	
Presença de serviços: DHCP										
Sim	0(0,0)	0(0,0)	0(0,0)	1(5,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	5(11,4)	0,038
Não	0(0,0)	0(0,0)	0(0,0)	3(15,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	0(0,0)	
Não se encaixa	15(100,0)	25(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7)	9(90,0)	8(100,0)	39(88,6)	
Presença de serviços: Firewall										
Sim	0(0,0)	0(0,0)	0(0,0)	2(10,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	0(0,0)	0,114
Não	0(0,0)	0(0,0)	0(0,0)	2(10,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	5(11,4)	
Não se encaixa	15(100,0)	25(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7) 0	9(90,0)	8(100,0)	39(88,6)	
Presença de serviços: SSA										
Sim	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	0,064
Não	0(0,0)	0(0,0)	0(0,0)	4(20,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	5(11,4)	
Não se encaixa	15(100,0)	25(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7) 0	9(90,0)	8(100,0)	39(88,6)	
Presença de serviços: FTP										
Sim	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(7,1)	0(0,0)	0(0,0)	0(0,0)	0,067
Não	0(0,0)	0(0,0)	0(0,0)	4(20,0)	0(0,0)	1(7,1)	1(10,0)	0(0,0)	4(9,1)	
Não se encaixa	15(100,0)	25(100,0)	21(100,0)	16(80,0)	15(100,0)	12(85,7)	9(90,0)	8(100,0)	40(90,9)	

Fonte: Dados da pesquisa, 2015.

Q14 Você sabe quais serviços estão rodando em seu roteador? Se sim, quais?

Embora a maioria dos alunos não saiba quais serviços estão executando em seu roteador, foi observado na quarta, sexta, sétima e nona fases, onde apenas 20,0% (n = 4), 14,3% (n=2), 10,0%(n=1), 11,4% (n=5) respectivamente, sabem quais são estes serviços (p=0,079), provavelmente relacionada à entrada no mercado de trabalho, realização de estágios ou até mesmo os alunos das fases finais terem cursado já a disciplina de redes de computadores. Dos tipos de proteção mais utilizados, os mais frequentes, nas fases avaliadas, foram o DNS (p=0,128) e DHCP (p=0,038).

Tabela 12 – Q15, Q16

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q15										
Sim	11(73,3)	21(84,0)	19(90,5)	18(90,0)	13(86,7)	11(78,6)	9(90,0)	7(87,5)	43(97,7)	0,339
Não	4(26,7)	4(16,0)	2(9,5)	2(10,0)	2(13,3)	3(21,4)	1(10,0)	1(12,5)	1(2,3)	
Q16										
Sim	15(100,0)	24(96,0)	21(100,0)	19(95,0)	13(86,7)	14(100,0)	10(100,0)	7(87,5)	43(97,7)	0,363
Não	0(0,0)	1(4,0)	0(0,0)	1(5,0)	2(13,3)	0(0,0)	0(0,0)	1(12,5)	1(2,3)	

Fonte: Dados da pesquisa, 2015.

Q15 Você acha correto a rede Wireless ser restrita/protegida por motivo de segurança?
Q16 Já acessou roteadores Wi-Fi em ambientes públicos (abertos)?

Quando questionados se acham correto a rede wireless ser restrita /protegida por motivo de segurança, a grande maioria afirmou que acha correto (p=0,339). Foi observado que alguns alunos disseram que não acham correto, certamente isso aconteceu, pois esses alunos não tem conhecimento sobre proteção de redes e não sabem os riscos que podem ocorrer em uma rede desprotegida. Em todas as fases, a maioria dos alunos afirmaram ter acessado a Wi-Fi em ambientes públicos (p=0,363).

Tabela 13 – Q17

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q17										
Sim	9(60,0)	8(32,0)	5(23,8)	9(45,0)	8(53,3)	8(57,1)	3(30,0)	6(75,0)	13(29,5)	0,059
Não	6(40,0)	17(68,0)	16(72,2)	11(55,0)	7(46,7)	6(42,9)	7(70,0)	2(25,0)	31(70,5)	
Motivo de achar seguro:										
Nunca teve problema	3(20,0)	3(12,0)	3(14,3)	7(35,0)	2(13,3)	2(14,3)	1(10,0)	3(37,5)	6(13,3)	
Só usa serviços básicos	1(6,7)	1(4,0)	2(9,5)	1(5,0)	2(13,3)	2(14,3)	1(10,0)	2(25,0)	1(2,3)	
Não acesso informações pessoais	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	2(14,3)	0(0,0)	0(0,0)	3(6,8)	0,014
Redes possuem proteções	1(6,7)	2(8,0)	0(0,0)	0(0,0)	3(20,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	
Usa Linux como monitoramento	0(0,0)	1(4,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	0(0,0)	
Sentem-se seguros	4(26,7)	0(0,0)	0(0,0)	1(5,0)	0(0,0)	2(14,3)	0(0,0)	0(0,0)	2(4,5)	
Uso de senhas	0(0,0)	0(0,0)	0(0,0)	0(0,0)	1(6,7)	0(0,0)	1(10,0)	1(12,5)	1(2,3)	
Não se encaixa	6(40,0)	17(68,8)	16(76,2)	11(55,0)	7(46,7)	6(42,9)	7(70,0)	2(25,0)	31(70,5)	
Motivo de não achar seguro:										
Rede desprotegida	4(26,7)	11(44,0)	7(33,3)	7(35,0)	5(33,3)	4(28,6)	4(40,0)	1(12,5)	13(29,5)	0,033
Usuários mal - intencionados	1(6,7)	5(20,0)	3(14,3)	2(10,0)	0(0,0)	0(0,0)	2(20,0)	0(0,0)	1(2,3)	
Invasão na rede	1(6,7)	1(4,0)	6(28,6)	3(15,0)	2(13,3)	2(14,3)	1(10,0)	1(12,5)	17(38,6)	
Não se encaixa	9(60,0)	8(32,0)	5(23,8)	8(40,0)	8(53,3)	8(57,1)	3(30,0)	6(75,0)	13(29,5)	

Fonte: Dados da pesquisa, 2015.

Q17 Você sente segurança ao utilizar estes serviços públicos? (Aeroporto, shopping). Se sim por quê? Se não por quê?

Quanto a utilização de serviços públicos, a maioria dos alunos da segunda, terceira, quarta, sétima e nona fase não se sentem seguros (p = 0,059), principalmente pelo fato de a rede ser desprotegida (p = 0,033). Os alunos que sentem-se seguros em acessar esse tipo de serviço, somente utilizam serviços básicos ou nunca tiveram problemas (p = 0,014).

Tabela 14 – Q18

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q18										
Insegurança pesquisas profissionais										
Sim	3(20,0)	4(16,0)	4(19,0)	3(15,0)	1(6,7)	2(14,3)	4(40,0)	2(25,0)	20(45,5)	0,027
Não	12(80,0)	21(84,0)	17(81,0)	15(85,0)	14(93,3)	12(85,7)	6(60,00	6(75,0)	24(54,3)	
Insegurança de download										0,135
Sim	4(26,7)	7(28,0)	7(33,3)	3(15,0)	1(6,7)	2(14,3)	2(20,0)	4(50,0)	5(11,4)	
Não	11(73,3)	18(72,0)	14(66,7)	17(85,0)	14(93,3)	12(85,7)	8(80,0)	4(50,0)	39(88,6)	
Insegurança redes sócias										0,001
Sim	7(46,7)	17(68,0)	9(42,9)	10(50,0)	7(46,7)	9(64,3)	4(40,0)	5(62,5)	6(13,6)	
Não	8(53,3)	8(32,0)	12(57,1)	10(50,0)	8(53,3)	5(35,7)	6(60,0)	3(37,5)	38(86,4)	
Insegurança serviços bancários										0,010
Sim	13(86,7)	23(92,0)	16(76,2)	19(95,0)	8(53,3)	14(100,0)	8(80,0)	7(87,5)	30(68,2)	
Não	2(13,3)	2(8,0)	5(23,8)	1(5,0)	7(46,7)	0(0,0)	2(20,0)	1(12,5)	14(31,8)	
Insegurança noticias, jornais e revistas										0,361
Sim	1(6,7)	0(0,0)	2(9,5)	0(10,0)	0(0,0)	0(0,0)	1(10,0)	1(12,5)	1(2,3)	
Não	14(93,3)	25(100,0)	19(90,5)	20(100,0)	15(100,0)	14(100,0)	9(90,0)	7(87,5)	43(97,7)	
Insegurança em compras										0,000
Sim	14(93,3)	21(84,0)	13(61,9)	14(70,0)	8(53,3)	14(100,0)	8(80,0)	7(87,5)	14(38,1)	
Não	1(6,7)	4(16,0)	8(38,1)	6(30,0)	7(46,7)	0(0,0)	2(20,0)	1(12,5)	30(68,2)	

Fonte: Dados da pesquisa, 2015.

Q18 Quais desses serviços você acha que é inseguro acessar em ambientes públicos? (Pode assinalar mais de uma opção).

Quando questionados quais desses serviços são inseguros acessar em ambientes públicos, em todas as fases a maioria afirmaram insegurança em serviços bancários (p=0,010), redes sociais (p=0,001), e compras (p=0,000), provavelmente foram escolhidas essas opções por serem expostos na rede os dados pessoais, sendo submetidos a riscos roubos.

Tabela 15 – Q19

	Fase									Valor-p
	1°	2°	3°	4°	5°	6°	7°	8°	9°	
Q19										
Sim	10(66,7)	13(52,0)	15(7,1)	17(85,0)	7(46,7)	8(57,1)	7(70,0)	6(75,0)	26(59,1)	0,332
Não	5(33,3)	12(48,0)	6(28,6)	3(15,0)	8(53,3)	6(42,9)	3(30,0)	2(25,0)	18(40,9)	

Fonte: Dados da pesquisa, 2015.

Q19 Já experimentou acesso em redes sem autorização?

Quando perguntado aos alunos se eles já utilizaram redes sem autorização, em todas as fases apresentou que a maioria já fez este tipo de acesso (p=0,332).

6.2.2 Avaliação dos resultados: Cruzamento

Para realizar o cruzamento de perguntas, foi escolhida a questão Q3 do questionário, sendo ela, relacionada com as questões Q7, Q8, Q9, Q10, Q12, Q13 e Q14, porque para utilizar esses tipos de proteções, controlar os dispositivos na rede entre outras funções, precisa-se já ter acessado o console do roteador.

Tabela 16 - Cruzamento questão Q3 x Q7

	Você já acessou o console do seu roteador?		Valor-p
	Sim	Não	
Q7			
Sim	131(94,2)	26(78,8)	0,005
Não	8(5,8)	7(21,2)	
Roteador: Notebook			
Sim	83(59,7)	20(60,6)	
Não	48(34,5)	6(18,2)	0,008
Não se encaixa	8(5,8)	7(21,2)	
Roteador: Celular			
Sim	98(70,5)	22(66,7)	
Não	33(23,7)	4(12,1)	0,011
Não se encaixa	8(5,8)	7(21,2)	
Roteador: Smartphone			
Sim	16(11,5)	3(9,1)	
Não	115(82,7)	23(69,7)	0,018
Não se encaixa	8(5,8)	7(21,2)	

Fonte: Dados da pesquisa, 2015.

Q7 Você sabe quais dispositivos se conectam no seu roteador? Se sim, quais?

Tabela 17 - Cruzamento questão Q3 x Q7

	Você já acessou o console do seu roteador?		Valor-p
	Sim	Não	
Roteador: Computador			
Sim	70(50,4)	8(24,2)	
Não	61(43,9)	18(54,5)	0,003
Não se encaixa	8(5,8)	7(21,2)	
Roteador: SmartTv			
Sim	21(15,1)	1(3,0)	
Não	110(79,1)	25(75,8)	0,006
Não se encaixa	8(5,8)	7(21,2)	
Roteador: Tablet			
Sim	21(15,1)	1(3,0)	
Não	110(79,1)	25(75,8)	0,006
Não se encaixa	8(5,8)	7(21,2)	
Roteador: iPad			
Sim	4(2,9)	0(0,0)	
Não	127(91,4)	26(78,8)	0,013
Não se encaixa	8(5,8)	7(21,2)	
Roteador: Xbox			
Sim	4(2,9)	1(3,0)	
Não	127(91,4)	25(75,8)	0,018
Não se encaixa	8(5,8)	7(21,2)	

Fonte: Dados da pesquisa, 2015.
Q7 Você sabe quais dispositivos se conectam no seu roteador? Se sim, quais?

Foi observado em todas as fases, nas tabelas 16 e 17, que os alunos sabem quais dispositivos estão conectados em seu roteador, isso é porque já acessaram o console do roteador (p=0,005). Os tipos de dispositivos mais utilizados foram notebook (p=0,008) celular (p=0,011) e computador (p=0,003).

Tabela 18 - Cruzamento questão Q3 x Q8 e Q3 x Q9

	Você já acessou o console do seu roteador?		Valor-p
	Sim	Não	
Q8			
Sim	21(15,1)	5(15,2)	
Não	107(77,0)	20(60,6)	0,025
Não se encaixa	11(7,9)	8(24,2)	
Tipo de restrição de velocidade			
Senha	13(9,4)	5(15,2)	
Limite de velocidade	1(0,7)	0(0,0)	0,392
Controle de Mac	8(5,8)	0(0,0)	
Não se encaixa	117(84,2)	28(84,8)	
Q9			
Sim	2(1,4)	2(6,1)	
Não	133(95,7)	22(66,7)	0,001
Não se encaixa	4(2,9)	9(27,3)	
Tipo de limite de velocidade			
Velocidade de download	1(0,7)	0(0,0)	
Controle de banda	1(0,7)	1(3,0)	0,480
Não se encaixa	137(98,6)	32(97,0)	

Fonte: Dados da pesquisa, 2015.

Q8 Existe alguma restrição de acesso por dispositivo? Se sim, qual?
Q9 Existe algum tipo de limitação de velocidade para alguns dos dispositivos? Se sim, qual?

Em todas as fases, observou-se que dos que afirmaram existir algum tipo de restrição por dispositivo, provavelmente tinham conhecimento por já terem acessado o console de seu roteador ou o técnico tenha informado (p=0,025), Dos tipos de restrição, as mais utilizadas via acesso ao console do roteador para a proteção de suas redes domésticas, foram senha e controle por Mac (p=0,392). E também sobre tipo de limitação de velocidade por dispositivos, poucos alunos afirmaram ter em sua rede doméstica (p=0,001). Dos tipos de limitação, os citados na pesquisa foram velocidade de download e controle de banda (p=0,480).

Tabela 19 - Cruzamento questão Q3 x Q10, Q3 x Q12 e Q3 x Q13

	Você já acessou o console do seu roteador?		Valor-p
	Sim	Não	
Q10			
1 semana	2(1,4)	0(0,0)	
1 mês	18(12,9)	3(91,1)	
3 meses	4(2,9)	1(3,0)	
4 meses	4(2,9)	0(0,0)	0,533
6 meses	8(5,8)	1(3,0)	
1 ano	46(33,1)	8(24,2)	
Não se encaixa	57(41,0)	20(60,6)	
Q12			
Sim	8(5,8)	1(3,0)	
Não	123(88,5)	22(66,7)	0,001
Não se encaixa	8(5,8)	10(30,3)	
Q13			
Sim	0(0,0)	0(0,0)	
Não	133(95,7)	30(90,9)	0,376
Não se encaixa	6(4,3)	3(9,1)	

Fonte: Dados da pesquisa, 2015.
Q10 Você tem o costume de trocar senha em quanto tempo?
Q12 Existe algum tipo de filtro de conteúdo?
Q13 Existe algum controle por horário?

Para a proteção das redes domésticas, dos alunos que afirmaram ter costume de trocar senha periodicamente, ocorre essa troca devido já ter acessado via console do seu roteador para fazer essas alterações (p=0,533). Dos tempos de troca de senha em todas as fases, os mais utilizados foram 1 mês, 6 meses e 1 ano. Embora na utilização de filtro de conteúdo, a maioria dos alunos não utiliza esse tipo de proteção (p= 0,001), só poderá ser feita, via console do roteador. Também sobre algum tipo de controle por horário, todos os alunos afirmaram não fazer uso desta proteção, talvez não seja só por não ter acessado o console do seu roteador, mais sim por não ter conhecimento sobre a importância de controle por horário para a proteção de redes (p=0,376).

Tabela 20 - Cruzamento questão Q3 x Q14

	Você já acessou o console do seu roteador?		Valor-p
	Sim	Não	
Q14			
Sim	12(8,6)	0(0,0)	0,126
Não	127(91,4)	33(100,0)	
Presença de serviços: DNS			
Sim	3(2,2)	0(0,0)	
Não	9(6,5)	0(0,0)	0,126
Não se encaixa	127(91,4)	33(100,0)	
Presença de serviços: DHCP			
Sim	7(5,0)	0(0,0)	
Não	5(3,6)	0(0,0)	0,216
Não se encaixa	127(91,4)	33(100,0)	
Presença de serviços: Firewall			
Sim	4(2,9)	0(0,0)	
Não	8(5,8)	0(0,0)	0,216
Não se encaixa	127(91,4)	33(100,0)	
Presença de serviços: SSA			
Sim	1(0,7)	0(0,0)	
Não	11(7,9)	0(0,0)	0,216
Não se encaixa	127(91,4)	33(100,0)	
Presença de serviços: FTP			
Sim	1(0,7)	0(0,0)	
Não	10(7,2)	0(0,0)	0,248
Não se encaixa	128(92,1)	33(100,0)	

Fonte: Dados da pesquisa, 2015.

Q14 Você sabe quais serviços estão rodando em seu roteador? Se sim, quais?

Em todas as fases contatou-se que a grande maioria não sabe quais serviços estão executando em seu roteador, mas para saber precisa ter feito o acesso via console do roteador, assim terá como acessar as demais funções do roteador. Dos tipos de serviços que rodam no roteador, em todas as fases avaliadas, foram DNS (p=0,126) e DHCP (p=0,216).

Comparando com uma pesquisa similar realizada por Silva et al. (2011), percebeu-se que a grande maioria dos entrevistados possui ou utiliza redes sem fio domésticas. Tratando-se em segurança da rede sem fio doméstica, notou-se que há uma grande diferença entre os trabalhos, pois este tem um grande índice de pessoas que utilizam senhas complexas para a maior segurança de sua rede. Ao contrário da outra pesquisa que poucos se preocupam com o uso.

Outro aspecto importante abordado nos dois trabalhos: foi que a grande maioria já acessou ambientes públicos (abertos). Devido a essas informações se torna preocupante por serem expostos na rede os seus dados pessoais, qualquer pessoa que possua um entendimento sobre redes pode tentar ter acesso a todos os dados existentes na mesma. É importante destacar que em ambas as pesquisas os usuários se preocupam com a integridade de seus dados, mas poucos aplicam os tipos mais comuns de segurança em suas redes sem fio domésticas.

Também outra pesquisa similar realizada por Diana Filho (2003), para segurança de redes sem fio domésticas, foi configurar o roteador utilizando as políticas de segurança mínimas para a proteção da rede, como por exemplo, o uso de senhas complexas, criptografia WPA2, desabilitar o *SSID Broadcast,* filtro MAC entre outros. Referente à segurança de redes sem fio domésticas, notou-se que há uma diferença entre os trabalhos, pois para a proteção da rede foi utilizado à ferramenta Orinoco Client Manager, e seus utensílios podem desabilitados e habilitados na mesma. A criptografia WEP não é considerada segura para proteções de redes domésticas, mas com o uso de autenticação RADIUS torna o protocolo WEP mais seguro. É importante destacar que nos dois trabalhos pelos menos são utilizados alguns métodos mínimos de segurança nas redes domésticas.

No próximo capítulo será proposto uma aplicação prática de política de segurança mínima, com o objetivo de proteger redes sem fio domésticas. Será apresentado procedimentos básicos a serem adotados por usuários para melhorar a condição de segurança de suas redes.

7 APLICAÇÃO PRÁTICA DE UMA POLÍTICA DE SEGURANÇA MÍNIMA

Ao instalar uma rede sem fio doméstica deve-se possuir conhecimento sobre a configuração do seu roteador e os riscos que possam ocorrer em uma rede mal configurada, por isso não é simplesmente instalar suas configurações, todo cuidado é preciso para que ela esteja funcionando corretamente pelo menos com suas configurações básicas.

Com isso foi aplicado um cenário de segurança de redes sem fio domésticas, demostrado o mínimo de procedimentos para proteção de uma rede. Portanto no cenário foram utilizados os respectivos equipamentos: um roteador TP-LINK, 150Mbps *wireless Lite N Router*, modelo NO. TLWR741N / TL-WR741ND. Um notebook Sony Vaio, processador Intel (R) Core (TM) I3 CPU M380 @ 2,53 GHz, sistema operacional de 64 bits, Windows 7, memória instalada (RAM) 4.00 GB.

De acordo com as contramedidas utilizadas para o cenário de rede sem fio doméstica, investigou-se inseguranças na rede e nele foram aplicadas políticas de segurança mínimas. Portanto, no cenário considerado, foram utilizadas as medidas preventivas.

Para acesso à configuração do roteador foi inserido o endereço de IP no navegador, de forma a obter acesso à interface de configuração. Nesta página foi obrigatório inserir o nome do usuário e senha do roteador, por ventura os mesmos vêm com padrão de fábrica, então por segurança a senha deve ser mudada, para que nenhum intruso tenha acesso às configurações e as modifique.

Dando início à página de configuração do roteador TL-WR741N, conforme a opção Network – Lan da configuração do roteador, o IP *Address* vem como padrão de fábrica, para a segurança dessa rede foi mudado esse endereço, com isso, dificultará os intrusos de acessar a rede com esse novo endereço.

Pelo fato, das redes sem fio domésticas transmitirem informações por ondas via rádio, às vezes ocorrem interferências de canais de redes Wi-Fi, por isso, aparece o baixo sinal, impedindo o acesso à Internet, isso pode acontecer porque a rede possui o mesmo canal de um roteador próximo ou também pode ser que este canal seja igual ao das redes próximas. Um modo prático para desvendar quais canais possuem suas redes próximas, a fim de melhorar o sinal da rede Wi-Fi, é de utilizar, por exemplo, um programa para fazer uma varredura dos canais utilizados e escolher um disponível. Com isso deve-se procurar um horário em que as redes

estejam ligadas para executar a varredura. Com esses procedimentos foi possível saber quais redes possuem o mesmo canal (BRITO, 2013). Os canais mais utilizados nas redes sem fio domésticas são o 1, 6, 11 (SILVA; SOUZA FILHO; RODRIGUES, 2010).

É possível desabilitar a opção *Enable SSID Broadcast*, com isso, a rede ficará oculta a todos, e o roteador não transmitirá o nome da rede no ar, sendo assim uma maneira de segurança para a rede. Mesmo o intruso sabendo que possui rede oculta, para acessá-la o mesmo necessita que o nome seja colocado manualmente junto com a senha.

Uma rede segura não necessita só colocar um novo nome à rede e ocultá-la, também precisa haver o cuidado ao ocultá-la, pois se o intruso utilizar a ferramenta de scanner, o mesmo terá acesso aos pacotes trafegados na rede. Por isso foi utilizado uma criptografia de segurança, conforme na opção Wireless Security, possuem os tipos de criptografias de segurança de redes sem fio, sendo elas WEP, WPA/WPA2 e a versão WPA-PSK/WPA2-PSK.

Dentre essas criptografias a mais utilizada é WPA-PSK/WPA2-PSK, após selecionar esta versão para proteção da rede, nela utiliza-se a chave de segurança AES. Ao contrário do WPA-PSK/WPA2-PSK, temos o WEP, este protocolo não é considerado seguro, pois ele mostra o número máximo de senhas a serem inseridas e sua criptografia já foi quebrada. Sendo hoje WPA-PSK/WPA2-PSK o mais seguro, pois ainda não conseguiram quebrar sua criptografia, nesse protocolo foi inserido uma senha com 8 dígitos, pelo menos ao máximo de 64 letras, para melhor segurança da rede.

Para possuir um controle de endereços que trafegam na rede, tem-se a opção Wireless MAC *Filtering*, a mesma pode permitir ou negar acesso à rede. A opção *Allow* será utilizada para permitir o acesso de endereços cadastrados. Já opção *Deny* será utilizada para negar que endereços específicos se conectem a rede.

Com isso, para identificar os intrusos conectados à rede, por segurança foi utilizada a opção DHCP List, a mesma exibe quantos endereços de IP estão conectados ao roteador, se acaso além dos usuários confiáveis tenha mais endereços, mostrará a relação de usuários conectados a rede. Então conforme a opção Wireless MAC *Filtering,* selecionando a opção *Deny,* o intruso conectado a rede será bloqueado e mesmo que ele tenha a senha para acesso, o intruso não se

conectará novamente a rede, nela mostrará falha ao conectar-se, isso só ocorrerá se a opção Wireless Mac *filtering* estiver habilitada.

Mais um controle do que uma segurança com a opção Parental controle *settings*, a mesma terá um limite de acesso a determinadas páginas na Internet não confiáveis, e também no *Advance schedule settings* é designado para possuir o controle de horário do usuário, determinado por dia, 24 horas, início de horário e o término de horário, ao cumprir esse horário a rede será desligada.

8 CONCLUSÃO

Neste trabalho, foi possível verificar que a utilização das redes sem fio domésticas, ainda trazem muita insegurança. Isso porque ao longo de todas as análises colhidas, observou-se que muitos usuários do curso de Ciência da Computação não possuem conhecimento adequado ou não demonstram importância acerca destes procedimentos.

As redes Wi-Fi trouxeram a mobilidade para seus usuários, no entanto ficam visíveis e enviam sinais para todos os lados por ondas de rádio, por conta disso, precisa-se utilizar procedimentos de proteção desta rede.

Na pesquisa percebeu-se que da quarta fase em diante os próprios usuários fizeram a configuração de seu roteador, devido o conhecimento adquirido ao longo do curso ou por conta própria. Em face disso, a maioria dos usuários afirmaram já terem acessado o console de seu roteador.

Segundo os dados colhidos uma grande parte dos alunos demonstraram possuir alguma proteção no roteador, de outro lado, notou-se que na quinta, sétima e oitava fases, não foi observada esta característica. Sobre o software para gerar senha a maioria não faz o uso deste recurso, provavelmente por não saber a sua importância necessária aos sistemas de segurança.

Importante destacar que a maioria dos usuários que possuem restrição por acesso a dispositivos estão concentrados na sétima e oitava fase, certamente pela realização de estágios ou conhecimento adquirido ao longo do curso. Observou-se que a maioria dos alunos utilizam senhas complexas, possuindo uma predominância na nona fase. Já na utilização de filtro de conteúdo, a maioria dos alunos não utiliza essa proteção. Não foi observada a existência de controle por horário em nenhuma resposta.

Importante ainda lembrar, que muito embora existam procedimentos de segurança para redes sem fio domésticas, a maioria dos alunos não sabem os serviços que executam em seu roteador, com isso os usuários não têm um controle mínimo sobre sua rede. Sobre a pergunta se acham correto a rede wireless ser restrita /protegida por motivo de segurança, a grande maioria afirmou que acha correto.

Também ficou demonstrado que a maioria dos alunos já acessou ambientes públicos e não sente segurança em acessá-lo, a situação se torna

preocupante, pois não se tem um controle de quantos dispositivos estariam conectados a rede.

Quando perguntados sobre quais serviços são inseguros acessar em ambientes públicos, em todas as fases a maioria afirmaram insegurança em serviços bancários, redes sociais e compras, provavelmente foram escolhidas essas opções por serem expostos na rede os dados pessoais.

É importante destacar sobre a utilização de redes sem autorização, em todas as fases apresentou que a maioria já fez este tipo de acesso. Nesse sentido, de acordo com toda a pesquisa realizada, a recomendação à aplicação de uma política de segurança para evitar problemas na rede.

Após os resultados da pesquisa, foi realizado um experimento a fim de demostrar os métodos mínimos de segurança a serem aplicados nas redes sem fio domésticas. Sendo alguns destes métodos: utilizar senhas complexas e alterar com frequência, modificar o endereço de IP do roteador. Se ocorrer interferências de canais em redes Wi-Fi, foi recomendado utilizar um programa para fazer a varredura dos canais utilizados e escolher um disponível. Também desabilitar o *SSID Broadcast* para não aparecer o nome da rede no ar, habilitar criptografia, foi verificado na lista DHCP, nela possui o controle de quantos endereços de IP estão conectados no roteador, então se a caso possuir intrusos, foi habilitado o filtro MAC. O filtro de conteúdo foi utilizado para bloquear conteúdos não confiáveis. Outro recurso que foi utilizado é o controle de horário, nele possui o início e o término em que a rede pode permanecer ligada.

Este trabalho permitiu um grande aprendizado sobre a segurança de redes sem fio domésticas, onde existem vários tipos de ameaças e ataques que podem ser minimizados com aplicação de uma política de segurança mínima.

Como trabalhos futuros, esta pesquisa pode ser aprofundada quanto à aplicação das políticas de segurança das redes sem fio domésticas, dando continuidade na análise de outros grupos e contramedidas estratégicas, uma vez que com avanço da tecnologia estas sempre podem ser aprimoradas.

REFERÊNCIAS

ALVES. **Segurança em redes sem fio.** O caso da Assembleia Nacional de Cabo Verde. Disponível em: <http://bdigital.unipiaget.cv:8080/jspui/bitstream/10964/148/1/Walter%20Alves.pdf>. Acesso em: 12 set. 2015.

AMARAL, Allan Francisco Forzza. **Redes de Computadores.** Disponível em: <http://sistemas.riopomba.ifsudestemg.edu.br/dcc/materiais/402283130_redes-computadores.pdf>. Acesso em: 22 ago. 2014.

BARBETTA, Pedro Alberto; REIS, Marcelo Menezes; BORNIA, Antônio Cezar. **Estatística para Cursos de Engenharia e Informática**. 3 ed. São Paulo: Atlas, 2010.

BOF, Edson. **Segurança em redes wireless**. 2010. 58 f. Monografia (Especialista em Gestão da Segurança da Informação) - Faculdade do Centro Leste, Serra, 2010. Disponível em: <http://br.monografias.com/trabalhos-pdf/seguranca-redes-wireless/seguranca-redes-wireless.pdf>. Acesso em: 22 set. 2015.

BRASIL ESCOLA. **Segurança em Redes de Computadores.** Disponível em: <http://www.brasilescola.com/informatica/seguranca-redes.htm>. Acesso em: 13 out. 2015.

CARAÇA, Francislaine Vanessa; PENNA, Roberta Galacine. **Segurança em redes sem fio: desafios, vulnerabilidades e soluções.** Disponível em: <http://fatecsjc.edu.br/trabalhos-de-graduacao/wpcontent/uploads/2012/03/BDR1_franscislaine_roberta2009.pdf>. Acesso em: 20 out.2015.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de computadores**. 2 ed. Porto Alegre: Bookman, 2009.

CARLESSI, Lucas da Silva. **Estudos de caso de segurança em redes sem fio utilizando ferramentas para monitoramento e detecção de ataques.** Disponível em: < http://tcc.kironunesc.net.br/arquivos/trabalhos/279.pdf>. Acesso em: 18 set.2015

CERT.br, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil.2012. Disponível em: < http://cartilha.cert.br/ataques/>. Acesso em: 25 ago. 2015.

_____. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil.2012. Disponível em: <http://cartilha.cert.br/redes/>. Acesso em: 28 ago. 2015.

CORRÊA JÚNIOR, Marcos Antônio Costa. **Evolução da Segurança em Redes sem Fio**. Disponível em: <http://www.cin.ufpe.br/~tg/2008-1/maccj.pdf>. Acesso em: 16 set. 2015.

CUNHA NETO, Raimundo Pereira da. **Vulnerabilidades em Redes Wireless**. Faculdade Faete. Teresina-PI, 2011. Disponível em: <http://www.faete.edu.br/revista/Artigo_VulnerabilidadesemRedesSemFios.pdf>. Acesso em: 08 out. 2014.

CUTRIM, Carlos Magno de Oliveira. **Segurança em Redes**: Segurança em Redes Sem Fio. 2013. 69 f. Monografia (Especialista em Segurança da Informação) - Faculdade SENAC do Distrito Federal – FACSENAC/DF, Brasília, 2013. Disponível em: <http://www.edilms.eti.br/uploads/file/orientacoes/seg02%20Carlos%20Magno%20de%20Oliveira%20Cutrim-TCC-final.pdf>. Acesso em: 04 set. 2014.

DEMARTINI. **WEP, WPA, WPA2:** O que as siglas significam para o seu Wi-Fi? Disponível em: <http://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>. Acesso em: 10 nov. 2014.

DIANA FILHO, Rogério Pereira. **Uma abordagem sobre segurança em redes wireless**. 2003. 90 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Presidente Antônio Carlos, 2003. Disponível em: <http://www.barbacena.unipac.br/site/bb/tcc/tcc-a517345722726c9a4e50e51eae58e3ac.pdf>. Acesso em: 08 out. 2014.

DUARTE, Carlos Anderson Andrade. **A Evolução dos Protocolos de Segurança das Redes Sem Fio: do Wep ao Wpa2 passando pelo Wpa**. 2010. 51 f. Monografia (Especialista em Redes de Computadores) – Pós-Graduação em Redes de Computadores da Escola Superior Aberta do Brasil. Vila Velha, 2010. Disponível em: <http://www.esab.edu.br/arquivos/monografias/carlos-anderson-andrade-duarte.pdf>. Acesso em: 08 out. 2014.

FARIA, Cristiano Henrique. **Segurança em redes sem fio e aplicação de sistema especialista para verificar a vulnerabilidade de redes.** Monografia. Jaguariúna, 2007.

FERREIRA, Érico José. **Segurança de Redes de Computadores**. UNIERO Centro Universitário. Brasília, 2009. Disponível em: <http://www.ericonet.com.br/admin/material/Seguranca_de_Redes_de_Computadores.pdf>. Acesso em: 10 set. 2014.

FERREIRA. **Diferentes tipos de Rede Wireless.** Disponível em: <http://www.oficinadanet.com.br/post/11081-rede-wireless>. Acesso em: 10 ago. 2014.

FERREIRA, Jeferson Luiz Miranda. **Segurança em Redes Sem Fio.** Universidade Tecnológica Federal do Paraná Departamento Acadêmico de Eletrônica Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, 2013. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf>. Acesso em: 10 mai 2015.

FIELD, Andy P. **Discovering statistics using SPSS**. Los Angeles, 2009.

FURGERI, Sérgio. **Projeto de Redes**. Seção Materiais. São Paulo, sd. Disponível em: <http://www.sergio.pro.br/trabalhos/34_topologias.pdf>. Acesso em: 08 out. 2014.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4ªed. São Paulo: Atlas, 2007.

GRASEL. **O que é e como funciona a 4G?** Disponível em: <http://www.oficinadanet.com.br/post/12569-o-que-e-e-como-funciona-4g>. Acesso em: 18 set. 2014.

GUIMARÃES. **Análise de Vulnerabilidades dos Principais Protocolos de segurança de Redes Sem Fio Padrão IEEE 802.11.** Disponível em: <http://www2.ic.uff.br/~celio/alumni/monografia-diego-guimaraes.pdf>. Acesso em: 18 mar. 2015.

GOMES, Olavo José Anchieschi. **Segurança total.** São Paulo: Makron Books, 2000.

HAMMERSCHMIDT, Roberto. **O que é 3G?** Disponível em: <http://www.tecmundo.com.br/celular/226-o-que-e-3g-.htm>. Acesso em: 12 nov. 2014.

INFOWEBSTER. **Hubs Witch Router.** Disponível em: <http://www.infowester.com/hubswitchrouter.php.alecrim>. Acesso em: 21 ago. 2014.

INFORWESTER. Tecnologia Bluetooth: **O que é e como funciona?** Disponível em: <http://www.infowester.com/bluetooth.php>. Acesso em: 18 set. 2014.

KUROSE James F; ROSS, Keith W. **Redes de Computadores e a Internet.** São Paulo: Pearson Addison Wesley, 2006.

LAUFER et al. **Negação de Serviço:** Ataques e Contramedidas. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/LMVB05a.pdf>. Acesso em: 05 nov. 2014.

LIMA. **Uma Abordagem Simplificada de Detecção de Intrusão Baseada em Redes Neurais Artificiais.** Disponível em: <http://www.inf.ufsc.br/~bosco/grupo/MestradoIgor.pdf>. Acesso em: 29 ago. 2014.

MARTINEZ. (sd) **Topologias de Redes**. Disponível em: <http://www.infoescola.com/informatica/topologias-de-redes/>. Acesso em: 01 out. 2014.

MEGGER, Chrystian Luiz. Estudo E Implementação de QoS EM Redes 802.11g SOB Topologia Malha. Universidade Tecnológica Federal do Paraná Programa de Pós-Graduação em Tecnologia Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, 2011. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/399/1/CT_GESER_1_2011_07.pdf. Acesso em: 02 Dez 2015.

MENDES, Douglas Rocha. **Redes de Computadores**: Teoria e Prática. São Paulo: Novatec, 2007. Disponível em <http://novatec.com.br/livros/redescom/capitulo9788575221273.pdf>. Acesso em: 28 set. 2014.

MICHEL, Maria Helena. **Metodologia e pesquisa científica em ciências sociais:** Um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos. São Paulo: Atlas, 2005.

MICROSOFT. **Planejando a proteção contra-ataques de inundação de negação de serviço.** Disponível em: <http://technet.microsoft.com/pt-br/library/dd897007.aspx>. Acesso em: 03 nov. 2014.

MORIMOTO, Carlos E. **Guia do hardware:** Bridge. Disponível em: <http://www.hardware.com.br/termos/bridge>. Acesso em: 11 ago. 2015.

_____. **Hardware Manual Completo.** Disponível em: <http://www.hardware.com.br/livros/hardware-manual/placas-rede-1.html>. Acesso em: 11 ago. 2014.

_____. **Iniciantes:** Entendendo os Roteadores Wireless. Disponível em: <http://www.hardware.com.br/artigos/basico-entendendo-rotesdores-wireless/>. Acesso em: 20 nov. 2014.

NÉRIO, Alex; RODRIGUES, Pedro. **Trabalho sobre Redes Sem Fio (Wireless)**. Logic – Engenharia de Sistemas. Salvador, 2003. Disponível em: <http://www.logicengenharia.com.br/mcamara/ALUNOS/Wireless.pdf>. Acesso em: 24 set. 2014.

ONO, Edson Toshiaki. **Implantação de Rede Wireless de Alta Velocidade**. 2004. 108 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2004. Disponível em: <https://projetos.inf.ufsc.br/arquivos_projetos/projeto_119/TCC%20-%20Relat%f3rio%20Final.pdf>. Acesso em: 05 set. 2014.

ORMOND. **Políticas de Segurança de Redes Corporativas.** Disponível em: <http://www.ic.ufmt.br:8080/c/document_library/get_file?p_l_id=58070&folderId=59704&name=DLFE-2171.pdf>. Acesso em: 15 set. 2014.

OUL. **Planos de internet móvel custam a partir de R$ 10; dicas ajudam a escolher.** Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2014/04/03/planos-de-internet-movel-custam-a-partir-de-r-10-saiba-como-escolher.htm>. Acesso em: 7 nov. 2014.

PEREIRA, Felipe Zanatta. **Segurança em Rede Sem Fio**. 2007. 82 f. Relatório do Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Universidade do Planalto Catarinense, Lages, 2007. Disponível em: <http://www.revistauniplac.net/ojs/index.php/tc_si/article/viewFile/796/506>. Acesso em: 02 set. 2014.

PINHEIRO, José Mauricio S. sd**. Topologia de Rede.** Curso de Tecnologia em Redes de Computadores. Disponível em: https://www.projetoderedes.com.br/aulas/ugb_redes_I/ugb_redes_I_material_de_apoio_04.pdf. Acesso em: O3 Dez 2015

PINZON, Alexandre. **Vulnerabilidade da Segurança em Redes Sem Fio**. 2009. 68 f. Trabalho de Conclusão de Curso II (Graduação em Sistemas de Informação) - Centro Universitário Ritter dos Reis, Porto Alegre, 2009. Disponível em: <http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf>. Acesso em: 17 out. 2014.

QUEIROZ, Claudemir da Costa. **Segurança Digital**: um estudo de caso. 2007. 71 f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) - Faculdade Lourenço Filho, Fortaleza, 2007. Disponível em: <http://www.flf.edu.br/revista-flf/monografias-computacao/seguranca_digital.pdf>. Acesso em: 16 out. 2014.

REIS, Gustavo Henrique da Rocha. **Redes sem Fio**. Instituto Federal de Educação, Ciência e Tecnologia. Rio Pomba, 2012. Seção Materiais. Disponível em: <http://sistemas.riopomba.ifsudestemg.edu.br/dcc/materiais/402257390_redes-sem-fio.pdf>. Acesso em: 04 out. 2014.

RIBEIRO, Igor C. G et al. **Segurança em Redes Centradas em Conteúdo**: Vulnerabilidades, Ataques e Contramedidas. Universidade Federal Fluminense. Rio de Janeiro, 2012. Disponível em: <http://www.dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/ceseg:2012-sbseg-mc3.pdf>. Acesso em: 02 out. 2014.

RIBEIRO, Jara Diego; FONTAN, Augusto Felipe. **Segurança em Redes Sem Fio.** Disponível em: <http://felipenegociosinfo.files.wordpress.com/2011/09/tcc-ii-seguranc3a7a-em-redes-sem-fio.pdf>. Acesso em: 19 set. 2014.

RODRIGUES, Pedro Edgar Bessa. **Segurança Informática de Redes e Sistemas (Abordagem Open-Source)**. 2007. 271 f. Dissertação (Mestrado em Engenharia Electrotécnica e de Computadores) - Universidade de Trás-os-Montes e Alto Douro, Portugal, 2007. Disponível: <http://repositorio.utad.pt/bitstream/10348/747/1/MsC_pebrodrigues.pdf>. Acesso em: 14 out. 2014.

SANTOS, Wylliams Barbosa. **Redes de Computadores**. Universidade Federal Rural de Pernambuco. Pernambuco, 2012. Seção Laboratório de Informática. Disponível em <http://200.17.137.109:8081/novobsi/Members/wylliams/laboratorio-de-informatica/2012.1/Aula%205%20-%20Redes%20de%20Computadores.pdf>. Acesso em: 05 out. 2014.

SCHWEITZER. **Tecnologias de Redes Sem Fio:** WPANs, WLANs E WMANs Desafios de Segurança, Vulnerabilidades E Soluções, 2005 Disponível em: <ftp://linorg.cirp.usp.br/pub1/SSI/SSI/SSI2005/Microcursos/MC04.pdf>. Acesso em: 22 out. 2014.

SILVA et al. **Segurança em Redes Sem Fio**: “As Duas Faces da Moeda”. Disponível

em: <http://www.sbpcnet.org.br/livro/63ra/arquivos/jovem/85seguranca.pdf>. Acesso em: 28 out. 2015.

SILVA, Érico José N. e; SOUZA FILHO, Ernani de Araújo de; RODRIGUES, Josiane do C. **Interferência em Redes Wireless Estudo de Caso:** Paragominas. Disponível em: <http://www3.iesampa.edu.br/ojs/index.php/computacao/article/viewFile/130/118>. Acesso em: 20 ago. 2015.

SILVA, Leandro Rodrigues. **Segurança em Redes Sem Fio (Wireless)**. Pontifícia Universidade Católica do Paraná (Pós-Graduação em Redes e Segurança de Sistemas). Curitiba, 2010. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Leandro%20Rodrigues%20Silva%20-%20Artigo.pdf>. Acesso em: 02 out. 2014.

SILVA, Marcel Santos. **Topologia. Fundamentos de Redes.** 2014. Disponível em:<http://marcelsantos.eti.br/wp-content/uploads/2014/02/04-Topologias.pdf>. Acesso em: 04 dez 2015.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de cumputadores das LANs, MANs e WANs às Redes ATM**. 2. ed. Rio de Janeiro: Ed. Campus, 1995.

SOUSA, Lindenberg Barros de. Redes de Computadores: Dados, Voz e Imagem. São Paulo: Editora Érica Ltda, 1999.

TANENBAUM, Andrew S. **Computer Networks**. 4 ed. Amsterdam: Campus, 2003. Disponível em: <http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf>. Acesso em: 27 set. 2015.

TECHTUDO. **Dicas-e-tutoriais:** Redes-WiFi. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/10/como-trocar-o-canal-da-sua-rede-wi-fi-evitando-interferencias.html>. Acesso em: 12 set. 2014.

TEIXEIRA, Iêda Paula de Farias; SILVA, Maria das Graças Maciel. **Segurança em Redes Sem Fio**. 2012. 56 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Universidade Federal de Alagoas, Olho d' Água das Flores - AL, 2012. Disponível em: <http://www.ufal.edu.br/unidadeacademica/ic/graduacao/sistemas-de-informacao/arquivos-monografias/arquivos-2012/seguranca-em-redes-sem-fio>. Acesso em: 29 set. 2014.

THOMAS, Robert M. **Introdução às redes locais**. Rio de Janeiro: Makron Books, 1997.

THOMAS, Tom. **Segurança de redes Primeiros passos.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2007.

TORRES, Gabriel. **Segurança Básica em Redes Sem Fio**. Clube do Hardware, ago. 2009. Seção Tutoriais. Disponível em:

<http://www.clubedohardware.com.br/artigos/Seguranca-Basica-em-Redes-Sem-Fio/963/1>. Acesso em: 07 out. 2014.

VERISSIMO, Fernando. **Segurança em redes sem fio**. Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2002. Disponível em: <http://land.ufrj.br/~verissimo/cos871/bibref/wns5.pdf>. Acesso em: 18 out. 2014.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores**: configuração, manutenção e expansão. São Paulo: Makron Books, 2000.

APÊNDICE (S)

APÊNDICE A - QUESTIONÁRIO DE DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

Data: __/__/__

Fase:_____

Idade:_____ anos

Sexo: ( ) Feminino ( ) Masculino

1 Você sabe o que é uma rede Wireless (Sem Fio)?

( ) Sim ( ) Não

Se você responder "não" vá para questão 16

2 Quem configurou o seu roteador Wi-Fi?

( ) Você ( ) Técnico ( ) Outros (especificar) _____

3 Você já acessou o console do seu roteador?

( ) Sim ( ) Não

4 Você utiliza algum tipo de proteção no seu roteador?

( ) Sim, Qual?_____

( ) Não

( ) Não sei

5 Você utiliza algum software para gerar senha?

( ) Sim, qual? _____ ( ) Não

6 Quantos dispositivos se conectam em sua rede?

( ) 1 ( ) 2 ( ) 3 ( ) Outros (especificar) _____ ( ) Não sei

7 Você sabe quais dispositivos se conectam no seu roteador?

( ) Sim, quais ? _____ ( ) Não

8 Existe alguma restrição de acesso por dispositivo?

( ) Sim, qual ? _____ ( ) Não ( ) Não sei

9 Existe algum tipo de limitação de velocidade para alguns dos dispositivos?

( ) Sim, qual? _____ ( ) Não ( ) Não sei

10 Você tem o costume de trocar senha em quanto tempo?

( ) 1 semana ( ) 1 mês ( ) 1 ano ( ) outros (especificar)_____

( ) Nunca

11 Você tem costume de utilizar senhas complexas?

( ) Sim ( ) Não

12 Existe algum tipo de filtro de conteúdo?

( ) Sim ( ) Não ( ) Não sei

13 Existe algum controle por horário?

( ) Sim ( ) Não ( ) Não sei

14 Você sabe quais serviços estão executando em seu roteador?

( ) Sim, quais?_____ ( ) Não

15 Você acha correto a rede Wireless ser restrita/protegida por motivo de segurança?

( ) Sim ( ) Não

16 Já acessou roteadores Wi-Fi em ambientes públicos (abertos)?

( ) Sim ( ) Não

17 Você sente segurança ao utilizar estes serviços públicos? (Aeroporto, shopping).

( ) Sim, porquê?_____

( ) Não, porquê?_____

18 Quais desses serviços você acha que é inseguro acessar em ambientes públicos? (Pode assinalar mais de uma opção).

( ) Pesquisas profissionais ( ) Downloads de softwares/jogos/MP3/vídeos/filmes

( ) Redes sociais ( ) Serviços bancários ( ) Acessar noticias, jornais, revistas

( ) Fazer compras.

19 Já experimentou acesso em redes sem autorização?

( ) Sim ( ) Não

Grata pela sua atenção!!!

APÊNDICE B – ARTIGO

DIAGNÓSTICO DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS

Maiara Miranda Bardini[1], Rogério Antônio Casagrade[1], Kristian Madeira[1]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense

(UNESC) – Criciúma – SC – Brasil

Maiara_bardini@hotmail.com

Abstract. *This research aims to explore the security of domestic wireless networks through an analysis of the security procedures adopted. It was performed a survey sample with 172 students from the Computer Science Course. Thus, it was noticed that many security flaws in Wi-Fi networks are due to the lack of knowledge or lack of concern of the users. The biggest problem is related to the misconfiguration of the networks and users' indifference to safety, and thus subject to invasions. Thus, when the vulnerabilities in networks were identified, it was proposed a scenario for practical application of minimal security policies to demonstrate the methods used in the experiment.*

Resumo. *Esta pesquisa tem como objetivo explorar a segurança das redes sem fio domésticas, por meio de uma análise dos procedimentos de segurança adotados. Foi realizada uma pesquisa por amostragem com 172 acadêmicos do Curso de Ciência da Computação. Deste modo, notou-se que muitas falhas de segurança nas redes Wi-Fi são devidas ao desconhecimento ou falta de preocupação dos próprios usuários. O grande problema se encontra nas redes mal configuradas, e no desinteresse com a segurança, sendo assim sujeitas a invasões. Assim, ao identificar as vulnerabilidades contidas nas redes, foi proposto um cenário para aplicação prática de uma política de segurança mínima para demostrar os métodos utilizados no experimento.*

1 INTRODUÇÃO

Com a evolução tecnológica a acessibilidade às redes sem fio se tornou um grande avanço em termos de facilidade e rapidez.

Esta expansão tecnológica trouxe para a sociedade moderna a inclusão digital, pois passou a dar mais mobilidade para seus usuários, permitindo que qualquer pessoa a qualquer hora, desde que se tenha um ponto de acesso a Wi-Fi, possa navegar pelo mundo da Internet (FIGUEIREDO; PINHEIRO; MELLO, 2011).

O mundo da tecnologia vem crescendo a cada dia, uma vez que o uso da Internet permitiu um avanço em termos de acessibilidade para toda a população. A facilidade do acesso à Internet é um dos maiores exemplos de expansão tecnológica.

O crescimento acelerado das redes sem fio juntamente com a expansão e a facilidade do acesso mostra-se evidente, pois no mercado atual elas vêm sendo mais divulgadas. Todavia, com esse crescimento surgem diversos problemas quanto à segurança tecnológica (DUARTE, 2010).

Tendo isso em vista, é fundamental conscientizar as pessoas da importância de manter suas redes domésticas seguras, para impedir o fácil acesso às informações e recursos compartilhados na rede (PINZON, 2009).

A prevenção é umas das medidas excelentes, uma vez que é o conjunto mínimo que dificulta a exploração de possíveis falhas no sistema que possam ocorrer bem como a proteção que busca inibir possíveis tentativas de ataques que o sistema pode sofrer (BOF, 2010).

Com isso procurou-se avaliar a utilização de redes sem fio domésticas com vistas às condições de usos e procedimentos de segurança da informação.

2 REDES SEM FIO

As redes sem fio são a passagem de dados entre dois ou mais mecanismos, através de ondas de rádio, portanto essa comunicação é feita sem o uso de cabos. Os sinais como os de televisão ou rádio FM, possuem os procedimentos do mesmo modo que as ondas de rádio são encaminhadas (FERREIRA, 2013).

Os padrões de redes sem fio mais utilizados são: Padrão IEEE 802.11b, Padrão IEEE 802.11a, Padrão IEEE 802.11g, Padrão IEEE 802.11n.

2.1 Criptografias para segurança

Na conexão com a rede sem fio é necessário à utilização de algum protocolo para que ocorra a segurança da mesma. Onde se tem os principais protocolos de segurança: Protocolos Wired Equivalente Privacy (WEP), Protocolos Wi-Fi Protected Access (WPA) e Protocolos Wi-Fi Protected Acess 2 (WPA2).

2.2 Redes sem fio domésticas

A grande maioria da população está utilizando redes sem fio domésticas, devido à facilidade que se tem ao acesso da Internet. Para isso, basta possuir um roteador de redes sem fio que faça conexão com diversos computadores, sendo que cada um deles pode trocar informações entre si (TANENBAUM, 2003).

Existem equipamentos de redes sem fio que são de extrema importância para transmitir sinal entre eles destacamos as Placas de redes sem fio, que são dispositivos que permitem a comunicação de diversos computadores de uma rede (MORIMOTO, 2002).

Access Point (AP) é um roteador para acessar as redes sem fio, ele é quem faz o gerenciamento da comunicação entre os usuários (PINZON, 2009).

Antenas, elas transmitem sinais para todos os lados, são conectadas ao ponto de acesso que permitem conexões à longa distância (ONO, 2004).

2.3 Tipos de redes sem fio domésticas

Os tipos de redes sem fio domésticas são classificados em Local Area Network (LAN) e Wide Area Network (WAN) (NÉRIO; RODRIGUES, 2003).
Os tipos mais comuns de tecnologias de acesso sem fio são: Banda larga móvel, Bluetooth, Infravermelho, Wi-Fi.

3 SEGURANÇA DE REDES SEM FIO

Para dar mais eficiência às redes sem fio é necessário à aplicação de políticas de segurança capazes de barrar possíveis invasores.

As políticas de segurança consistem em normas que determinam se os dados de uma rede possuem segurança ou não. Neste entendimento, referem-se a um sistema de segurança estruturado para a proteção de dados obtidos na rede (SOARES; LEMOS; COLCHER, 1995).

Os Pilares da segurança são constituídos por três pilares: a Confidencialidade, a Integridade de dados e a Disponibilidade (FERREIRA, 2009).

Os endereços MAC são endereços físicos, exclusivos compostos por 12 números hexadecimais, fazendo com que eles sejam reconhecidos na rede. Assim, com filtragem destes endereços é possível que apenas as máquinas com os endereços de MAC cadastrados tenham acesso à rede (BOF, 2010).
Conforme Verissimo (2002) existem quatros tipos de ataques, sendo que os intrusos possuem maneiras diferentes para encaminhar mensagens. Os tipos são: Interrupção, Interceptação, Modificação, Fabricação.

As vulnerabilidades são falhas que ocorrem no sistema quando um programa é mal projetado, deixando-o suscetível às invasões. Caso isso ocorra, tanto os usuários que possuem permissão total do sistema, quanto os que não possuem podem executar alterações, colocando em risco os dados lá armazenados (QUEIROZ, 2007).

As contramedidas examinam as inseguranças de um sistema suscetível a ocorrer invasões, objetivando prevenir que algo malicioso venha a ocorrer (RODRIGUES, 2007).

Existem as ameaças que podem atingir a rede, neste caso serão citadas algumas contramedidas de segurança para as ameaças mais comuns (TECNET, 2004), são elas:

Falsificando o IP/ sequestro de sessão, Ataques de negação de serviço (dos – denial of service), Varredura (scanning), Sniffers (farejadores) e Força Bruta (Brute Force).

4 DESENVOLVIMENTO

Neste trabalho, foram elaborados os estudos sobre segurança em redes sem fio domésticas. Foi aplicado um questionário com 172 usuários. Também foi realizado um experimento para verificar o melhoramento na segurança de redes sem fio domésticas por meio de um cenário de configuração básico.

4.1 Estratégia de pesquisa

Os dados coletados foram analisados por meio do software IBM Statistical Package for the Social Sciencies (SPSS) versão 21.0. As variáveis qualitativas foram

expressas por meio de frequências e porcentagens. A idade foi expressa por meio de média e desvio padrão. As análises inferenciais foram realizadas com um nível de significância α = 0,05 e confiança de 95%. A distribuição da idade quanto à normalidade foi avaliada por meio da aplicação do teste de Shapiro-Wilk. A comparação das médias de idade entre as fases estudadas foi realizada por meio da aplicação do teste H de Kruskal-Wallis seguido post hoc teste de Dunn. A investigação da existência de associação entre as variáveis qualitativas foi avaliada por meio da aplicação do teste qui-quadrado de Peason (FIELD, 2009).

4.2 Caracterização do ambiente da pesquisa

Foram entrevistados acadêmicos do curso de Ciência da Computação da Universidade de Extremo Sul Catarinense – UNESC - Município de Criciúma/SC, regularmente matriculados no segundo semestre do ano de 2015.

Foi entregue um questionário para todos os entrevistados selecionados da 1ª à 9ª fase do curso de Ciência da Computação, a pesquisa foi realizada em sala de aula, onde o pesquisador aplicou o instrumento.

4.3 População e amostra

Foram considerados 307 acadêmicos matriculados, a partir dessa informação foi realizado o cálculo do tamanho mínimo da amostra, por meio da fórmula proposta por Barbetta, Reis e Bornia (2010, p. 193):

$$n_o = \frac{z_\gamma^2 p(1-p)}{E_o^2}$$
$$n_o = \frac{1{,}96^2 \times 0{,}5(1-0{,}1)}{0{,}05^2}$$
$$n_o = 385 \text{ acadêmicos}$$

Em que, “γ” refere-se ao nível de significância adotado, nesse caso, 0,05, “z” é a estatística padrão normal, que para γ =0,05 é 1,96, “P” é à proporção que maximiza o tamanho da amostra, 0,50, “E_0” é o erro amostral máximo tolerável, 0,05, e, “no”, trata-se da primeira aproximação para o tamanho mínimo da amostra, nesse caso 385 entrevistados.

O resultado da primeira aproximação para o cálculo do tamanho mínimo da amostra foi corrigido por meio da fórmula proposta por Barbetta, Reis e Bornia (2010, p.193):

$$n = \frac{N \times n_o}{N + n_o - 1}$$
$$n = \frac{307 \times 385}{307 + 385 - 1}$$
$$n = \frac{118195}{691}$$
$$n \cong 172 \text{ acadêmicos}$$

Em que “N” refere-se ao total de alunos, e “n” é o tamanho mínimo da amostra a ser pesquisada, que resultou em aproximadamente 172 entrevistados.

4.4 Plano de amostragem

Foram entrevistados 15 alunos da primeira fase, 25 alunos da segunda fase, 21 alunos da terceira fase, 20 alunos da quarta fase, 15 alunos da quinta fase, 14 alunos da sexta fase, 10 alunos da sétima fase, 8 alunos da oitava fase e 44 alunos da nona fase. O processo de amostragem foi estratificado proporcionalmente, com amostragem aleatória simples dentro de cada estrato.

4.5 Utensílios de coleta de dados

Para a coleta de dados foi realizado um questionário sobre redes sem fio domésticas, elaborado pelo autor, e seu orientador. O questionário contém 19 perguntas, sendo dez delas descritivas (abertas) e nove de múltipla escolha.

4.6 Resultados obtidos

Foram pesquisados 172 acadêmicos do curso de Ciência da Computação, predominantemente do sexo masculino (n = 154; 89,5%), com média de idade de 22,02 ± 3,73 anos, sendo o aluno mais jovem com 17 anos e o de mais idade com 40 anos.

4.7 Avaliação dos Resultados: Fases x Conhecimento

A grande maioria dos alunos matriculados no curso é do sexo masculino, concentrando-se o maior número de indivíduos do sexo feminino na nona fase (n = 8; 18,2%), sendo que não se observou existência de associação entre gênero e fase (p = 0,524).

Todos os entrevistados afirmaram ter esse conhecimento sobre o que é uma rede Wireless. Embora exista uma tendência de o próprio aluno da quarta fase em diante configurar o seu roteador Wi-Fi, essa relação não se mostrou estatisticamente significativa (p = 0,279). Percebe-se que a maioria dos alunos, já acessou o console do seu roteador (p = 0,138). Embora a maioria dos alunos utilize proteção no seu roteador, essa característica não foi observada na quinta, sétima e oitava fases, onde apenas 20,0% (n = 3), 40,0% (n = 4) e 37,5% (n = 3) respectivamente, utilizavam algum tipo de proteção (p = 0,125). Dos tipos de proteção mais utilizados, os mais frequentes, nas fases avaliadas, foram o WEP, WPA, WPA2 e controle por MAC, não havendo associação estatisticamente significativa (0,096).

Percebeu-se que a maioria dos alunos não utiliza algum tipo de software para gerar senha (p =0,446). Em relação aos tipos de software para gerar senha, essa característica foi observada na sexta fase onde apenas 7,1% (n=1), utiliza software para gerar senha, sendo este, o *LastPass,* não havendo associação estatisticamente significativa (p = 0,183). A respeito de quantos dispositivos se conectam na rede, a pesquisa apresentou que a maioria dos alunos tem em média três dispositivos conectados (p = 0,218).

Quando questionados se eles sabem quais dispositivos se conectam no seu roteador, a maioria dos alunos afirmou ter esse conhecimento (p = 0,429). Em relação aos tipos de dispositivos que se conectam no roteador, foi observado que os dispositivos menos utilizados pelos usuários foram Smartphone (p=0,637), SmartTv (p=0,617), Tablet (p=0,057), iPad (p= 0,603), Xbox (p=0,015). Dos tipos de

dispositivos mais utilizados e conectados no roteador, foram notebook, celular e computador (p = 0,05).

Existe alguma restrição por acesso ao dispositivo, observou-se nos alunos da sétima e oitava fase (p=0,002). Dos tipos de restrição, observou-se que em todas as fases, a mais utilizada é restrição por senha. Quando questionados se sabem se possuem algum tipo de limitação de velocidade para alguns dos dispositivos, foi observado que na primeira, quinta a oitava fases os alunos não sabem (p=0,107). Foram observadas limitações quanto à velocidade de download, controle de banda, no entanto, esses foram relatos isolados (p = 0,856). O período mais frequente observado para troca de senhas foi o de 1 ano (p = 0,088).

Sobre a utilização de senhas complexas em todas as fases existem alunos que utilizam essa proteção, havendo predominância na nona fase (p=0,242). Já na utilização de filtro de conteúdo, a maioria dos alunos não utiliza essa proteção, sendo o seu uso mais frequente na nona fase (p = 0,003). Não foi observado a existência de controle por horário (p=0,266).

Embora a maioria dos alunos não saiba quais serviços estão executando em seu roteador, foi observado na quarta, sexta, sétima e nona fases, onde apenas 20,0% (n = 4), 14,3% (n=2), 10,0%(n=1), 11,4% (n=5) respectivamente, sabem quais são estes serviços (p=0,079). Dos tipos de proteção mais utilizados, os mais frequentes, nas fases avaliadas, foram o DNS (p=0,128) e DHCP (p=0,038).

Quando questionados se acham correto a rede wireless ser restrita /protegida por motivo de segurança, a grande maioria afirmou que acha correto (p=0,339). Em todas as fases a maioria dos alunos afirmaram ter acessado a Wi-Fi em ambientes públicos (p=0,363).

Quanto a utilização de serviços públicos, a maioria dos alunos da segunda a quarta, sétima e nona fase não se sentem seguros (p = 0,059), principalmente pelo fato de a rede ser desprotegida (p = 0,033). Os alunos que sentem-se seguros em acessar esse tipo de serviço, somente utilizam serviços básicos ou nunca tiveram problemas (p = 0,014).

Quando questionados quais desses serviços são inseguros acessar em ambientes públicos, em todas as fases a maioria afirmaram insegurança em serviços bancários (p=0,010), redes sociais (p=0,001), e compras (p=0,000). Quando perguntado aos alunos se eles já utilizaram redes sem autorização, a maioria já fez este tipo de acesso (p=0,332).

4.8 Avaliação dos Resultados: Cruzamento

Para realizar o cruzamento de perguntas, foi escolhida a questão Q3 do questionário, sendo ela, relacionada com as questões Q7, Q8, Q9, Q10, Q12, Q13 e Q14, porque para utilizar esses tipos de proteções, controlar os dispositivos na rede entre outras funções, precisa-se já ter acessado o console do roteador.

Constatou-se que a maioria dos alunos sabem quais dispositivos estão conectados em seu roteador, isso é porque já acessaram o console do roteador (p=0,005). Os tipos de dispositivos mais utilizados foram notebook (p=0,008) celular (p=0,011) e computador (p=0,003).

Em todas as fases dos que afirmaram existir algum tipo de restrição por dispositivo, provavelmente tinham conhecimento por já terem acessado o console de seu roteador ou o técnico tenha informado (p=0,025), Dos tipos de restrição, as mais utilizadas via acesso ao console do roteador para a proteção de suas redes domésticas, foram senha e controle por Mac (p=0,392). E também sobre tipo de

limitação de velocidade por dispositivos, poucos alunos afirmaram ter em sua rede doméstica (p=0,001). Dos tipos de limitação, os citados na pesquisa foram velocidade de download e controle de banda (p=0,480).

Dos entrevistados que afirmaram ter costume de trocar senha periodicamente, ocorre essa troca devido já ter acessado via console do seu roteador para fazer essas alterações (p=0,533). Dos tempos de troca de senha em todas as fases, os mais utilizados foram 1 mês, 6 meses e 1 ano. Embora na utilização de filtro de conteúdo, a maioria dos alunos não utiliza esse tipo de proteção (p= 0,001), só poderá ser feita, via console do roteador. Sobre algum tipo de controle por horário, todos os alunos afirmaram não fazer uso desta proteção, talvez não seja só por não ter acessado o console do seu roteador (p=0,376).

Contatou-se que a grande maioria dos entrevistados não sabe quais serviços estão executando em seu roteador, mas para saber precisa ter feito o acesso via console do roteador, assim terá como acessar as demais funções do roteador. Dos tipos de serviços que rodam no roteador, em todas as fases avaliadas, foram DNS (p=0,126) e DHCP (p=0,216).

4.9 Aplicação prática de uma política de segurança mínima

Foi aplicado um cenário de segurança de redes sem fio domésticas, demostrado o mínimo de procedimentos para proteção de uma rede. No cenário foram utilizados os respectivos equipamentos: um roteador TP-LINK, 150Mbps wireless Lite N Router, modelo NO. TLWR741N / TL-WR741ND. Um notebook Sony Vaio, processador Intel (R) Core (TM) I3 CPU M380 @ 2,53 GHz, sistema operacional de 64 bits, Windows 7, memória instalada (RAM) 4.00 GB.

Para acesso à configuração do roteador foi inserido o endereço de IP no navegador, de forma a obter acesso à interface de configuração, conforme a opção Network – Lan da configuração do roteador, o IP Address vem como padrão de fábrica, para a segurança dessa rede foi mudado esse endereço.

Às vezes ocorrem interferências de canais de redes Wi-Fi, por isso, aparece o baixo sinal, impedindo o acesso à Internet, isso pode acontecer porque a rede possui o mesmo canal de um roteador próximo ou também pode ser que este canal seja igual ao das redes próximas. Para melhorar o sinal da rede Wi-Fi, é de utilizar, por exemplo, um programa para fazer uma varredura dos canais utilizados e escolher um disponível (BRITO, 2013).

Ao desabilitar a opção Enable SSID Broadcast a rede ficará oculta a todos, e o roteador não transmitirá o nome da rede no ar. Foi utilizado uma criptografia de segurança, conforme na opção Wireless Security, WPA-PSK/WPA2-PSK, após selecionar esta versão para proteção da rede, nela utiliza-se a chave de segurança AES.

Para identificar os intrusos conectados à rede, na opção DHCP List, a mesma exibe quantos endereços de IP estão conectados ao roteador, se acaso além dos usuários confiáveis tenha mais endereços, mostrará a relação de usuários conectados a rede. Então conforme a opção Wireless MAC Filtering, selecionando a opção Deny, o intruso conectado a rede será bloqueado e mesmo que ele tenha a senha para acesso, o intruso não se conectará novamente a rede, nela mostrará falha ao conectar-se, isso só ocorrerá se a opção Wireless MAC filtering estiver habilitada.

Mais um controle do que uma segurança com a opção Parental controle settings, a mesma terá um limite de acesso a determinadas páginas na Internet não

confiáveis, e também no Advance schedule settings é designado para possuir o controle de horário do usuário, após cumprir esse horário a rede será desligada.

5 CONCLUSÃO

Neste trabalho, foi possível verificar que a utilização das redes sem fio domésticas, ainda trazem muita insegurança. Isso porque ao longo de todas as análises colhidas, observou-se que muitos usuários do curso de Ciência da Computação não possuem conhecimento adequado ou não demonstram importância acerca destes procedimentos.

A pesquisa demonstrou que a maioria dos procedimentos básicos de segurança não são utilizados corretamente, mesmo usuários de fases avançadas não possuem os mínimos cuidados com a segurança de sua rede. Mas é importante destacar que o que preocupa os usuários é acesso a ambientes públicos, mas em casa não demonstram preocupação, sem saber dos riscos que podem estar correndo, de modo que se possuir algum usuário com conhecimentos básicos sobre redes, poderá ter acesso aos dados.

Nesse sentido, de acordo com toda a pesquisa realizada, a recomendação à aplicação de uma política de segurança para evitar problemas na rede.

Após os resultados da pesquisa, foi realizado um experimento a fim de demostrar os métodos mínimos de segurança a serem aplicados nas redes sem fio domésticas.

Com pesquisas futuras pode ser aprofundada quanto à aplicação das políticas de segurança das redes sem fio domésticas, dando continuidade na análise de outros grupos e contramedidas estratégicas, uma vez que com avanço da tecnologia estas sempre podem ser aprimoradas.

Referências

BARBETTA, Pedro Alberto; REIS, Marcelo Menezes; BORNIA, Antônio Cezar. **Estatística para Cursos de Engenharia e Informática**. 3 ed. São Paulo: Atlas, 2010.

BOF, Edson. **Segurança em redes wireless**. 2010. 58 f. Monografia (Especialista em Gestão da Segurança da Informação) - Faculdade do Centro Leste, Serra, 2010. Disponível em: <http://br.monografias.com/trabalhos-pdf/seguranca-redes-wireless/seguranca-redes-wireless.pdf>. Acesso em: 22 set. 2015.

DUARTE, Carlos Anderson Andrade. **A Evolução dos Protocolos de Segurança das Redes Sem Fio: do Wep ao Wpa2 passando pelo Wpa**. 2010. 51 f. Monografia (Especialista em Redes de Computadores) – Pós-Graduação em Redes de Computadores da Escola Superior Aberta do Brasil. Vila Velha, 2010. Disponível em: <http://www.esab.edu.br/arquivos/monografias/carlos-anderson-andrade-duarte.pdf>. Acesso em: 08 out. 2014

FERREIRA, Érico José. **Segurança de Redes de Computadores**. UNIERO Centro Universitário. Brasília, 2009. Disponível em: <http://www.ericonet.com.br/admin/material/Seguranca_de_Redes_de_Computadores.pdf>. Acesso em: 10 set. 2014.

FERREIRA. **Diferentes tipos de Rede Wireless.** Disponível em:

<http://www.oficinadanet.com.br/post/11081-rede-wireless>. Acesso em: 10 ago. 2014.

FIELD, Andy P. **Discovering statistics using SPSS**. Los Angeles, 2009.

MENDES, Douglas Rocha. **Redes de Computadores**: Teoria e Prática. São Paulo: Novatec, 2007. Disponível em <http://novatec.com.br/livros/redescom/capitulo9788575221273.pdf>. Acesso em: 28 set. 2014.

MICROSOFT. **Planejando a proteção contra-ataques de inundação de negação de serviço.** Disponível em: <http://technet.microsoft.com/pt-br/library/dd897007.aspx>. Acesso em: 03 nov. 2014.

MORIMOTO Carlos E. **Hardware Manual Completo.** Disponível em: <http://www.hardware.com.br/livros/hardware-manual/placas-rede-1.html>. Acesso em: 11 ago. 2014.

NÉRIO, Alex; RODRIGUES, Pedro. **Trabalho sobre Redes Sem Fio (Wireless)**. Logic – Engenharia de Sistemas. Salvador, 2003. Disponível em: <http://www.logicengenharia.com.br/mcamara/ALUNOS/Wireless.pdf>. Acesso em: 24 set. 2014.

ONO, Edson Toshiaki. **Implantação de Rede Wireless de Alta Velocidade**. 2004. 108 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2004. Disponível em: <https://projetos.inf.ufsc.br/arquivos_projetos/projeto_119/TCC%20-%20Relat%f3rio%20Final.pdf>. Acesso em: 5 set. 2014.

PINZON, Alexandre. **Vulnerabilidade da Segurança em Redes Sem Fio**. 2009. 68 f. Trabalho de Conclusão de Curso II (Graduação em Sistemas de Informação) - Centro Universitário Ritter dos Reis, Porto Alegre, 2009. Disponível em: <http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf>. Acesso em: 17 out. 2014.

QUEIROZ, Claudemir da Costa. **Segurança Digital**: um estudo de caso. 2007. 71 f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Faculdade Lourenço Filho, Fortaleza, 2007. Disponível em: <http://www.flf.edu.br/revista-flf/monografias-computacao/seguranca_digital.pdf>. Acesso em: 16 out. 2014.

RODRIGUES, Pedro Edgar Bessa. **Segurança Informática de Redes e Sistemas (Abordagem Open-Source)**. 2007. 271 f. Dissertação (Mestrado em Engenharia Electrotécnica e de Computadores) - Universidade de Trás-os-Montes e Alto Douro, Portugal, 2007. Disponível: <http://repositorio.utad.pt/bitstream/10348/747/1/MsC_pebrodrigues.pdf>. Acesso em: 14 out. 2014.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de cumputadores das LANs, MANs e WANs às Redes ATM**. 2. ed. Rio de Janeiro: Ed. Campus, 1995.

TANENBAUM, Andrew S. Computer Networks. 4 ed. Amsterdam: Campus, 2003. Disponível em: <http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf>. Acesso em: 27 set. 2015.

TECHTUDO. **Dicas-e-tutoriais:** Redes-WiFi. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/10/como-trocar-o-canal-da-sua-rede-wi-fi-evitando-interferencias.html>. Acesso em: 12 set. 2014.

VERISSIMO, Fernando. **Segurança em redes sem fio**. Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2002. Disponível em: <http://land.ufrj.br/~verissimo/cos871/bibref/wns5.pdf>. Acesso em: 18 out. 2014.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores**: configuração, manutenção e expansão. São Paulo: Makron Books, 2000.