**CENTRO UNIVERSITÁRIO METROPOLITANO DE SÃO PAULO**

**CURSO ADMINISTRAÇÃO DE EMPRESAS**

**SEGURANÇA DE REDE WIRELESS**

**CAETANO RAFACHO**

**Guarulhos**

**Novembro - 2014**

**CAETANO RAFACHO**

**SEGURANÇA DE REDE WIRELESS**

**Trabalho de Conclusão de Curso apresentado como exigência para a obtenção do grau de Bacharel em Administração de Empresas do Curso de Administração do Centro Universitário Metropolitano de São Paulo.**

**Orientador(a): Prof.(a): Paulo José L. Folgueral**

**CENTRO UNIVERSITÁRIO METROPOLITANO DE SÃO PAULO**

**GUARULHOS – 2014**

**CAETANO RAFACHO**

**SEGURANÇA DE REDE WIRELESS**

**Guarulhos,\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_de 2014.**

**Nota\_\_\_,\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Prof. Paulo J. L. Folgueral - Orientador**

**Centro Universitário Metropolitano de São Paulo**

**DEDICATÓRIA**

Dedico este trabalho, primeiramente à Deus, que foi minha fonte de energia, a minha mãe, Dra Sirlei Aparecida Gramari que está sempre ao meu lado mesmo quando estou errado em decisões, as minhas irmãs Cláudia Leite a Fábia Adriana Rafacho que me apoiam e sempre me ajudam em diversas situações, à minha filha Luíza Helena R. Rafacho, onde busco minha força para continuar, aos meus amigos e colegas. Sem todos nada eu seria.

**AGRADECIMENTOS**

Primeiramente agradeço à Deus pela oportunidade enquanto muitos não a tem, ao Professor Paulo Folgueral que acreditou e depositou em mim a confiança e me orientou nesse trabalho, ao Professor Paulo Leandro Maia que também me orientou com muita paciência no início do trabalho e me acompanhou junto ao Professor Paulo Folgueral. Aos amigos de trabalho Remo Almeida e Luíz Alberto de Mello que me ajudaram com informações aqui utilizadas. Aos amigos: Cristiano, Rafael e Fernando da turma da sala 630, que me incentivaram e apoiaram.

**RESUMO**

As redes atuam em computadores, periféricos e em linha de produção, reduzindo processos, diminuindo tempo e melhorando o operacional das empresas.

Sua história iniciou-se no anos 1960 quando a telefonia dominava o mundo, onde me 1961, cientistas começaram estudos sobre o compartilhamento de informações.

A primeira rede foi conhecida como ARPAnet e apresentada apenas em 1972 na Conferencia Internacional de Computadores.

A ARPAnet foi utilizada na Guerra Fria, era usada pelos Estados Unidos para comunicação militar. Após a Guerra, ela foi entregue as universidades transformando-se no fenômeno conhecido hoje por Internet.

A rede Wireless, passou a existir graças a invenção do rádio, que em sua tradução significa comunicação sem fim, tendo seu maior trunfo em 1901, quando o físico italiano Gugliano Marcone Marchesi, conseguiu emitir sinais de rádio de um continente ao outro pelo Oceano Atlântico.

É preciso entender a rede Wireless, é bem mais vulnerável que outras redes devido ao fato de funcionar sem fio, porém são diversos os sistemas de segurança para proteger a rede das ameaças de invasões, onde, com estudos profundos, a Cisco Systens, tem seu próprio protocolo de segurança e a Wi-Fi Alliance desenvolveu o WPA liberando a vários empresas à produção desse sistema de segurança.

**PALAVRAS CHAVE: Redes, Compartilhamento e Segurança**

**ABSTRACT**

The networks operate on computers, peripherals and production line, reducing processes, reducing time and improving the operating businesses.

His story began at 60 when the phone ruled the world, where I 1961 scientists began studies on information sharing.

The first network was known as ARPAnet and presented only in 1972 at the International Conference on Computers.

The ARPAnet was used in the Cold War, it was used by the United States for military communication. After the war, she was delivered universities becoming known today by the Internet phenomenon.

Wireless network came into being thanks to the invention of the radio, which in translation means your communication worm, having its greatest asset in 1901, when the Italian physicist Gugliano Marcone Marchesi, could emit radio signals from one continent to another by Ocean Atlantic.

You need to understand the wireless network, is more vulnerable than other systems due to the fact operate wirelessly, but there are various security systems to protect the network from threats of invasion, where, with deep studies, Cisco Systens has its own security protocol and the Wi-Fi Alliance developed WPA releasing several production companies this security system.

**KEYWORDS: Networks, Information sharing and Security.**

**EPÍGRAFE**

Nunca a comunicação sem fio esteve tão presente na vida do usuário final como atualmente. Seja através do acesso à Internet via celular, seja na transmissão de infravermelho e periféricos. (FILIPPETTI, 2011, p 71)

**LISTA DE FIGURAS**

**Figura 01:** Ilustração da Rede de Computadores.....................................................................11

**Figura 02:** Ilustração de várias redes em uma empresa...........................................................12

**Figura 03:** Hardware, peças físicas internas de um computador.............................................13

**Figura 04:** Softwares, programas operacionais........................................................................14

**Figura 05:** Primeiro computador..............................................................................................15

**Figura 06:** Logotipo ARPAnet.................................................................................................16

**Figura 07:** Ilustração à uma chave ou senha de rede...............................................................17

**Figura 08:** Ilustração à emissão do sinal Wireless...................................................................21

**Figura 09:** Vulnerabilidades e Soluções..................................................................................23

**Figura 10:** Roteador Cisco 2801..............................................................................................27

**Figura 11:** Patch Panel.............................................................................................................27

**Figura 12:** Switch Cisco 2960C...............................................................................................28

**Figura 13:** Aparelho telefônico Cisco IP 7942G.....................................................................29

**SUMÁRIO**

[INTRODUÇÃO 11](#_Toc398705438)

[CAPÍTULO I 12](#_Toc398705439)

[1. REDES DE COMPUTADORES 12](#_Toc398705440)

[1.1 Conceito de rede 12](#_Toc398705441)

[1.2 Definição de rede 13](#_Toc398705442)

[1.2.1 Hardware 13](#_Toc398705443)

[1.2.2 Software 14](#_Toc398705444)

[1.3 História das redes 15](#_Toc398705445)

[1.4 Segurança de redes 18](#_Toc398705446)

[CAPÍTULO II 20](#_Toc398705447)

[2. WIRELESS 20](#_Toc398705448)

[2.1 Conceito 20](#_Toc398705449)

[2.2 Definição 20](#_Toc398705450)

[2.3 A história da rede wireless 21](#_Toc398705451)

[2.4 Segurança de rede wireless 22](#_Toc398705452)

[2.5 Padrões de segurança wireless 24](#_Toc398705453)

[2.5.1 WEP 24](#_Toc398705454)

[2.5.2 Cisco Interim Solutiom 24](#_Toc398705455)

[2.5.3 WI-FI Protected Access (WPA) 25](#_Toc398705456)

[2.5.4 IEEE 802.11i e WPA-2 25](#_Toc398705457)

[3. ESTUDO DE CASO 26](#_Toc398705458)

[CONCLUSÃO 31](#_Toc398705459)

[BIBLIOGRAFIA 32](#_Toc398705460)

[APÊNDICE 33](#_Toc398705461)

**INTRODUÇÃO**

Nunca a tecnologia esteve tão presente na vida das pessoas como hoje. Atualmente, até uma criança de sete anos ou menos consegue acessar à Rede Internet.

Na maioria dos casos, com a pressão diária das empresas e em meio trabalhos domésticos, cada vez menor se torna o tempo das pessoas para resolverem seus problemas particulares ou de trabalho.

A presente pesquisa, foi embasada em uma questão fundamental envolvendo esse tema:

- É seguro resolver os problemas pela rede sem fim, ou seja, é seguro pagamento de contas ou compras pela Internet através do celular, notebook ou qualquer outro periférico lançando seus dados à nuvem externa sem qualquer ligação física?

Vários são os recursos para manter a rede segura, seja residencial ou corporativa. Porém, deve-se seguir os aconselhamentos e requisitos dos fabricantes desses recursos para evitar que invasores tragam inconveniências, se não, toda a rede estará comprometida.

O objetivo desse trabalho científico é trazer conhecimento sobre as redes, redes sem fio, demonstrar os mecanismos usados para proteger uma rede própria e como operá-los, por exemplo com senhas, que devem ser trocadas periodicamente para manter a proteção do usuário.

A justificativa, refere-se justamente à segurança que se tem ao liberar senhas e dados pessoais para compras, pagamentos e outras operações sem precisar sair de seu ambiente pela rede sem fio ou até mesmo em deslocamento. Não apenas nesse ponto, mas na rotina de empresas que envolvem operações financeiras, informações confidenciais de Recursos Humanos, Propaganda e Marketing, operações comuns das empresas que cada vez mais, estão eliminando o cabeamento e aderindo a rede sem fio.

No capítulo I, apresenta-se o conceito, definição, história e segurança de rede cabeada de computadores, pois antes de atingir a rede sem fio, um pouco deve-se entender sobre Redes.

No capítulo II, apresenta-se o conceito, definição, história, segurança e padrões de segurança das redes sem fio, e alguns cuidados valiosos para proteger a rede.

No capítulo III, foi pesquisado em uma empresa como se monte uma rede de wireless segura, com os cuidados devidos contra a invasão de hackers.

# CAPÍTULO I

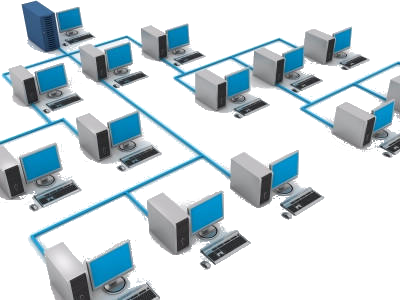
# 1. REDES DE COMPUTADORES

Formada por um conjunto de módulos processadores capazes de trocar informações e partilhar recursos, interligados por um sistema de comunicações, com o objetivo de troca de dados e partilha de recursos de hardware e software.

## 1.1 CONCEITO DE REDE

O conceito de rede basea-se em um grupo de computadores em pleno funcionamento em que independe de outros, permitindo compartilhamento de informações, softwares, arquivos, etc.

Figura 1: Ilustração de uma rede de computadores



**Fonte:www.mitodasredes.blogspot**

Podem atuar em computadores, periféricos e em linha de produção, reduzindo os custos, minimizando processos, economizando tempo e melhorando o desempenho operacional de uma empresa.

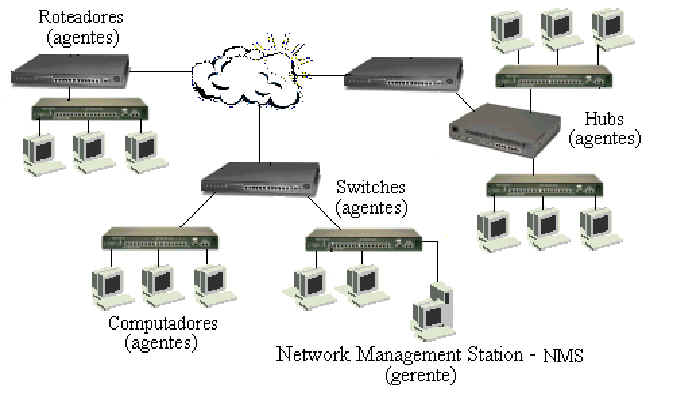
Quando um computador se conecta à uma rede, ele passa a ter informações presentes em outros computadores conectados na mesma rede, permitindo um número maior de informações possíveis através daquele computador.

## 1.2 DEFINIÇÃO DE REDE

Uma rede consiste em dois ou mais computadores conectados entre si para compartilhar serviços como:

* Dados;
* Mensagens por e-mail;
* Impressoras.

Figura 2: Ilustração de várias redes na mesma empresa



**Fonte: www.ti-iseg-t12.wikidot.com/g4**

Muitas redes são conectadas pela rede mundial de computadores, a Internet, onde existem vários recursos e formas de equipamentos que podem ser compartilhados ou interligados, através de protocolos, requisitos de segurança e meios de acesso.

Existem basicamente dois tipos de rede conhecidos:

* Rede Lan: são chamadas Local Área Networks ou locais, interligando os computadores no mesmo espaço físico, normal em uma empresa ou até mesmo em residências;
* Rede WLan: Rede local onde se elimina todo cabeamento, hoje normal em residências, empresas ou locais públicos.

Seu funcionamento depende de um determinado conjunto de meios físicos conhecidos por hardware e componentes de software.

### 1.2.1 Hardware

Quando falamos em hardware, uma rede precisa ter:

1. Computadores periféricos , impressoras, modens, fax, etc...
2. Cabeamento que façam a interligação dos computadores.
3. Placas de interface de rede, modens ou outros dispositivos que fazem a ligação dos computadores à rede.

Figura 3: Hardware, peças físicas internas de um computador



**Fonte: www.ti-iseg-t12.wikidot.com/g1**

**1.2.2 Software**

Ao falarmos em softwares, são necessários:

1. Drives de rede, que são peças de softwares que se unem ao sistema de operações do computador para que este se comunique com a interface da rede;
2. Protocolos, que são normas em software que tornam possíveis a transmissão entre computadores envolvidos na rede;
3. Sistemas que interligam o sistema;
4. Programas de aplicação para trabalho em rede.

Figura 4: Softwares, programas operacionais



**Fonte: www.infoblacksheep.blogspot.com.br**

## 1.3 HISTÓRIA DAS REDES

Uma rede teve seu início nos anos de 1960, onde a rede de telefonia dominava o mundo, de modo que a voz se transmitia por comutação de circuitos com taxa constante desde a origem até seu destino.

Nesta década, deu-se início o desenvolvimento de microcomputadores de bom desempenho, com menos rigidez de unidade e temperatura, onde conseguiu-se considerável poder computacional em vários locais diferentes, porém faltava um meio de união destes computadores.

Mesmo com alto custo dos computadores, diz-se com o surgimento da multiprogramação, ocorre a necessidade do compartilhamento de informações em diferentes regiões.

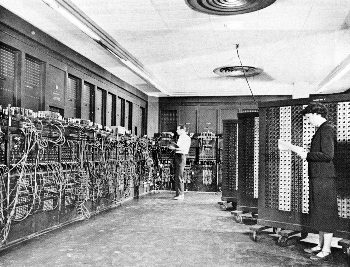
O tráfego de informações gerados pelos usuários ocorriam em sequencia de atividades, onde acionando um comando de longe, esse comando ficaria inativo por alguns instantes aguardando uma resposta.

Três grupos de pesquisa começaram os estudos sobre como transformas a ligação de circuitos para ligação por pacotes, sendo o primeiro em 1961, no laboratório MIT, Leonard Kleinrock usou a teoria em filas, ou seja, a ligação de pacotes baseado em tráfegos em rajadas.

Em 1964 no Rond Institute, Paul Baran estudou a ligação de pacotes para a segurança da transmissão de voz para redes militares.

Em paralelo, no National Physical Laboratory na Inglaterra, Roger Scontlebury e Donald Davies estudavam as ideias da comutação de pacotes.

Figura 5: Primeiro computador ocupava uma sala inteira, 1936



**Fonte: www.sites.google.com/site/historiasobreossitesdebusca/Historia-da-tecnologia/historia-do-primeiro-computador**

Todos esses trabalhos, juntando-se com Lauwrence Roberts comandavam Do MIT, comandavam um projeto de computadores na Agência de Projetos de Perquisas Avançadas (ARPA), onde cerca de 1967, Robests gerou a percusora da grande rede mundial de computadores – a Internet – sendo uma rede de comutação de pacotes, com o primeiro comutador conhecido como IMPs (Interface Message Processous) ou Processadores de mensagens de Interface, fabricados pela empresa BBN.

Em 1972, já com 15 anos, ARPANET foi apresentada na Conferência Internacional de Computadores por Robert Kalin.

Na década de 1970, outras redes surgiram como comutações de pacotes:

* ALOHANET: Rede de microondas que interligava as ilhas do Hawaii.
* TELENET: Pacotes comerciais da BBN;
* TAYMNET e TRANSPIC: Rede de comutação francesa.

Cresciam-se cada vez mais o número de redes com o princípio de rede local, uma ETHERNET, hoje chamadas de Lans.

Devido a Guerra Fria, nos final da década de 1970, cerca de 200 computadores estavam ligados à ARPANET devido à comunicação militar, onde todas as mensagens passagem por um computador central no Pentágono, onde após a Guerra Fria, sem valor, a ARPANET foi passada à Universidade e outros pesquisadores, chegando ao início da década de 1980 com mais de 100 mil computadores interligados, formando a rede mundial de computadores – Internet – onde transferia-se arquivos e os email´s eram processados pela rede de bits.

Em janeiro de 1983, surgiu o primeiro backbone, o NSFNET, que fornecia acesso a outros centros computacionais. Nessa mesma época, surgiu o nome de Domínio no Sistema, que transformava endereços em palavras, na forma de endereço IP de 32 bits, para fácil memorização.

A ARPANET deixou de existir na década de 1990, e a MILNET e a Rede de Dados de Defesa contratavam grande parte do tráfego do Departamento de Defesa dos Estados Unidos e a NFSNET passou a ser o backbone entre os Estados Unidos e todas as redes do exterior, porém em 1995, perdeu seu valor comercial, transferindo a tarefa à provedores da Internet.

De 1989 até 1991, foram desenvolvidas as primeiras versões de HTML, HTTP, Serviços Web e Browser.

Figura 6: Logotipo ARPAnet



**Fonte: www.elon.edu/e-web/predictions/150/1960.xhtml**

Em 1990, o Brasil criou a Rede Nacional de Pesquisas (RNP). Em 1992 criou-se a Internet Society, já com 200 servidores Web operando, onde as pesquisas voltavam-se ao desenvolvimento de Browsers.

Entre os anos de 1993 e 1994, a Embratel passou a disponibilizar o acesso à rede às empresas e usuários particulares ao Netscape e Mosaic. Os estudantes usavam todos os dias esses dois Browsers para navegar na Web e as empresas para transações comerciais.

No ano de 1996, a Microsoft emplacou na Web o Internet Explorer, avançando a cada dia pesquisas por roteadores de alta velocidade para redes locais e recursos como comércio eletrônico, textos, imagens, multimídias e outros.

Após 1996, surgiram as redes INTRANET, sendo redes locais ligadas à Internet, utilizada por empresas em comunicação com suas filiais.

Ainda hoje, a grande rede continua com os protocolos criados no fim da década de 1970, sendo eles: TCP, IP e UDP, logicamente que aperfeiçoados.

Atualmente, mais de 1 bilhão de pessoas acessam a rede mundial em computadores e celulares cada vez mais modernos para todas as suas atividades diárias.

A rede mundial não para de crescer, porém os recursos úteis permanecem com blog´s, chats, vídeos, etc.

## 1.4 SEGURANÇA DE REDES

Segundo a ISSO (Internatinal Standardization Organization), toda rede possui fraquezas, que podem ser exploradas e violar seus sistemas de informações.

Figura 7: Ilustração à uma chave ou senha de rede de vários logoritmos



**Fonte: www.segurancaiesb.blogspot.com.br/2013/07/serie-e-bom-saber-da-dicas-para.html**

Diversas são as ameaças:

* Destruição da informação;
* Deturpação da informação;
* Roubo ou perde de informações;
* Interrupção dos serviços.

Temos também os ataques intencionais:

* Personificação;
* DDOs;
* Replay;
* Modificações;
* Engenharia soci
* Recusa de serviços.

Os mecanismos mais comuns usados hoje, são os Firewall´s, além de políticas de segurança, conjunto de regras, leis e prática visando a proteção:

* Criptografia;
* Assinatura digital;
* Controle de acesso;
* Rótulos de segurança;
* Enchimento de tráfego;
* Controle de roteamento.

Os Firewall´s, são dispositivos que servem de barreiras de proteção, onde podem ser como software ou hardware, ou uma combinação dos dois.

# CAPÍTULO II

# 2. WIRELESS

Wireless em sua tradução, significa comunicação sem fio, ou rede sem fio, onde utilizamos uma rede de computadores sem uso de cabos, tornando cômodo o acesso às redes.

## 2.1 CONCEITO

O funcionamento do Wireless dá-se através de equipamentos que usam radiofrequência, comunicação via ondas ou infravermelho.

A rede Wireless pode ser utilizada para ligar tanto prédio quanto redes internas deles, sendo bastante útil em redes que crescem rapidamente, sendo mais fácil sua expansão, não exigindo cabeamento.

Mas existem suas desvantagens, como os custos, onde os equipamentos agem com a velocidade equiparável a equipamentos com fio.

## 2.2 DEFINIÇÃO

Wireless significa que a informação é transferida por dois ou mais pontos sem conexão física, onde a distância pode ser poucos metros, ou pode variar em milhares ou milhões de quilômetros via rádio do espaço.

Sua aplicação pode ser através de computação móvel, notebook, palmtop, celulares, walkie-talkie e até satélites artificiais.

Seu uso comum, é servindo de meio de acesso à Internet por locais remotos como escritórios, aeroportos, parques, bares, residências, etc...

Porém diversos indivíduos confundem o fato de um local possuir o sistema com acesso livre à Internet, o que na maioria dos locais é necessário introdução de senha.

## 2.3 A HISTÓRIA DA REDE WIRELESS

Sem a descoberta do rádio, o sistema Wireless não existira. É a rede que mais cresceu e expandiu-se de tal forma que podemos fazer qualquer processo por um celular conectado à rede como: pagamentos, transferências de valores, pesquisas, compras, agendamentos, etc...

O físico alemão Heinrich Rudolf Herz, nascido em 1888, produziu a primeira onda de rádio onde seis anos depois, em 1894, tornou-se forma de comunicação.

Herz abriu o caminho para o rádio, TV e com a descoberta das ondas eletromagnéticas, Gugliano Marconi Marchese, italiano, logo em seguida, ampliou o envio das ondas para duas milhas de distância.

Em 1899, Marchese conseguiu ampliar o sinal através do Canal de Bristol (Inglaterra) para 9 milhas, e logo depois para 31 milhas pelo Canal Inglês para a França. E foi em 1901, Marchese conseguiu enviar sinais de rádio atravessando o Oceano Atlântico.

O primeiro grande obstáculo foi a a Segunda Guerra Mundial, onde os Estados Unidos foi o primeiro país a usar ondas de rádio para transmissão de dados e muito possivelmente, poderia ter ganho a Guerra para os americanos.

Um grupo de pesquisadores, liderados por Norman Abranson, da Universidade do Hawaii, em 1971, criou o primeiro pacote de rede de rádio chamado ALOHAnet, composto por sete computadores.

Em 1972, o ALOHAnet conseguiu se conectar com a ARPAnet no continente, tornando-se um sistema inovador no setor das telecomunicações entre computadores.

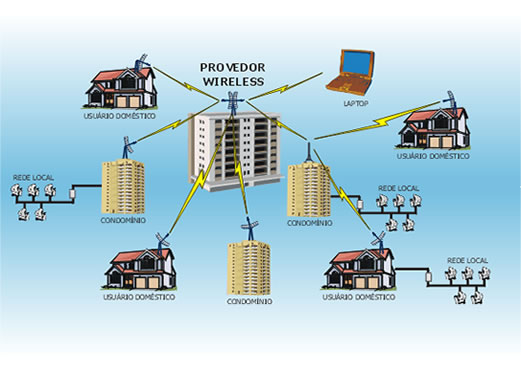
No ano de 1990, criou-se um grupo de trabalho, denominado 802.11, para trabalhar em uma norma sem fio para que os computadores se comuniquem sem fio normatizados.

A norma criada, IEEE 802.11, foi aceita em formato padrão de comunicação de dados para redes.

A tecnologia não para de crescer e atualmente, grandes incorporações e governos estão sempre de olho para padrões mais rápidos.

*O que faz o grande sucesso das redes sem fio é a possibilidade de escalabilidade e mobilidade levando em conta que as informações são enviadas e recebidas no ar, através das ondas de rádio*

Figura 8: Ilustração da emissão do sinal Wireless



**Fonte: www.tecniservice.com.br/26364.html**

## 2.4 SEGURANÇA DE REDE WIRELESS

Deve-se entender que a rede Wireless possui diversas vulnerabilidades não existentes em redes convencionais com fios.

Seu acesso permite o furto de informações, arquivos, senhas ou paradas por exemplo de grandes servidores em grandes empresas, causando prejuízos inimagináveis.

Por esses motivos, deve-se compreender os riscos e medidas disponíveis para implementação preventiva. Algumas ameaças são:

* WAR DRIVERS:

São indivíduos que querem acessar livremente a Internet. Atuam com um notebook e uma antena Wi-Fi em busca de um sinal de AP (Access Point) sem esquema de segurança;

* HACKERS

A ideia desses indivíduos é a obtenção de valiosas informações, e ou, puro terrorismo como por exemplo: derrubar servidores;

* FUNCIONÁRIOS

Podem sim ser uma ameaça, auxiliando o acesso à rede por Hackers não avisando o sistema de segurança sobre a instalação de um AP;

* ROGLE AP

É um AP clonado, onde captura-se frames emitidos pela rede WLAN, obtendo-se informações como chaves de segurança criptografadas. Normalmente descriptografam as chaves e utilizam as informações para configurar o Rogue AP, aparecendo como legítimo no mapeamento da rede.

Para evitar as situações mencionadas, são três as principais ferramentas de segurança de uma rede WLAN:

* AUTENTICAÇÃO MÚTUA

Utilizada entre o usuário e o AP, onde utiliza-se uma chave secreta, devendo ser configurada tanto no usuário como no AP. O AP consegue visualizar se o usuário possui a chave por meio de sofisticados algoritmos. Da mesma forma, o usuário também consegue ver a idoneidade do AP.

* CRIPTOGRAFIA

Esse sistema usa uma chave de um algoritmo para misturar o conteúdo dos frames ou pacotes, e o usuário usa outro algoritmo para colocar as informações em ordem e poder processar.

* FERRAMENTAS ANTIINTRUSÃO

As mais comuns são: *Intrusion Detection Systens* (IDS) e *Intrusion Prevention Systens* (IPS), além de ferramentas específicas de cada fornecedor.

A tabela abaixo mostra suas vulnerabilidades já apresentadas e suas soluções:

:

|  |  |
| --- | --- |
| **VULNERABILIDADE** | **SOLUÇÃO** |
| WAR DRIVERS | MECANISMOS EFICIENTES DE AUTENTICAÇÃO |
| FURTO DE INFORMAÇÕES VIA WLAN | MECANISMOS EFICIENTES DE CRIPTOGRAFIA |
| ACESSO EXTERNO A REDE VIA WLAN | MECANISMOS EFICIENTES DE AUTENTICAÇÃO |
| INSTALAÇÃO NÃO AUTORIZADA DE APS | APLICAÇÃO DE IDS / SWAN |
| AP CLONADO (ROGUE AP) | MECANISMOS EFICIENTES DE AUTENTICAÇÃO, IDS / SWAN |

Fonte: Filippetti, 2011, pág 85

## 2.5 PADRÕES DE SEGURANÇA WIRELESS

Os padrões evoluem conforme o tempo e a demanda por políticas mais rígidas.

O padrão inicial de segurança, conhecido por *Wired Equivalence Privacy* (WEP), e outros três apresentados, mostram a evolução dos padrões criados para corrigir falhas do WEP.

### 2.5.1 WEP

Adotado pelo 802.11, era o padrão original de autenticação e criptografia, facilmante invadido. Seus principais problemas eram:

* STATIC PRESHARED KEYS (PSK)

A chave deveria ser codificada em cada cliente e AP sem intervenção humana. Ninguém se incomodava em trocar as chaves regularmente com os resultados;

* CHAVES FACILMENTE CRACKEADAS

A chave era pequena, de 64bits, e facilitava sua predição. Esse motivo era o fato de raramente se trocar as chaves, facilitava com grande tempo aos invasores.

Foram criadas algumas táticas para tentar reduzir as invasões:

* Bloqueio do broadcast do IP pelo AP, onde os usuários precisam de informações do AP para seu acesso, conhecido por SSID;
* Impedimento do AP enviar sinais por ondas de rádio, conhecido como SSID cloaking;
* Filtragem do endereço MAC, onde o AP tem definido os usuários autorizados ao acesso.

Ambas as técnicas são válidas, mas não impedem um ataque real.

### 2.5.2 Cisco Interim Solutiom

**A** empresa Cisco Systens e outros fabricantes entraram profundamente criando soluções proprietárias devido aos problemas apresentados pelo WEP.

Eis as propostas da Cisco:

* Dymamic Key Exchange (ao invest de chave estática);
* Autenticação 802.1x;
* Pacotes criptografados diferentes.

### 2.5.3 WI-FI Protected Access (WPA)

Após a Cisco criar seu método proprietário de segurança, uma empresa chamada Wi-Fi Alliance, finalizou seu padrão de segurança ao passo que o IEEE trabalhou no padrão 802.11i. O mercado precisava de uma solução rápida, não havia tempo de publicação no padrão IEEE, assim, a Wi-Fi Alliance pegou o padrão 802.11i já criado, fez algumas suposições e criou o padrão “De Fato”, batizado como WPA.

O WPA, traz a mesma solução que a criada pela Cisco, com algumas ressalvas. O WPA incluiu o TKIP para troca dinâmica de chaves. Também incorporou a autenticação 802.1x.

Não há muitas diferenças entre a solução Cisco e WPA, mas a principal é que da Cisco, é proprietária e WPA, pode ser fabricado por outros fabricantes. Os dois não são compatíveis.

### 2.5.4 IEEE 802.11i e WPA-2

Finalmente em 2005, o padrão 80211i foi publicado pelo IEEE.

Segundo as linhas WPA e Cisco, o padrão 80211i, implementa mais rigidez de criptografia, e propicia a troca dinâmica das chaves. Porém, continuam incompatíveis entre si.

Um avanço entre WPA e Cisco foi a inclusão do padrão AES (Advanced Encryption Standart), provendo ainda um método mais seguro de criptografia, com chaves maiores e algoritmos mais robustos.

Salienta-se que nenhuma rede oferece a segurança total, mas existe a possibilidade de torná-la mais segura e menos vulnerável ao ataque de invasores utilizando protocolos de segurança próprios e demais utilizados na rede cabeada.

**CAPITULO III**

# 3. ESTUDO DE CASO

Nesse estudo de caso, foi pesquisado a empresa New Infotel, sendo uma empresa com soluções em TI, nova no mercado mas com experiência. Atua com instalações e soluções em Telecom com presença nos segmentos de Operadoras de Telecomunicações,, Governo, Corporativos e Integradoras de Provedores de Serviços, fornecendo soluções e consultoria.

Hoje em dia, a tecnologia de rede sem fio está ao alcance de todas as pessoas, operadores oferecem o serviço como um valor agregado ao produto de venda.

A operadora que inclusive é utilizada na empresa, oferece um serviço de internet e como valor agregado, disponibiliza um AP (access point) para acesso da rede sem fio na empresa.

Esse AP é utilizado para rede interna, no uso das estações de trabalho, para os notebooks e celulares dos colaboradores e também para convidados que estejam no ambiente da empresa e precisam utilizar a internet.

Normalmente para o acesso de convidados, utiliza-se uma faixa de IP, criando uma SUB-REDE específica para essa rede "Guest", limitando o acesso dos dispositivos para serviços específicos, no caso, somente a internet que se resume ao HTTP ou HTTPS. Isso é feito de uma maneira simples, mas que oferece uma certa blindagem aos dados confidenciais e específicos da empresa. Feito da seguinte forma, a operadora me oferece um IP público para acesso à internet, porém não se pode utilizar esse IP que já vem "subnetado" para somente 1 dispositivo e é necessário traduzir esse IP para compartilhar a rede interna.

Esse compartilhamento de IP pode ser feito de diversas formas, mas a utilizada é com a seguinte topologia:

* Modem 30 megas - Disponibilizado pela operadora, no caso a operadora entrega o sinal e esse sinal é estendido ao roteador da empresa, modelo Cisco 2801. A ligação é feita através de cabo RJ45 em uma porta Ethernet do roteador, que possui 2 portas Ethernet Nativas, no caso utilizo para essa conexão a porta FE0/0).
* ROTEADOR - Do roteador estende-se através de outro cabo RJ45, para um switch Cisco modelo 2960-C de 8 portas utilizando a interface F0/1.

**Figura 10: Roteador Cisco 2801**



FONTE: INTERNET - GOOGLE IMAGENS

* SWITCH - Do Switch estende-se para a rede interna através de um patch panel com as portas espelhadas exatamente como no switch.

Figura 11: Patch Panel



FONTE: INTERNET - GOOGLE IMAGENS

* 1° - A porta f0/1 está o servidor de arquivos - Intel Core I5 3.2 GHZ - 8 GB DDR3 1300 MHZ - Windows 7 Ultimate
* 2° - A porta f0/2 vai um AP modelo Cisco Linksys WRT54G2
* 3° à 5° - Telefones IP Cisco Modelo 7942G
* 6° à 8° - Reservadas e desativadas logicamente.

**Figura 12: Switch 2960C**



FONTE: INTERNET - GOOGLE IMAGENS

São 3 estações de trabalho e 2 impressoras que pertencem à uma VLAN denominada "OPERACIONAL" . Existe também 1 VLAN denominada "SERVIDOR" e uma 1 VLAN denominada "GUEST".

As configurações de VLAN foram realizadas no roteador e também no Switch utilizando "TRUNK" para fazer a amarração das VLANs e o isolamento das informações.

A configuração de IP da VLAN SERVER, além da função TRUNK, foi utilizada "PORT SECURITY", amarrando o MAC Adress da porta de rede do servidor na porta FE0/1 do Switch Cisco, com uma função de desligamento da porta caso seja conectado algum outro dispositivo na porta com um MAC Adress diferente, além de definir um IP fixo no servidor, sendo o primeiro IP válido do range definido no início para o Switch e o último IP válido para o Servidor.

Para a VLAN OPERACIONAL foram configurados também com a função TRUNK, sendo necessário configurar o range de IP que irá disponibilizar, verificando a faixa de IP reservada e também fazendo a correta amarração com a VLAN destinada. As estações de trabalho são configuradas com IP´s fixos na mesma faixa reservada da VLAN "OPERACIONAL" e para fortalecer a segurança, é feito uma amarração com o MAC Adress das 3 estações de trabalho, assim como das impressoras e os telefones IP, para que somente esses endereços consigam autenticar e conectar na VLAN e consequentemente da Rede "OPERACIONAL".

Para a VLAN "GUEST", foi utilizado um mecanismo de DHCP, sendo esses IP´s divulgados através do roteador, com 60 ip´s válidos, sendo utilizados por convidados (clientes e fornecedores) e pelos dispositivos móveis dos colaboradores.

Modem, Roteador, Switch, Servidor e AP, são interligados por cabos Cat5e com padronização de conectorização EIA/TIA 568A para todos os cabos. Apesar do manual de boas práticas exigir um cabo cross para ligação entre roteador e switch, os dispositivos mais novos dispõem de tecnologia MDIX, que automaticamente garante a compatibilidade de cabos CROSS/Straight. Todas as conexões cabeadas estão com "Port Security" com amarração de IP´s e MAC Adress para garantir que somente os dispositivos conhecidos sejam capazes de se conectar à Rede Internet.

A conexão entre os 3 telefones IP´s também são ligados através de cabos Cat 5e com o mesmo padrão de conectorização 568A.

Figura 13: Aparelho telefônico Cisco 7942G



FONTE: INTERNET - GOOGLE IMAGENS

A conexão das redes "OPERACIONAL" e "GUEST", são efetuadas por Wireless.

Rede "Guest" - O AP faz a divulgação da Rede com o SSID "NEWINFOTEL - CONVIDADOS", com uma senha "newinfotel...". Essa rede tem acesso somente à internet, com acesso irrestrito aos sites externos, desde que sigam as políticas de segurança da empresa que é divulgado através de uma página que é carregada no início da conexão do usuário.

A rede Guest tem 60 Ip´s válidos e é efetuada uma mudança da senha normalmente a cada semana, com a senha impressa na recepção para que os usuários possam acessar e para evitar que usuários externos fiquem com acesso por muito tempo, tornando a rede lenta. Há

uma configuração de largura de Banda, que limita o tráfego em 5 MB para a VLAN "GUEST", consequentemente para os dispositivos de convidados, que normalmente só precisam de um acesso temporário a e-mails e sites da internet. É necessário uma configuração de DHCP no roteador para que seja possível a navegação dessa rede.

No roteador, além das configurações de VLAN, telefonia (QoS de VOZ), DHCP e de balanceamento de carga, algumas ACL´s para garantir que nenhuma VLAN consiga acesso à outra, para proteção dos dados. Devido ao tamanho da empresa ser pequena, não foi necessário nenhuma outra ferramenta de Firewall (Cisco ASA) ou VPN para acesso remoto aos dados da empresa, que se resumem a planilhas, que podem facilmente ser armazenadas na casa dos Gigabytes em um servidor. Quando é necessário um acesso, é feito diretamente no Servidor, além do acesso remoto através das VLAN´s, feito com auxílio de Group Polices e softwares de criptografia.

No Switch, é necessário também a configuração de ACL`s, Trunk´s e principalmente de Port Security para garantir a segurança da rede.

A Rede "OPERACIONAL" também é feita através do AP, com o SSID "NEWINFOTEL - OPERACIONAL", porém foi desativado a divulgação da rede no AP. Essa configuração que deve ser feita diretamente para que o AP não divulgue a rede, dificultando a visualização e prevenindo ataques externos. Foi feito a fixação dos IP´s, amarrando aos IP´s dos dispositivos dessa rede, estações de trabalho, telefones e impressoras. Mesmo que seja descoberta, além de ter que passar pelo filtro do IP, terá que dar um "Match" no MAC Adress de cada dispositivo.

As políticas de segurança da empresa são bem simples, sendo alertado e divulgado à todos os funcionários verbalmente e através de documento via e-mail que é proibido a visualização de sites com conteúdo pornográfico e que não sejam condizentes com a moral e bons costumes. Pede-se evitar sites desconhecidos, para que não haja infecção por vírus e também evitar redes sociais em horário de trabalho quando há detrimento com os trabalhos desempenhados no ambiente de trabalho.

Há também uma recomendação no que se refere ao uso de Pen drives e HD´s móveis.

Além disso, os equipamentos são periodicamente atualizados e softwares Anti-vírus sempre com as últimas releases para manter o ambiente livre de falhas e invasões.

# CONCLUSÃO

Baseando-se na pesquisa bibliográfica e de campo, respondo ao problema de invasões nas redes de forma que diversos especialistas trabalham incansavelmente em pesquisas para que a rede se torne mais segura possível.

Baseando-se na pesquisa bibliográfica e de campo, satisfaço a hipótese em que se implantando todos os cuidados recomendados por fabricantes, podemos manter nossa rede segura, como por exemplo, rodando periodicamente o anti-vírus instalado e mudando senhas, se não, diversas são as vulnerabilidades com maiores prejuízos em redes domésticas, pois em corporativos, profissionais trabalham dia e noite para manter a rede segura de ataques.

No mundo de hoje, a tecnologia toma conta da sociedade e surgem diariamente novas tecnologias e dispositivos de segurança, porém os invasores também acompanham esse mercado e a sociedade terá que conviver ainda um bom tempo com essas situações, pois quando falamos em equipamentos, sempre existem falhas e nada é 100% confiável.

**BIBLIOGRAFIA**

**MAIA,** P. L**. O abc da Metodologia, métodos e técnicas para elaborar trabalhos científicos (ABNT)** 3 ed. São Paulo: Leud, 2011.

**SOUSA,** L. B. **Redes, transmissão de dados, voz e imagem.** São Paulo: Érica, 1996.

**FOROUZAN,** B. A. **Comunicação de Dados e Redes de Computadores.** 4 ed. Porto Alegre: AMGH, 2008.

**FILIPPETTI,** M. A. **CCNA 4.1, Guia Completo de Estudo.** Florianópolis: Visual Books, 2011.

**Disponível em http://**[www.lifestyles.com.br](http://www.lifestyles.com.br) **acesso em 25/02/2014.**

**Disponível em http://**[www.significados.com.br](http://www.significados.com.br) **acesso em 10/03/2014.**

**Disponível em http://**[www.urs.inf.ufsm.br](http://www.urs.inf.ufsm.br) **acesso em 17/03/2014.**

**Disponível em http://**[www.tecniservice.com.br/26364.html](http://www.tecniservice.com.br/26364.html)**acesso em 25/03/2014.**

**Disponível em http://**[www.segurancaiesb.blogspot.com.br/2013/07/serie-e-bom-saber-da-dicas-para.html](http://www.segurancaiesb.blogspot.com.br/2013/07/serie-e-bom-saber-da-dicas-para.html) **acesso em 10/04/2014.**

**Disponível em http://**[www.mitodasredes.blospot](http://www.mitodasredes.blospot) **acesso em 20/04/2014.**

**Disponível em http://**[www.ti-iseg-t12.wikidot.com/g4](http://www.ti-iseg-t12.wikidot.com/g4) **acesso em 02/05/2014.**

**Disponível em http://**[www.ti-iseg-t12.wikidot.com/g1](http://www.ti-iseg-t12.wikidot.com/g1) **acesso em 04/05/2014.**

**Disponível em http://**[www.infoblacksheep.blogspot.com.br](http://www.infoblacksheep.blogspot.com.br) **acesso em 27/05/2014.**

**Disponível em http://**[www.sites.google.com/site/historiasobreositedebusca/Historia-da-tecnologia-/historia-do-primeiro-computador](http://www.sites.google.com/site/historiasobreositedebusca/Historia-da-tecnologia-/historia-do-primeiro-computador) **acesso em 10/08/2014.**

**Disponível em http://**[www.elon/edu/e-web/predictions/150/1960.xhtml](http://www.elon/edu/e-web/predictions/150/1960.xhtml) **acesso em 20/08/2014.**

# APÊNDICE

# APÊNDICE 1: ENTREVISTA REALIZADA EM CAMPO

Esta entrevista tem a finalidade de mostrar como pensa e como age um profissional e empreendedor de uma empresa do ramo de TI.

Com certificação CCNA, fornecido pela empresa Cisco Systens, o Sr Luiz Alberto de Melo, mostrou com propriedade seu conhecimento e aplicação na área.

Proprietário da empresa New Infotel, me recebeu com enorme educação e simpatia, abrindo as portas de sua empresa para uma conversa e mostrou passo a passo como monstar uma rede Wireless segura.

Ele também é analista e consultor técnico na empresa Stell Solutions, onde coordena uma equipe técnica em infraestrutura de Telecom.

**COMO VOCÊ DEFINE A SEGURANÇA DE REDE WIRELESS ATUALMENTE?**

Em constante evolução, sendo necessário sempre estar atualizado às novas tecnologias com os fabricantes de hardware e software para manter sua empresa segura e principalmente propagar aos clientes as boas práticas para manter sua rede segura. Na maior parte das vezes, boas práticas de segurança como senhas robustas são suficientes para a maioria dos usuários. Alguns protocolos de segurança e algumas práticas também ajudam, mas depende bastante de como será sua rede, uma segurança de uma rede corporativa é um pouco diferente de uma rede doméstica.

**QUAL A DIFERENÇA ENTRE UMA REDE DOMÉSTICA E UMA REDE CORPORATIVA?**

Uma rede doméstica são utilizados como premissas de segurança uma senha robusta, composta de letras, números e caracteres especiais, bem como a diferenciação entre maiúsculas e minúsculas e para uma rede corporativa, além das citadas anteriormente, a chance de ataques é maior devido aos dados que trafegam na rede. Acessando uma rede doméstica, o máximo que a pessoa irá conseguir, será uma internet grátis, e para uma rede corporativa, os dados que estão em jogos tem muito mais valor, uma informação roubada pode valer muito dependendo da intenção do invasor.

**VOCÊ PODE ESPECIFICAR ESSAS DIFERENÇAS DE HARDWARE E SOFTWARE DE CITOU?**

De Hardware quando a empresa faz uso de algum Firewall físico, como por exemplo a linha ASA da Cisco, ou faz uso de algum servidor para essa função e no caso de software, me refiro a antivírus e firewalls como por exemplo Avast que tem função de antivírus e Internet Security. Estando com atualizações em dia, diminui bastante a chance de invasão.

**A TV E A MÍDIA EM GERAL, HOJE PROPAGA DIVERSOS TIPOS DE SITUAÇÕES. SERÁ QUE O INVESTIMENTO NESSE TIPO DE INFORMAÇÃO, NO QUE SE REFERE A SEGURANÇA DE INFORMAÇÃO, NÃO IRIA MELHORAR A SEGURANÇA, CONSEQUENTEMENTE AOS ATAQUES VIRTUAIS?**

Nesse caso, acho que há uma divulgação no acesso aos sites seguros, aos sites confiáveis, mas o que acontece, é que ataques virtuais, fraudes digitais acaba sendo outro tema, já que a educação digital do usuário no que se refere a navegação precisa sempre ser alertada à exaustão, porém as operadoras quando vendem o serviço de internet, não priorizam esse alerta aos usuários, apenas vendendo o serviço e instalando os equipamentos com técnicos às vezes sem essa prioridade de segurança, instalando o modem e AP no cliente, e após o teste de funcionamento, deixam o cliente às vezes sem a devida segurança nos dados, instalando com pouca segurança deixando os dados do usuários fragilizado aos ataques externos.

**É POSSÍVEL IDENTIFICAR SE UMA INVASÃO VEM ATRAVÉS DE UMA REDE FÍSICA, OU SEJA DE UM LOCAL FÍSICO, OU DE UM LOCAL SEM FIO, OU SEJA, UM NOTEBOOK POR EXEMPLO?**

Sim, há softwares específicos em que você monitora as tentativas de ataque e há empresas que deixam o invasor acessar um primeiro nível para contra atacar e identificar a origem do hacker. Um exemplo de software que faz essa varredura é o Wireshark e o Nmap. São ferramentas que identificam IP´s, portas de acesso e diversas outras informações. Vale lembrar que são ferramentas complexas para identificar e normalmente você "enxerga" esses dados de uma maneira muito técnica, sendo necessário ter um bom conhecimento sobre TCP/IP e entendimento de Camada OSI.

**FALANDO EM EDUCAÇÃO DIGITAL, VOCÊ NÃO ACHA QUE ESSE TIPO DE DIRECIONAMENTO, COMO INVASÃO,, SABENDO-SE DESDE O INÍCIO COMO SE EXECUTA, NÃO SERIA MAIS FÁCIL COMBATER, ISSO FALANDO DE PESSOAS LEIGAS, EM CURSOS COMPUTACIONAIS?**

A premissa da inclusão digital, é que seja uma coisa simples, ao alcance de todos. A expectativa também é que todos os técnicos que fazem a implantação dos serviços, sejam especializados, ao menos familiarizados com as boas práticas de mercado para deixar o usuário menos exposto. Não acho que cursos especializados seja a solução para isso, infelizmente, não podemos ser reféns de piratas virtuais e as leis precisam ser revistas para que todos possam navegar com segurança. Usando uma analogia meio torpe, seria como se todas as pessoas tivessem que andar armadas para garantir a segurança, o direito constitucional de ir e vir, mas como existem ladrões de todas os tipos, poderemos a qualquer momento ter que disparar para poder andar livremente, então não acho que seja necessário especialistas em todas as casas para garantir o acesso, e sim leis que garantam e oprimam esses piratas. Talvez com o novo Marco Civil da Internet, seja o primeiro passo para essa educação digital.

**QUAL O PERFIL DESSES PIRATAS?**

Não sei se houve ou se há algum estudo em andamento, não sei nem se existe uma estatística desses piratas virtuais, mas creio que são pessoas bem inteligentes que buscam brechas para enriquecimento, às vezes para autopromoção e às vezes até os chamados White Hats, que são Hackers, ou especialistas em TI que acham brechas e divulgam para os fabricantes para que melhores seus produtos e melhorem a experiência do usuário.

Mas na maioria das vezes, são mesmo ladrões ou golpistas que buscam enriquecimento através de vulnerabilidades dos usuários.

**VOCÊ JÁ INVADIU ALGUMA REDE?**

Não, nunca tive esse conhecimento todo, nunca foi meu foco. Claro que a curiosidade já foi grande, para ver como seria, mas sei que há diversos níveis de invasão. Invadir ou conseguir uma senha de rede Wireless é bem diferente do acesso aos dados, isso chega em outro nível de compartilhamento de arquivos e permissões. O que a maioria das pessoas acham, que quando você "invade" alguma rede, você tem acesso irrestrito à tela do invadido, o que na verdade não é bem assim, uma invasão desse nível é muito complexo. Há softwares de acesso remoto, que você realmente tem o acesso ao micro do usuário, porém normalmente há uma série de dispositivos de segurança para essa conexão.

**A SEGURANÇA DE REDE WIRELESS É SEGURA?**

Sim, é segura. Há diversos profissionais que trabalham para garantir que nosso acesso seja seguro. Confio plenamente no sistema de rede, sabendo que há brechas e não podemos ficar reféns de piratas virtuais. A Informática que eu aprendi a muito tempo atrás, seria um termo de Informação Automática está para ser utilizado e não há como não usufruir disso, mais uma vez, não posso ficar refém de piratas, tenho que pensar positivamente que ela é segura, desde que haja de forma segura também. Mais uma vez, minhas analogias, há lugares para se caminhar tranquilamente e há bairros que não são recomendados, a premissa é a mesma com a internet, há sites e sites, se andar em locais conhecidos, a chance de dar problema é mínima.

**FORNECERIA SEU CÓDIGO DE CARTÃO DE CRÉDITOS OU FARIA ALGUMA TRANSAÇÃO BANCÁRIA DE ALTO VALOR SABENDO DOS RISCOS?**

Há sempre uma premissa de segurança, verificar se o site é seguro, se há certificado digital na página, entre outras coisas e faço compras pela internet desde que foi possível. Celular para acesso bancário e pagamento de contas através de dispositivos móveis também não vejo problemas, sou grande fã dessas facilidades e compro sem medo, desde que em sites confiáveis.

**O QUE VOCÊ ESPERA DA TECNOLOGIA DE REDE WIRELESS PARA O FUTURO, ISSO FALANDO QUE O FUTURO EM TI JÁ É DAQUI A ALGUNS MINUTOS COM CONSTANTES MUDANÇAS E CRESCIMENTO?**

Eu espero que essa inclusão digital seja cada vez mais constante, que cada vez mais e mais brasileiros de regiões isoladas tenham acesso à internet. A Rede Wireless é o maior rompedor de barreiras, já que alcança longas distâncias, com uma Antena e uma boa largura de banda, é possível abastecer um bairro inteiro como acontece em vários países do mundo. O investimento é necessário e também a infra estrutura para isso é necessário. A segurança da informação cresce na mesma medida em que cresce o número de usuários e estamos todos trabalhando para que o acesso seja seguro para todos.