INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS
CAMPUS MANAUS DISTRITO INDUSTRIAL

EDVANDERSON PEREIRA VIEIRA

TECNOLOGIA WIRELESS: REDE LOCAL DE ACESSO SEM FIO

Manaus
2023

EDVANDERSON PEREIRA VIEIRA

TECNOLOGIA WIRELESS: REDE LOCAL DE ACESSO SEM FIO

Monografia apresentada ao curso de graduação em Sistemas de Telecomunicações do Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, como requisito para obtenção do Título de Tecnólogo em Sistemas de Telecomunicações.

Orientador: Prof. Esp. Celso Souza Cordeiro.

Manaus
2023

Dados Internacionais de Catalogação na Publicação (CIP)

V658t Vieira, Edvanderson Pereira.

Tecnologia wireless: rede local de acesso sem fio. / Edvanderson Pereira Vieira. – Manaus, 2023.
43f. : il. color.

TCC (Tecnologia em Sistema de Telecomunicações) – Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, *Campus* Manaus Distrito Industrial, 2023.
Orientador: Prof. Esp. Celso Souza Cordeiro.

1. Tecnologia wireless. 2. Rede local. 3. Acesso sem fio. I. Cordeiro, Celso Souza (Orient.) II. Instituto Federal de Educação, Ciência e Tecnologia do Amazonas. III. Título.

CDD 621.382

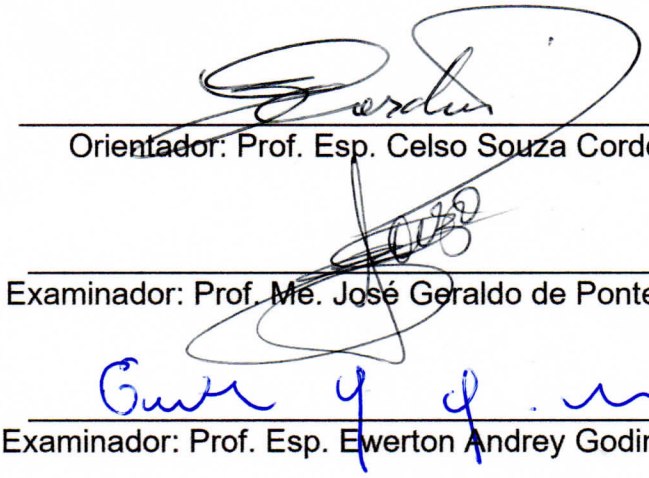
Elabora por Fcª. Amélia Frota, registro n.858 (CRB11)

EDVANDERSON PEREIRA VIEIRA

TECNOLOGIA WIRELESS LOCAL AREA NETWORK: REDE LOCAL DE ACESSO SEM FIO

Monografia apresentada ao curso de graduação em Sistemas de Telecomunicações do Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, como requisito para obtenção do Título de Tecnólogo em Sistemas de Telecomunicações.

Aprovada em: 09 / 03 / 2023, por:



Orientador: Prof. Esp. Celso Souza Cordeiro

1º Examinador: Prof. Me. José Geraldo de Pontes e Souza

2º Examinador: Prof. Esp. Ewerton Andrey Godinho Ribeiro

Manaus
2023

Minha Família,

Mãe Nelcy, fonte de toda a razão.

Esposa Alberniza, fonte de toda compreensão.

Filho Samuel, fonte de toda força.

Eu daria tudo o que tenho para mantê-los seguros das armadilhas deste mundo.

A única razão das minhas lutas é deixá-los seguros e felizes, além de deixar boas lembranças e poder ensinar algo de bom para as novas gerações.

AGRADECIMENTOS

Agradeço a DEUS, por ter me escolhido mesmo sabendo que eu falharia por muitas vezes, e que faria coisas que o entristeceria. Mas ainda assim, Ele não desistiu e confiou em mim. “Alguém que tinha tudo para não dar certo. Mas Deus disse é possível e aqui estou”. Foram 10 anos de UEA sem formar, e agora mais 7 anos de luta no IFAM onde finalmente consigo ir até o fim provando que é possível, mesmo com todas as dificuldades. (idade, família cedo, trabalho e estudos simultaneamente).

Ao meu professor e mestre orientador, Profª. Esp. Celso Cordeiro, pela disponibilidade, colaboração, conhecimentos transmitidos e capacidade de estímulo ao longo de todo o trabalho.

Aos colegas de graduação de Tecnologia em Sistemas de Telecomunicações e demais cursos com os quais pude compartilhar conhecimentos cursando disciplinas em comum e pela alegria da convivência, solidariedade e amizade.

Aos professores, funcionários e alunos do Instituto de Educação Federal Tecnológica do Amazonas, pelo incentivo e estímulo.

Aos coordenadores do curso pelo constante suporte e puxões de orelha para fechamento das disciplinas dentro do período

À minha família, pelo apoio incondicional ao longo desses anos.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.

Marthin Luther King

RESUMO

A tecnologia Wireless Local Área Network (Rede Local de Acesso sem Fio), conhecida como WLAN, permite que usuários estabeleçam conexões sem fio em uma área local. Sua principal característica é a vantagem do custo benefício, por ser de fácil instalação e de custo menos elevado. As WLAN têm a mesma funcionalidade das LANs (redes cabeadas), porém, as redes sem fio eliminam a necessidade de cabos e de outros equipamentos de rede.
Entre os dispositivos utilizados nas redes sem fio, estão computadores de mesa, computadores portáteis, assistentes digitais pessoais (PDAs), pagers e telefones celulares, entre outros. Esses equipamentos móveis permitem uma série de aplicações. Com tanta comodidade e redução nos custos de implantação.

Palavras-chave: Tecnologia wireless; Rede local; Acesso sem fio.

ABSTRACT

Wireless Local Area Network technology, known as WLAN, allows users to establish wireless connections in a local area. Its main characteristic is the cost-benefit advantage, as it is easy to install and has a lower cost. WLANs have the same functionality as LANs (wired networks), however, wireless networks eliminate the need for cables and other networking equipment. Among the devices used in wireless networks are desktop computers, portable computers, personal digital assistants (PDAs), pagers and cell phones, among others. These mobile devices allow a series of applications. With so much convenience and reduction in implantation costs.

Keywords: Wireless technology; Local network; Wireless access.

LISTA DE SIGLAS

DHCP - Dynamic Host Configuration Protocol

ESS – Estended Service Set

EUA – Estados Unidos da América

ICMP - Internet Control Message Protocol

IEEE - Institute of Eletrical and Eletronic Engineers

NELA - National Electric Light Association

VoIP – Voice over Internet Protocol

WEP - Wired Equivalency Privacy

WLAN - Wireless Local Area Network

WMAN – Wireless Metropolitan Area Network

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Este trabalho foi idealizado pela pesquisa do uso, implementação e vantagens das redes wireless (acesso sem fio) assim como na definição do assunto e dos principais tópicos relacionados a essa rede. O uso da tecnologia wireless rede sem fio, caminha entre transceptores de rádio indo até o uso em satélites no espaço sideral, usados com mais frequência em redes de computadores e dispositivos moveis, utilizado como forma de acessar a internet, usando-se em restaurantes, aeroportos, consultórios ou na própria casa (BUSCH, 2018).

As redes sem fio ou wireless, teve seu início da mesma forma que muitas outras tecnologias, no âmbito militar. Naquela época os militares tiveram a necessidade de criar um método simples e protegido para realizar a troca informações no campo de batalha.

Segundo Farias (2015), com o passar do tempo a tecnologia evoluiu, partindo do âmbito militar para se tornar acessível as empresas, universidades e até mesmo ao usuário doméstico.

De acordo com o mesmo autor na atualidade pode-se refletir em redes Wireless como uma opção bastante inovadora em relação às redes cabeadas. Suas aplicabilidades são variadas e tem como principal característica sua locomobilidade, fato que a torna mais aceita nos ambientes corporativos.

Atualmente os usuários começaram a notar as vulnerabilidades da segurança no uso de dispositivos e computadores com acesso sem fio. O uso dessa tecnologia wireless redes sem fio para os usuários tornou-se prático e necessário, se tornando um grande facilitador diário. Entretanto, essa tecnologia trafega diversos tipos de informações em seus dados, sejam elas restritas ou não, e usando de forma errada essa tecnologia, essas informações podem expor os dados dos usuários e causar danos irreversíveis aos mesmos (CANCELA, GUIMARÃES et al,.2018).

O uso das redes sem fio está se multiplicando cada vez mais à medida que a qualidade das mesmas vai melhorando e os preços dos equipamentos vão se tornando mais acessíveis (SYMANTEC, 2013).

O uso deste tipo de tecnologia vai desde a transceptores de rádio até satélites. Sendo o uso mais popular é em redes de computadores, atendendo como meio de acesso à Internet por locais longínquos (BUSCH, 2018).

1.1 FORMULAÇÃO DO PROBLEMA

As redes sem fio ou wireless se iniciaram nos anos 90 a partir de sinais de rádio frequência, e desde então foi evoluindo gradativamente, no entanto sua segurança não foi progredida, havendo assim a necessidade em cuidados dos usuários para suprir esse problema, hoje à informação é muito importante tendo em vista os acessos a links e programas desconhecidos que o dispositivo ao acessar está repleto de informações pessoais como mensagem, fotos, documentos e dentre outros (CANCELA, GUIMARÃES et al,.2018).

Uma rede cabeada com computadores interligados por meio de fios, é necessário mudanças físicas, obras e arrumações. Os problemas estruturais do local como a alteração de layout de móveis, salas, divisórias e salões de reunião. E cabos aparentes espalhados por todo local.

Ao expandir novos pontos de rede emergenciais ou simplesmente ampliar a rede de forma a acomodar os funcionários, onde quer que eles estejam, os fios novamente atrapalham. Havendo a necessidade de alocar/disponibilizar um ambiente de informática para um projeto de curta duração, onde colocá-los sem alterar na estrutura física e cabos (BANDIVIDTH, 2010)..

1.2 JUSTIFICATIVA

A importância deste tema está no interesse de usuários e empresas terem demonstrado dificuldades quanto a esse assunto em implantar, manter e/ou ampliar redes cabeadas tomando assim as redes wireless sem fio muito mais viável.

Para Cancela & Guimarães et al (2018), na atualidade, existe uma grande quantidade de computadores conectados à rede de internet mundial sendo a maioria deles dispositivos moveis onde buscam a utilização de serviços online para suprir as necessidades, onde se trafegam várias informações sigilosas da vida de cada usuário, seja de redes sociais, mensagens de texto, pesquisas na internet.

Destaca-se que, em uma empresa, a informação pode valer até mais do que a própria infraestrutura dessa". Isso se destaca principalmente em redes sem fio ou até mesmo cabeadas lotadas em empresas e corporações que se pode ver atualmente.

1.3 MOTIVAÇÃO

A conectividade da rede é feita de forma rápida, fácil e a custos acessíveis, com acesso seguro e altamente funcional para qualquer tamanho de empresa, escritório e residências, tanto para novos prédios como para lugares temporários. Possibilitando constantes mudanças de layout e um ambiente tecnologicamente moderno e visualmente atrativo.

1.4 OBJETIVOS

Demonstrar a importância da tecnologia wireless área network assim como auxiliar nos processos referentes a implementação/migração do wireless rede local de acesso sem fio. E como objetivo específico: demonstrar de forma simples e objetiva as vantagens em utilizar a tecnologia wireless sem a necessidade de cabos interligando computadores.

1.5 METODOLOGIA

A metodologia utilizada para efetivação deste trabalho se deu por meio de pesquisa bibliográfica incluindo livros, artigos científicos, revista eletrônicas. Sendo uma pesquisa qualitativa, buscando adquirir conhecimento para se associar aos conceitos pesquisados.

1.6 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em 4 capítulos. No primeiro, trata-se da introdução que é o início de todo trabalho. Mostrando os itens formulação do problema, justificativa, motivação, objetivos, metodologia utilizada para o levantamento de dados e organização do trabalho. No capítulo 1 demonstra o referencial teórico sendo cada tópico referente ao tema. No terceiro capítulo foi apresentado os materiais e métodos alguns equipamentos mais comuns utilizados em redes wireless. No quarto capítulo encontra-se os resultados e discussões, seguido dos trabalhos futuros e conclusão.

2 REFERENCIAL TEÓRICO

2.1 TECNOLOGIA WIRELESS

A tecnologia wireless utiliza ondas de rádio para transmissão de dados entre dispositivos, e envolve uma série de descobertas e avanços científicos que foram sido desenvolvidos, onde o resultado final é uma rede de comunicações global e uma grande malha de redes disponíveis em variados espaços públicos, empresas, e residências no mundo e no Brasil (CHENG & MARSIC, 2012).

As versões sobre a tecnologia wireless, é que busca enfatizar uma visão dessa tecnologia e o que o seu conceito apresenta. O início mais enfocado por livros e cursos é o envio de códigos Morse por Marconi em 1901, mas vários outros marcos são utilizados, como a descoberta da indução eletromagnética por Faraday em 1831 e a demonstração pública de Tesla em 1893, e podem ser citados como sendo início dessa tecnologia, portanto estaremos traçando uma linha do tempo, com uma análise posterior de onde o início do wireless poderia ser posicionado (DOWNEY, 2009).

Nessa contextualização histórica, segue alguns nomes importantes que deram sua contribuição para tecnologia wireless como: Michael Faraday em 1831, descobre os princípios da indução eletromagnética. Joseph Henry em 1842, descobre que uma faísca elétrica entre dois condutores pode ser utilizada para induzir magnetismo entre agulhas, esse efeito é detectado a uma distância de 30 metros. Feddersen em 1858, descobre o caráter oscilatório das faíscas elétricas (JACOBSON, 2012).

James Clarck Maxwell em 1867, desenvolve sua teoria do eletromagnetismo e prediz a existência de ondas elétricas no éter. Von Bezold em 1870, descobre a interferência com descargas de compensadores. Thomas Edison em 1875, nota um fenômeno que denominou “força etérica”, mas abandonou a ideia quando Elihu Thompson, dentre outros, criticaram (BOLOT, 2013).

David E. Hughes em 1879, descobre que um tubo de arquivamentos férreos fica condutivo por ação à distância através de faíscas elétricas, ele faz um sinal audível em um fone em uma distância de 500 metros, mas parou suas experiências, pois Sir George Stokes julgou que os acontecimentos demonstravam indução simples. Graham Bell e William H. Preece em 1882, transmitem sinais de Telégrafo Wireless através do mar por meios de indução, entre a Inglaterra e a Ilha Wight. Heinrich Rudolph Hertz em 1887, professor privado em Kiel, descobre que o

efeito de faíscas elétricas está baseado nos fenômenos das ondas no éter. Ele confirmou a teoria de Maxwell, onde as ondas viajam pela mesma velocidade de luz. Branly em 1890 chama a atenção às propriedades de tubos com arquivamentos férreos que foram redescobertos e desenvolve o primeiro coherer para detectar ondas de rádio (CARTER & CORVELA, 2016).

Preece em 1892, sinaliza no canal de Bristol com seu sistema de indução. Tesla em 1893, demonstra publicamente a comunicação wireless via rádio em St. Louis, descrevendo em detalhes os princípios da comunicação via rádio (LAI & BAKER, 2019).

Ledge em 1894 repete os testes de Herz com um coherer. Tesla em 1895 encontra sinais de recebimento das telegrafias de seu laboratório em Nova Iorque em West Point, Marconi transmite o primeiro telégrafo, e Popoff constrói um receptor para ondas elétricas naturais onde tenta descobrir temporais (PAXSON, 2017).

Marconi em 1896, demonstra a telegrafia wireless ao escritório de telégrafo inglês, após um ano testando na Itália. Ele prova as possibilidades de telegrafia sem fios com um coherer. Marconi em 1897, adquire a patente do telégrafo wireless e estabelece a primeira "Estação Marconi" em Needles (Ilha Wight), esta estação envia um sinal à costa inglesa a mais de 22 km (PAXSON, 2018).

Needles em 1898, é enviado a primeira telegrafia wireless paga, e em 20 julho, a primeira mensagem de jornal é enviada de um navio para o Daily Express sobre os resultados de uma competição de navegação. 1901 – Marconi usa sintonia entre os receptores e transmissores, e em 12 e 13 dezembro, primeiro sinais são enviados pelo Oceano Atlântico de Poldhu para New Foundland (2800 km) (LAKSHMINARAYANAN et al 2015).

Marconi em 1902, desenvolve o detector magnético, e há a primeira comunicação bidirecional através do Atlântico. Schlömilch em 1903, desenvolve o detector eletrolítico, Poulsen descobre a transmissão de ondas contínuas com um arco elétrico, e surge o primeiro serviço de notícias para navios em mar, o "Serviço Marconi" wireless de Londres para o "Handelsblad" holandês (ASYMMETRIC, 2015).

(...) Em 1971 a primeira rede wireless, a Alohanet, na Universidade do Hawaii. a ponto de obscurecer a trajetória de vários desses notáveis pesquisadores em detrimento da aplicação comercial por Marconi, que foi importante, mas de forma alguma a única.

O prêmio Nobel da física de 1909 e a patente foram conferidas à Marconi, porém a descoberta do rádio ocorreu no mesmo ano que um russo, Popoff, fazia experimentos para a detecção de tempestades utilizando a mesma tecnologia, e há um impasse sobre a descoberta, mesmo sendo universalmente aceita como sendo dos EUA (POSTEL, 2011).

Além disso, em 1983, Tesla demonstrara publicamente uma transmissão via rádio. Devido esses fatos, e ao do governo dos EUA não desejar pagar pela utilização das patentes de Marconi na Primeira Guerra Mundial, em 1943 a patente foi transferida para Tesla, poucos anos após sua morte.

Vários livros e cursos apresentam uma história bem descrita no final da linha do tempo, mas pobre em seu início, e falham em descrever como a comunicação wireless começou. Pode-se ver que as comunicações wireless datam de bem antes da primeira rede, a Alohanet, ter sido formada, ou da primeira comunicação via celular, que aconteceu em 1946 pela NTT do Japão (LINHARES, 2017).

Partindo da definição de wireless, que é a de dados se propagando via ondas de rádio, as descobertas e testes de transmissão via indução não podem ser considerados, e as teorias sobre o a aplicação do rádio não podem ser utilizadas, até terem sua aplicação confirmada para o fim proposto no significado. Assim, partimos direto para a utilização das ondas de rádio (BOLAND, 2014).

A aplicação de Tesla em 1983, no Franklin Institute of Philadelphia e no National Electric Light Association, continha todos os elementos antes da invenção da válvula de osciloscópio. Tesla foi o primeiro a aplicar o mecanismo da condução elétrica para finalidades wireless. Ele utilizou receptores eletromagnéticos, que eram versões anteriores dos cohereres utilizados por Marconi em tempos mais recentes. Após essa demonstração, os princípios da comunicação via rádio ficaram comprovados e amplamente conhecidos (FARIAS, 2015).

As redes sem fio, segundo Engst & Fleishman (2015), iniciou-se de um projeto que ligou as universidades do Havaí em 1971, que conectavam os computadores de quatro ilhas. Elas entraram para o uso da computação pessoal em 1980, quando a ideia de compartilhar dados entre computadores começava a se tornar popular.

As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade no início dos anos 90, quando os processadores se tornaram mais rápidos a ponto de suportar tal aplicação. As redes existentes na época eram patenteadas e

incompatíveis, por isso, no meio da década de 90 as atenções se voltaram para o novo modelo do IEEE (*Institute of Eletrical and Eletronic Engineers*) (ENGST & FLEISHMAN, 2015)

Em 1999 o IEEE finalizou o padrão 802.11b (11Mbps a 2,4GHz). Em 2002, foi distribuído ao mercado o 802.11a (54Mbps a 5GHz), que é incompatível com o padrão 802.11b. No mesmo ano, foi ratificado o padrão 802.11g (54Mbps a 2,4GHz), que opera na mesma velocidade do 802.11a e na mesma frequência do 802.11b. (ENGST & FLEISHMAN, 2015).

Portanto, a história do wireless trata de descobertas que iniciou no século passado, e envolve a contribuição de vários pesquisadores, que não são menos ou mais importantes umas quanto às outras, e não deveriam ser ignoradas. Atualmente este tipo de rede já se tornou bem popular, e seu futuro parece ser ainda mais difundido no momento. Apesar da facilidade de uso deste tipo de rede, suas vulnerabilidades devem ser tratadas de forma a melhorar a proteção da rede (BARROZO, 2019).

Marques & Barrozo (2019), destaca alguns benefícios da rede wireless sem fio como: flexibilidade: a ausência de cabos permite chegar a lugares de difícil acesso para a rede cabeada; Mobilidade: os usuários podem acessar a rede de qualquer local dentro do campo de ação do ponto de acesso; Ambiente: podem ser utilizadas tanto em ambientes internos quanto externos.

Esses autores, citam que uma das principais desvantagens de utilizar uma rede sem fio e a sua má qualidade de serviço. Pois, ela é inferior em relação as redes cabeadas, que mesmo com a expansão da tecnologia, possui uma banda passante menor, sua segurança também é limitada e possui muitas falhas de comunicação devido a constantes interferências.

2.2 EQUIPAMENTOS E FUNCIONAMENTO

Segundo Arthas (2014, p.98), a topologia de uma rede IEEE 802.11 é composta pelos seguintes elementos:

> **BSS** - *Basic Service Set* - corresponde a uma célula de comunicação *wireless*.
> **STA** - *Stations* - são as estações de trabalho que comunicam-se entre si dentro da BSS.
> **AP** - *Access Point* - funciona como uma *bridge* entre a rede *wireless* e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de *Internet* pelos outros micros da rede. Eles veem de fábrica como servidores DHCP (*Dynamic Host Configuration Protocol*), facilitando a obtenção de um endereço IP na rede. Também conhecido como concentrador.
> **Bridge** - Faz a ligação entre diferentes redes, por exemplo, uma rede sem fio para uma rede cabeada convencional.
> **ESS** - Estended Service Set - consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional.

Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado *Roaming*. Dois modos de operação são previstos:

> **Infrastructure mode** - quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS).
> **Ad-Hoc mode** - quando não existe AP e as estações se comunicam entre si diretamente. Este modo não é recomendado pelo padrão (ARTHAS, 2014, p. 101).

Existem vários tipos de hardwares para acessar uma rede sem fio, como placas USB (externas), placas PCI (internas), Mini PCI (internas para notebooks), PCMCIA (internas para notebooks) e adaptadores de placas *Ethernet*.

Segundo Engst & Flsieshman (2015), palavra *Wireless* significa sem fio, ou seja, são redes cujos cabos são substituídos por ondas de rádio. Sua utilização é muito simples, assim como sua instalação, o que ajuda a proporcionar seu crescente uso atual.

Existem vários tipos e padrões de redes *wireless*, como por exemplo, o *WiMax, Bluetooth*, *Wi-Fi(Wireless Fidelity)*, *InfraRed* (Infravermelho) (ARTHAS, 2014).

Uma rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor estão se comunicando sem a presença de fios, no nosso caso, por ondas de rádio (ENGST & FLEISHMAN, 2015).

Encaixam-se nessa categoria os seguintes tipos de rede: locais sem fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), por exemplo o WiMAX (*Worldwide Interoperability for Microwave Access*), Redes de Longa Distância sem Fio ou WWAN

(*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e o novo conceito de Redes Pessoais sem fio ou WPAN (*Wireless Personal Area Network*) (ARTHAS, 2014).

Segundo Teixeira (2015), o WiMAX, que utiliza o padrão IEEE 802.16, foi ratificado em Dezembro de 2001, estava focando basicamente as faixas de frequências situadas entre 10GHz e 66GHz considerando sempre aplicações com linha de visada, obtendo até 34Mbps.

Conforme Engst & Flsieshman (2015), a grande vantagem em instalar uma rede sem fio é a mobilidade. Há alguns anos, um cenário onde permitia-se que as pessoas pudessem desfrutar da conectividade de uma rede sem a necessidade de fios era um tanto quanto futurista.

As redes sem fio proporcionam a mesma conectividade de uma rede cabeada comum dentro do perímetro de alcance da rede, tornando possível que aquele e-mail que não poderia esperar por resposta possa ser respondido no meio de uma reunião.

Segundo publicado na revista INFO Exame (Coleção 2015 – *Wi-Fi*) pela jornalista Débora Fortes (2015), algumas empresas, como a CISCO, estão adotando novas políticas de uso para este tipo de rede, como manter os *laptops* fechados durante uma reunião.

Segundo Arthas (2014, p.108), quando se discute a configuração de uma WLAN existem alguns padrões, desenvolvidos ou em desenvolvimento pelo IEEE (*Institute of Eletrical and Eletronic Engineers*) que devem ser considerados:

> **IEEE 802.11a**: é o padrão que descreve as especificações da camada de enlace e física para redes sem fio que atuam na frequência de 5GHz. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta frequência.
> **IEEE 802.11b**: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP (*Wired Equivalency Privacy)*. Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.
> **IEEE 802.11g**: descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps.
> **IEEE 802.11i**: trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e 802.11g.
> **IEEE 802.11e**: fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e 802.11a.

Os melhoramentos incluem a capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS *Quality of Service*), como também melhoramentos em aspectos de segurança. Isto significa a habilidade de oferecer vídeo e áudio à ordem (*on demand*), serviços de acesso de alta velocidade a *Internet* e Voz sobre IP (VoIP – *Voice over Internet Protocol*) (PAXSON, 2018).

Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Segundo ARTHAS (2014, p.110), os grupos do IEEE que estão desenvolvendo outros protocolos são:

> **Grupo 802.11d** – Está concentrado no desenvolvimento de equipamentos para
> definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).
> **Grupo 802.11f** – Está a desenvolver *Inter-Access Point Protocol* (Protocolo de
> acesso entre pontos), por causa da corrente limitação de proibir *roaming* entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.
> **Grupo 802.11g** – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.
> **Grupo 802.11h** – Está em desenvolvimento do espectro e gestão de extensões
> de potência para o 802.11a do IEEE para ser utilizado na Europa.

2.3 IMPLEMENTAÇÃO

Nos últimos anos, verificou-se um crescimento explosivo das “Wireless LANs”, devido ao enorme marketing feito pelos fabricantes baseando-se no principal triunfo que é a mobilidade. Outra vantagem seria, em adição àquela é a facilidade de instalação.

Entretanto, para se implementar uma rede local sem fio deve-se ficar atento a diversos fatores. É necessário um projeto bastante detalhado. O planejamento de uma rede sem fio pode durar poucos dias ou mesmo semanas, dependendo da complexidade e funcionalidades exigidas pelo seu cliente.

Esse é um processo passo a passo, em que o projetista da rede deve descobrir/pesquisar características que podem ser divididas em seis grupos:

> **Análise do ambiente** – Primeiramente deve se analisar o ambiente em será implementada a rede sem fio. Pode-se citar um escritório em que 20 pessoas farão uso da rede, uma residência com poucos computadores, um aeroporto, ou mesmo um hospital que se caracteriza como o mais complexo ambiente para a instalação de uma rede sem fio devido aos equipamentos radiológicos, portas de incêndio, longos corredores, elevadores e usuários móveis. Além da diferença do tamanho da rede, deve-se levar em conta a quantidade de usuários existentes na rede, nível mínimo de segurança exigido, largura de banda desejada, impacto que a rede terá sobre o ambiente, etc.
> **Infra-estrutura existente** – Há uma rede (cabeada ou sem fio) existente no local? O projetista deve ter muita atenção nesse item, pois se houver uma rede já existente, uma documentação detalhada deve existir contendo itens como o hardware utilizado, a frequência que está sendo usada (caso seja uma rede sem fio), número de usuários, política de segurança implementada, sistema operacional de rede em uso, convenção de nomenclatura dos equipamentos, topologia da rede, etc.
> **Localização do ambiente** – Após uma análise do ambiente, já se sabe em que local será instalada a rede. Será em um ambiente "indoor", "outdoor" ou ambos. Em ambientes "outdoor" como ligação entre prédios, pode-se ter inúmeras situações e obstáculos que dificultem a instalação e manutenção de uma rede sem fio. Obstáculos como: árvores, montanhas, prédios, e condições climáticas desfavoráveis como: fortes chuvas, ventos e neve podem enfraquecer ou mesmo eliminar o sinal de transmissão. Pode-se fazer o uso de uma torre para superar tais obstáculos, requerendo um projeto de engenharia, um estudo do local onde será instalada a torre, assim como a permissão de órgãos especializados dependendo da altura necessária. Em ambientes "indoor" como escritórios, fábricas e galpões a implementação da rede sem fio torna-se mais fácil por não possuir obstáculos naturais e pela limitação nas distâncias.
> **Finalidade do negócio** – A instalação de uma rede sem fio deve atender as necessidades de negócio do cliente. Portanto, é de crucial importância saber a finalidade da implementação da rede sem fio. Pode-se citar dois exemplos. Primeiro, a criação de um escritório temporário para conectividade dos jornalistas na cobertura de uma Olimpíada (BOLAND, 2014, p.171).

Nesse caso, a rede deve ser de alta velocidade (802.11a) com taxa de transmissão de até 54 Mbps, devido à enorme quantidade de informação que irá trafegar assim como o grande número de usuários se beneficiando da rede ao mesmo tempo.

Segundo exemplo, um escritório em que somente trafegariam na rede: arquivos, imagens, emails, etc, não necessitando de uma rede sem fio de alta velocidade. Enfim, deve-se analisar quais aplicações serão utilizadas pelos usuários.

> **Recursos disponíveis** – A cada dia, o preço dos equipamentos de rede sem fio vem caindo gradativamente, isso faz com que mais empresas invistam na implementação das redes sem fio. Entretanto, na fase de planejamento, é viável e necessário saber do cliente quais recursos estão disponíveis. Recursos financeiros, profissionais qualificados e tempo alocado para a execução do projeto são os mais importantes.
> **Nível de segurança** – A segurança é um dos fatores que mais influenciam na decisão de se adotar uma nova tecnologia. E com as redes sem fio, essa

> preocupação não é diferente. Pelo contrário, deve se utilizar todas as ferramentas disponíveis para se obter o nível mínimo de segurança. O projetista deve explicar ao cliente que as redes sem fio são mais vulneráveis que as redes cabeadas por não possuírem fronteiras de transmissão das ondas de rádio. Baseado nisso, é viável seguir a política de segurança empregada na empresa como a utilização de rede virtual privada (BARROZO, 2019, p.45).

Após um levantamento detalhado das necessidades do cliente, o projetista deve ter em mãos toda a documentação da análise realizada. Esse documento servirá como um mapa para a implementação da rede e também para uma futura referência aos técnicos e administradores. Caso o planejamento de uma rede sem fio seja feito de forma inapropriada, a rede pode não funcionar adequadamente e o cliente pode gastar muito dinheiro em hardware e software e não ter suas necessidades atendidas.

A fase de planejamento pode demorar mas é o passo mais importante na implementação de uma rede sem fio. As principais barreiras que podem afetar a propagação do sinal Wireless:

> **Antenas Baixas: u**m dos mantras repetidos à exaustão pelos manuais de pontos de acesso se refere à localização do equipamento. Quanto mais altas as antenas estiverem posicionadas, menos barreiras o sinal encontrará no caminho até os computadores. Trinta centímetros podem fazer enorme diferença.
> **Telefones sem fio:** nas casas e nos escritórios, a maioria dos telefones sem fio operam na frequência de 900Mhz. Mas há modelos que já trabalham na de 2.4GHz, justamente a mesma usada pelos equipamentos 802.11b e 802.11g. Em ambientes com esse tipo de telefone, ou próximos a áreas com eles, a qualidade do sinal Wireless pode ser afetada. Mas isso não acontece necessariamente em todos os casos.
> **Concreto e Trepadeira:** eis uma combinação explosiva para a rede Wireless. Se o concreto e as plantas mais vistosas já costumam prejudicar a propagação das ondas quando estão sozinhos, imagine o efeito somado. Pode ser uma verdadeira barreira.
> **Microondas:** A lógica é a mesma dos aparelhos de telefone sem fio. Os microondas também usam a disputada frequência livre de 2,4GHz. Por isso, o ideal é que fiquem isolados do ambiente onde está a rede. Dependendo do caso, as interferências podem afetar apenas os usuários mais próximos ou toda a rede.
> **Micro no Chão:** o principio das antenas dos pontos de acesso que quanto mais alta melhor, também vale para as placas e os adaptadores colocados nos micros. Se o seu desktop é do tipo torre e fica no chão e o seu dispositivo não vier acompanhado de um fio longo, é recomendável usar um cabo de extensão USB para colocar a antena numa posição mais favorável.
> **Água:** grandes recipientes com água, como aquários e bebedouros, são inimigos da boa propagação do sinal de Wireless. Evite que esse tipo de material possa virar uma barreira no caminho entre o ponto de acesso é as maquinas da rede.
> **Vidros e Árvores:** o vidro é outro material que pode influenciar negativamente na qualidade do sinal. Na ligação entre dois prédios por wireless, eles se somam a árvores altas, o que compromete a transmissão do sinal de uma antena para outra.

> **Migração:** para migrar de uma rede com fios para uma wireless deve-se observar alguns fatos para somente depois iniciar a implementação (FARIAS, 2015, p.67).

Quantos desktop e notebooks terão acesso sem fio a rede. Qual a área a ser coberta. O responsável do local já possui planta baixa impressa desta área. Caso positivo, o projetista deve ter muita atenção nesse item, uma documentação detalhada deve existir contendo itens como o hardware utilizado, número de usuários, política de segurança implementada, sistema operacional de rede em uso, convenção de nomenclatura dos equipamentos, topologia da rede, etc.

Se já houver um local pré-definido para a colocação do ponto de acesso, verificar a existência de tomada elétrica estabilizadora e ponto de rede de dados neste local específico.

Definir um dos padrões a utilizar: 802.11a, 802.11b ou 802.11g. Ter em mente que, dependendo da potência da antena no apartamento, a rede doméstica pode abranger uma área muito maior que apenas a da casa. Com isto a rede pode ser utilizada sem o conhecimento ou ter o tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da casa (POSTEL, 2011).

Alterar configurações padrão que acompanham o seu ponto de acesso. Alguns exemplos são: alterar as senhas. Usar senhas difíceis, que misturem caracteres e com tamanho mínimo de 8 caracteres; alterar o SSID (Server Set ID); desabilitar o broadcast de SSID.

Usar sempre que possível WEP (Wired Equivalent Privacy), para criptografar o tráfego entre os clientes e o ponto de acesso. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada.

Trocar as chaves WEP que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits); - Desligar o ponto de acesso quando não estiver usando sua rede. Existem configurações de segurança mais avançadas para redes wireless, que requerem conhecimentos de administração de redes como 802.1X, RADIUS, WPA (LAI & BAKER, 2019).

2.4 CUSTOS

Muitos usuários migram para redes sem fios por sua relação custo-benefício comparada a uma rede cabeada. Em algumas instâncias uma rede cabeada é cara demais para ser instalar.

Embora uma rede wireless de rede sem fios tenha bom custo-benefício, há assuntos que precisam ser considerados como alcance de sinal, velocidade de rede e interferência (CARTER & CROVELA, 2016).

Com ponto de partida para os gastos foi levado em conta equipamentos básicos para montar uma rede 802.11b/g de 11/54Mbps, em uma pequena e objetiva pesquisa de mercado atual levando em consideração as marcas e modelos mais conhecidos e usados.

- Access Point
Preço: R$ 320,00
- Placa de Rede Wireless PCI
Preço: R$ 190,00
- Cartão Pcmcia 11mbps 802.11b 2.4GHz
Preço: R$ 198,00
- Adaptador Wi-Fi USB 802.11g USB
Preço: R$ 129.00

2.5 SEGURANÇA

Este tipo de rede, por ser realizada através de ondas de rádio, não se limita ao perímetro onde se encontra o ponto de acesso, atravessando paredes o sinal pode chegar a alcançar a área externa do estabelecimento, facilitando o acesso indevido.

Para se evitar que um computador alheio obtenha acesso indevido a rede ou capture as informações ali trafegadas, este capítulo demonstra os métodos e ações que podem ser implementados em busca de assegurar uma maior confiabilidade e autenticidade, se utilizando, por exemplo, de criptografia como o WEP (*Wired Equivalency Privacy*) ou o WPA (*Wi-Fi Protected Access*), assegurando a confiabilidade das informações (BOLOT, 2013).

Para assegurar a autenticidade dos usuários, utilizar um servidor RADIUS (*Remote Authentication Dial-In User Server*), autenticando os usuários que podem acessar a rede.

Devido à simplicidade de uso e de configuração, a segurança tem sido o elemento mais preocupante neste tipo de rede, pois uma pessoa mal intencionada pode obter acesso de modo fácil utilizando uma antena, por exemplo, feita com uma lata tubular com papel alumínio e softwares específicos para cada situação (JACOBSON, 2012).

Uma rede wireless utilizando, por exemplo, o padrão IEEE 802.11g obtém velocidade nominal de 54mbps com um alcance, também nominal, de 100m. Para se estabelecer uma rede sem fio é preciso no mínimo, no modo estruturado, um Acess Point (AP) e um dispositivo (USB, PCI, PCMCIA) que acesse o AP (DOUNEY, 2009).

Este tipo de rede é excelente para locais onde uma rede cabeada comum não se encaixaria, obrigando a mudar todo o layout do local. Mobilidade é a palavra chave que caracteriza este tipo de rede.

Porém, é um novo ambiente, onde novos tipos de ataques surgem, forçando então a criação de mecanismos de defesa para esta aplicação. É aconselhável evitar que o sinal da rede sem fio ultrapasse os limites físicos do local onde ela opera, evitando que um atacante se posicione fora dos limites físicos do local, aumentando assim o conforto do mesmo (CHENG & MARSIC, 2012).

Para evitar que o sinal saia dos limites físicos a posição do AP é essencial, existem locais onde não há como evitar este tipo de falha, mas é uma precaução a ser estudada.

Para uma rede sem fio caseira ou de um escritório pequeno, é indicado utilizar o primeiro padrão de criptografia desenvolvido, o WEP. O WEP trabalha com chaves simétricas, ou seja, a mesma chave é sempre utilizada para encriptar e desencriptar às informações que serão trafegadas na rede (ASYMMETRIC, 2015).

Sua principal desvantagem é exatamente esta, pois um atacante que deseja ter acesso à rede pode, por meio de escuta, obter a chave, tornando possível a desencriptação dos dados da rede.

Outra desvantagem significativa é que a chave deve ser conhecida por todos aqueles que acessam a rede, o que pode facilitar a disseminação ilegal da mesma. Para corrigir as vulnerabilidades apontadas no WEP, foi criado o WPA, protocolo de criptografia mais robusto do que o anterior (PAXSON, 2017).

No WPA existe um protocolo chamado TKIP, que é responsável pelo gerenciamento das chaves temporárias, podendo alterar as chaves a cada pacote, dificultando ainda mais a escuta do tráfego da rede.

No WPA existe também um protocolo chamado EAP, responsável por permitir uma autenticação de usuário. Utilizando um servidor RADIUS para autenticar usuários a rede fica restrita apenas às pessoas que possuem uma conta cadastrada no servidor (LINHARES, 2017).

A segurança aumenta com a autenticação de usuários, porém, por utilizar novos recursos, como bancos de dados e servidores, aumenta-se a possibilidade de um ataque diretamente em cada recurso separadamente.

A criptografia tem como meta proteger as informações trafegadas na rede, mas, existem outros modos de se melhorar a segurança de uma rede sem fio, que devem ser utilizados em conjunto com a criptografia para se obter maiores níveis de segurança 9BOLAND, 2014).

Alguns APs possuem um servidor DHCP (Dynamic Host Configuration Protocol) incluso, fazendo com que qualquer pessoa que tente entrar na rede obtenha um endereço IP válido, permitindo seu acesso (PAXSON, 2018).

Desabilitar o envio do SSID (Nome da Rede), deste modo, uma pessoa que queira se conectar a rede é obrigada a saber o SSID do AP para então estabelecer uma conexão. Este recurso não é efetivo por si só, já que uma pessoa interessada em atacar pode capturar pacotes e identificar a rede (FARIAS, 2015).

Listar os endereços MAC permitidos é um recurso que pode ser utilizando em paralelo com todos os outros já citados, ele autentica apenas o aparelho que utiliza a rede, tornando possível que qualquer pessoa utilize a rede por meio de um aparelho permitido.

Existem meios de se alterar um endereço MAC de uma placa, após um atacante escutar o tráfego e obter um endereço MAC válido ele consegue alterar o endereço de sua placa e obter o acesso a rede (BARROZO, 2019).

Após associar todas as formas de segurança já citadas, a rede sem fio se torna mais segura internamente, porém, ainda vulnerável a ataques externos vindos do meio público (Internet).

Para bloquear conexões indevidas, utiliza-se um firewall na saída da rede ou mesmo em cada dispositivo que utiliza a rede. Deste modo, dificulta-se o acesso indevido pelo meio externo.

Utilizar um antivírus sempre atualizado, para evitar que pragas virtuais possam se instalar na rede e abrir portas para intrusos remotos. Um antivírus evita também que um programa de código malicioso faça com que a rede seja comprometida de forma a contaminar arquivos vitais dos sistemas operacionais. Utilizar VPN nas ligações externas da rede evita que o tráfego que sai dos AP seja capturado por um atacante (BANDIVIDTH, 2010).

Proteger apenas a rede sem fio em seu ambiente interno não é o suficiente para se garantir a privacidade dos dados trafegados, pois, os dados entram e saem do ambiente seguro, tornando o ambiente externo como foco para ataques.

3 MATERIAIS E MÉTODOS

Esse método de estudo trata-se de uma pesquisa bibliográfica de caráter qualitativo. A pesquisa Qualitativa é um estudo de método exploratório, com foco está no subjetivo do objeto analisado.

Segundo Rocha (2013), neste método as respostas costumam não ser objetivas e os resultados obtidos não são contabilizados em números exatos.

A pesquisa qualitativa tem como objetivo demonstrar os mistérios do nosso cotidiano, identificando processos de uma determinada comunidade. Não se preocupando em quantidade de dados e sim demonstrando e interpretando o acontecimento em observação. Um estudo qualitativo deve deixar explícito qual o fator problema a ser pesquisado, estabelecendo as bases da pesquisa e selecionando um determinado referencial teórico que dê suporte a pesquisa em execução (NEVES, 2015).

O mesmo autor diz que independente da maneira de como os dados foram coletados, eles têm que ser investigados e examinados cuidadosamente. A análise dos dados pode ser executada antes ou após a coleta das informações, pois desta forma é possível o pesquisador atingir conclusões mais concreta sobre o estudo em foco.

Ao contrário de números, normas ou outras generalizações, a pesquisa qualitativa labora com descrições, comparações e interpretações. Essa pesquisa busca compreender determinadas situações em profundidade, usando de questões tipo “como” e “por que”, sendo que a primordialidade é entender o fenômeno que é estudado (YIN,2015).

> Esses autores descrevem as principais características que deve estar presente na pesquisa qualitativa: a pesquisa qualitativa ocorre em um cenário natural, de forma que o pesquisador vai até o participante, o que permite uma melhor visão e envolvimento do pesquisador com o participante; a pesquisa qualitativa utiliza-se de múltiplos métodos de coletas de dados, que são interativos e humanísticos, e buscam estabelecer harmonia e credibilidade com as pessoas no estudo; uma parte considerável da pesquisa qualitativa surge durante o próprio estudo, podendo as questões de pesquisa mudar e ser refinadas, o processo de coleta de dados pode se alterar para se adequar a novas situações, como dados que se disponibilizam e dados que deixam de estar disponíveis etc.; a pesquisa qualitativa é fundamentalmente interpretativa, ou seja, ela surge da interpretação que o pesquisador faz dos dados coletados; a pesquisa qualitativa fornece uma visão ampla e abrangente dos fenômenos, ao invés de microanálises; o pesquisador qualitativo busca reconhecer os vieses que ele próprio traz à pesquisa, através de uma reflexão sistemática sobre quem ele é na pesquisa; O pesquisador qualitativo usa um raciocínio complexo multifacetado, interativo e simultâneo; O pesquisador qualitativo adota uma ou mais estratégias de investigação em seu estudo (ROSSMAN; RALLIS, 2008 apud CRESWELL, 2011).

A escolha da pesquisa qualitativa se deu pela forma investigativa do estudo, que tem como objetivo principal demonstrar a importância da tecnologia wireless área network assim como auxiliar nos processos referentes a implementação/migração do wireless rede local de acesso sem fio; demonstrar de forma simples e objetiva as vantagens em utilizar a tecnologia wireless sem a necessidade de cabos interligando computadores.

Para essa pesquisa, foi realizado um levantamento bibliográfico com os principais autores que permeiam sobre tecnologia wireless: rede local de acesso sem fio e descrito de forma clara e objetiva a ideia principal de cada autor assim como seus pontos de vistas.

Neste estudo foi realizado a explanação e descrição das ideias principais de diversos autores que defendem a tecnologia wireless: rede local de acesso sem fio, assim como também, foi realizado a discussão dos resultados obtidos.

4. RESULTADOS E DISCUSSÃO

A tecnologia wireless: rede local de acesso sem fio, tem como prioridade a proteção da informação, visto que seus objetivos principais é demonstrar a importância da tecnologia wireless área network assim como auxiliar nos processos referentes a implementação/migração do wireless rede local de acesso sem fio. E como objetivo específico: demonstrar de forma simples e objetiva as vantagens em utilizar a tecnologia wireless sem a necessidade de cabos interligando computadores.

Melhoria sem fio: propósito, cobertura, gestão, segurança sem fio para visitantes, implementação N/W para celulares, investimento, orçamento e investimento.

A melhoria do N/W Wireless aumentando a cobertura 30 Access Point 41 Access Point para cobrir toda a fábrica, melhorando a gestão, muitos AP para controlar todos os AP controlados por WLC*.

Figura 1 - WLC – Wireless LAN Controller (todos os pontos de acesso serão gerenciados por um único equipamento N/W.

Fonte> própria

Melhorando a segurança sem fio para visitantes, autenticação por senha, autenticação por ID e senha via Portal Web. Implementação N/W para celulares, os celulares usam o mesmo NW para visitantes e será criado N/W apenas para celulares.

Beal & Sêmola (2013), conceituam a segurança sem fio em redes como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. Se traduz como um método de proteção da informação das ameaças a sua confidencialidade e

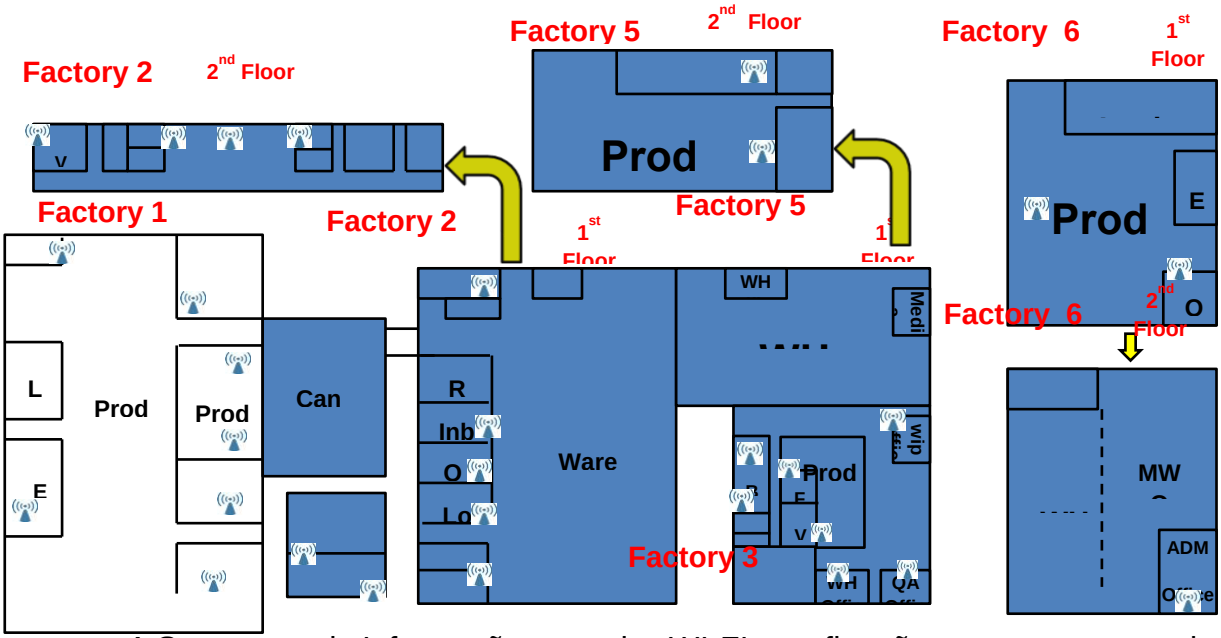
integridade.

Um detalhe importante que deve ser ressaltado é que todos os meios que lidam com as tecnologias da informação precisam elencar quais são os priores para a proteção já que não é possível controlar tudo de maneira uniforme. Pois para Beal (2015), a informação é um recurso importante para qualquer instituição, seja ela de pequeno ou grande porte.

O autor explica que as Instituições geram muitas informações e compartilham da mesma internamente para determinados nichos. Essas informações são restritas e confidenciais e que se caso não tenha uma adequada Segurança da Informação esses dados podem vazar e prejudicar de forma desmesurada a Instituição.

Posthumus e Von Solms (2014), completa que a informação tem uma grande relevância dentro das Instituições e deve ser assegurada de forma adequada e sigilosa. Erros por parte da equipe de Tecnologia da Informação se tratando sobre a Segurança da Informação, podem comprometer os dados e podem gerar grandes consequências como prejuízos financeiros e danos irreversíveis à imagem das Instituições.

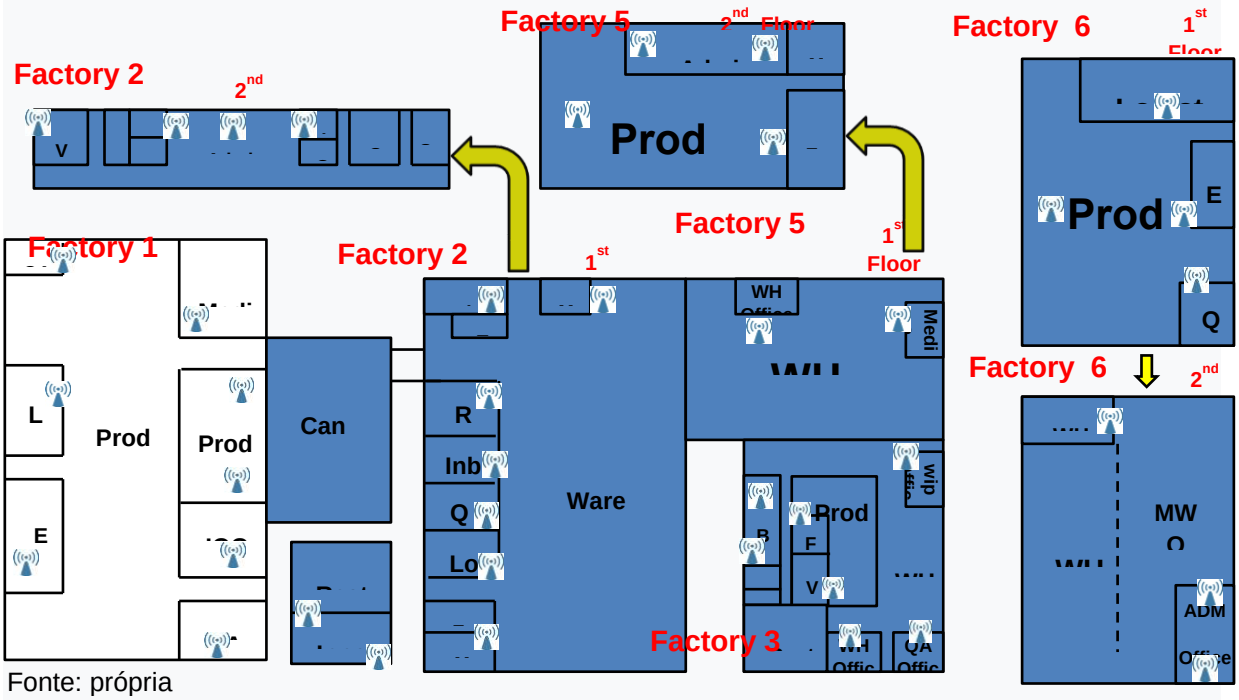
Figura 2 - AS-IS (30 pontos de acesso para todos os de fábrica



A Segurança da Informação em redes WI-FI sem fio, não se trata somente de aperfeiçoar um sistema de segurança somente em um grupo de computadores, utilizando antivírus ou barreiras de proteção ligadas na rede. Uma conexão wireless, mal protegida se torna porta de entrada fácil para invasores, especialmente em âmbito

Institucional. Por isso é necessária uma equipe de segurança da informação focada na seguridade dos dados.

Figura 3 - TO-BE 41 pontos de acesso para todos



Fonte: própria

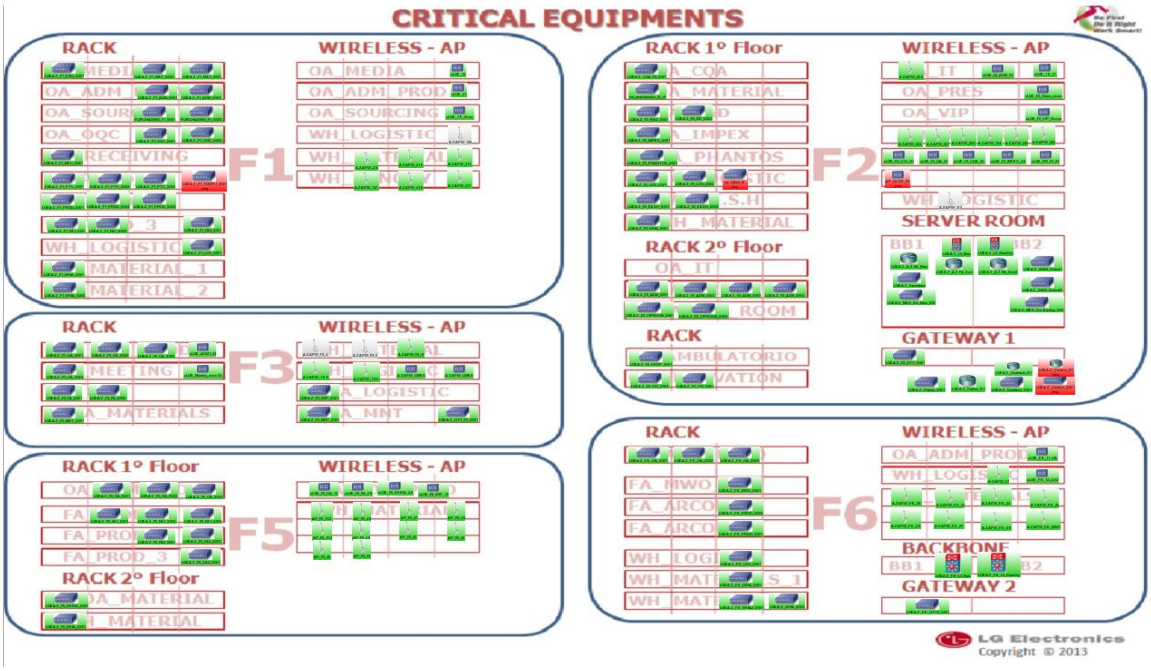
É relevante que os profissionais de sistema de telecomunicações invistam seu tempo em aprendizado de técnicas cada vez mais avançadas, com o objetivo de empregar medidas de segurança cada vez mais refinadas. Pois os invasores quando têm acesso as quaisquer redes de WI-FI conseguem acompanhar todos os passos dos usuários que a utiliza.

Para Henriques (2019), o Wi-Fi sem fio não precisa de permissão para ser instalado nem para atuar. A maior parte das Instituições fazem o uso do Wi-Fi com o objetivo de facilitar o trabalho interno e externo, entretanto muitos não têm o conhecimento de quais são os riscos e cuidados que deve ter ao utilizar a rede Wi-Fi sem fio.

Porque através da rede Wi-Fi é possível que os invasores tenham acesso a quais sites são acessados por aquela rede e com isso tenham acesso total as informações trocadas como logins na rede e arquivos confidenciais.

Para evitar esse acesso as informações confidenciais pelo o Wi-Fi, foi possível observar com este estudo, que a equipe de Segurança da Informação em redes deve utilizar protocolos de segurança como a Criptografia para proteger dados e senhas dos usuários que se conectam as redes de Wi-Fi.

Figura 4 - Todos os pontos de acesso são controlados individualmente



Fonte: própria

A quantidade de pontos de acesso não cobre toda a fábrica. A Gerência é muito difícil. Todos os pontos de acesso são controlados individualmente. Não há nenhuma rede apenas para celulares. Não há controle de acesso para rede sem fio para convidados. (mesma senha para todos)

De acordo com Linhares e Gonçalves (2017), o WPA2 é o protocolo de segurança mais seguro da atualidade, pois ele utiliza a certificação AES e devido a sua elevada complexidade, o relato de quebras de segurança desse protocolo é praticamente nula. Sendo o protocolo mais usado nas Instituições. O autor destaca outras criptografias como WEP e o WAP, porém não são tão seguras e não são utilizadas atualmente devido a suas falhas de segurança.

Figura 5 - Controlador de LAN sem fio Série WLC 5508

Fonte: própria

Aumente a quantidade de pontos de acesso para cobrir toda a fábrica. Instale o equipamento WLC para gerenciar todos os pontos de acesso. Crie uma nova rede apenas para celulares. Faça a política por WLC para controlar o ID e a senha.

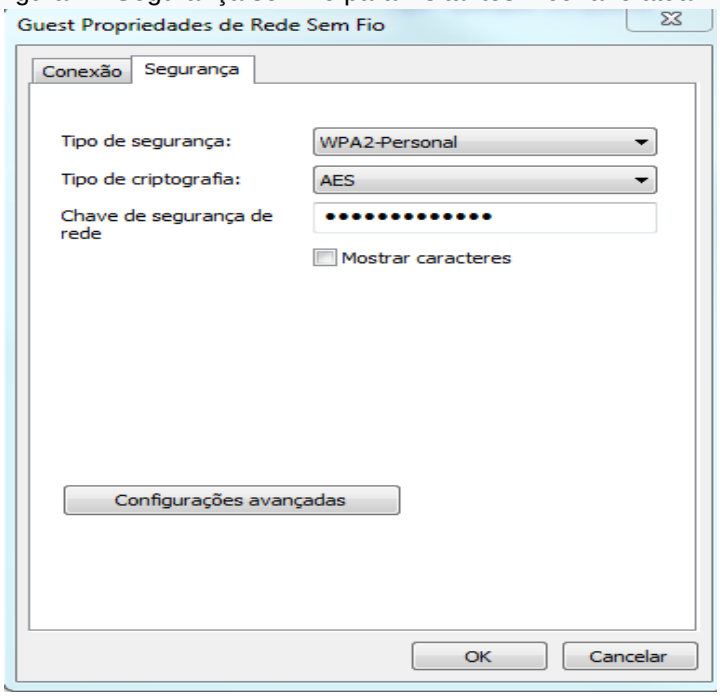
Henriques (2019), destaca que além da criptografia em redes, outra forma de segurança da informação básica e limitar o acesso à rede, principalmente em redes que são corporativas. Pois com essa limitação as Instituições conseguem ter um controle maior sobre seus usuários que se conecta à rede e para que eles a usam.

Figura 6 - 02 WLC para redundância

Fonte: própria

Assim sendo, foi possível destacar neste estudo a relevância da rede wifi sem fio, assim como também a importância de profissionais capacitados e voltados para o sistema de telecomunicações em redes Wi-Fi sem fio, com o objetivo de monitorar constantemente a rede, detectando possíveis ameaças antes que elas possam causar danos dolosos às Instituições e aos usuários.

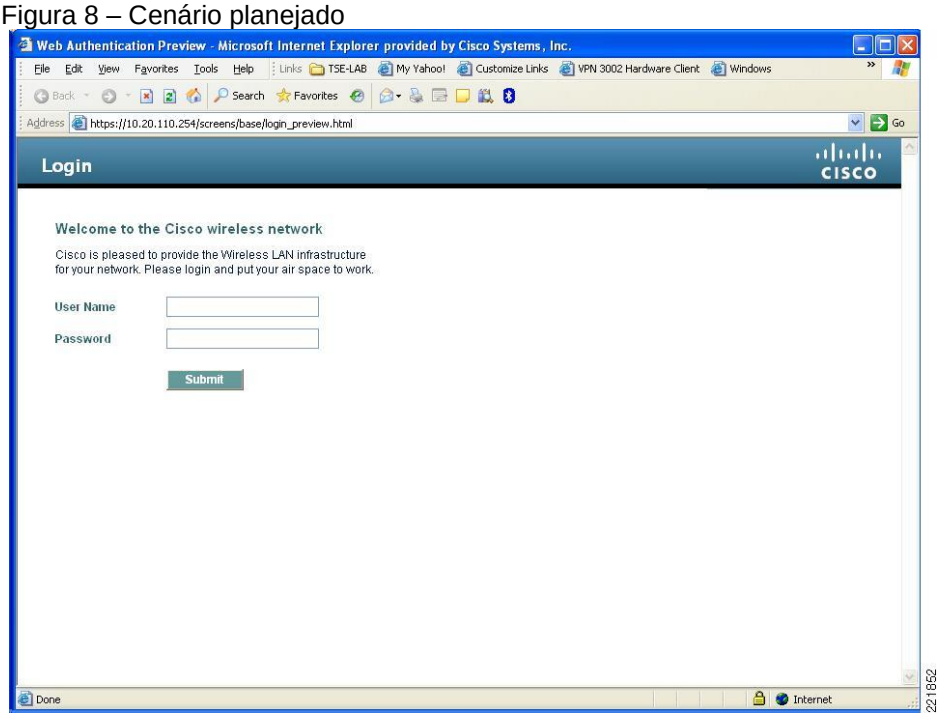
Figura 7 - Segurança sem fio para visitantes – cenário atual



Fonte: própria

Fácil de hackear a senha sem fio por outro desktop, A senha pode ser facilmente descoberta por meio de outra área de trabalho. Todos os usuários usam a mesma senha.

Figura 8 – Cenário planejado



Fonte: própria

A autenticação será feita pelo portal Web através de ID e senha, cada usuário deve ter ID e senha diferentes e o acesso será permitido por período através da Configuração WLC

Figura 9 – Investimento
AS- IS

Factory	Quantity
1	9
2	9
3	7
5	2
6	3
Total	**30**

Fonte: própria

Figura 10 – TO - BE

Factory	Quantity
1	9
2	11
3	7
5	7
6	7
Total	**41**

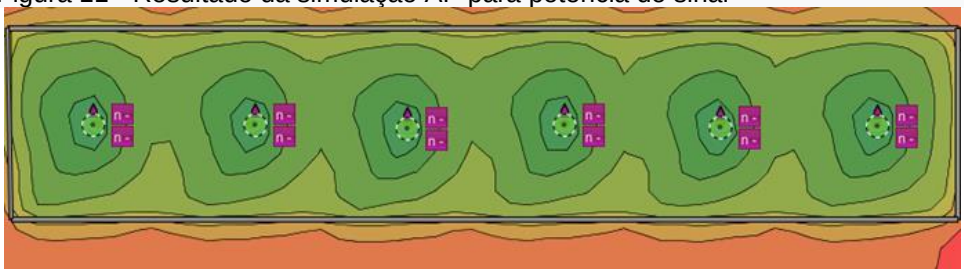
Fonte: própria

Ponto de acesso por fábrica

11 AP CISCO AIR-SAP2602I-T-K9 (NOVO

- 30 AP CISCO AIR-SAP2602I-T-K9

Figura 11 - Resultado da simulação AP para potência do sinal



Fonte: própria

Big Office (100m X 20m) – 4 or over APs

Figura 12 - Resumo

Type	QTY	PRODUCT	DESCRIPTION	UNIT PRICE	TOTAL PRICE	Dolar Rate
Access Point	11	AIR-SAP2602I-T-K9	802.11n SAP w/CleanAir; 3x4:3SS; Mod; Int Ant; T Reg Domain	697,00	7.667,00	2,33
	11	CON-CNT-C262IK	SmartNet 8x5x NBD 802.11n CAP w/CleanA	58,00	638,00	
	11	AIR-PWRINJ4=	POWER INJECTOR 2600 SERIES	105,00	1.155,00	
	11	AIR-AP-BRACKET-2=	CISCO AIR AP Universal Mounting Bracket	10,00	110,00	
	3	WS-C2960S-48TS-L	CISCO CATALYST 2960-S 48 PORT GIGE 4XSFP LAN BASE	2.685,00	8.055,00	
	3	CON-SNT-2960S4TS	SmartNet 8x5x NBD CATALYST 2960-S 48 PORT	323,00	969,00	
WLC	2	AIR-CT5508-50-K9	Cisco 5508 Series Controller for up to 50 APs	14.215,00	28.430,00	
	2	CON-SNT-CT5508	SmartNet 8x5x NBD 5508 Series Controller	3.455,00	6.910,00	
	2	AIR-CT5508-HA-K9	Cisco 5508 Series Wireless Controller for High Availability	12.950,00	25.900,00	
	2	CON-SNT-CT5508HA	SmartNet 8x5x NBD Cisco 5508 Series	3.095,00	6.190,00	
	4	AIR-PWR-5500-AC	Cisco 5500 Series Wireless Controller Redundant Power Supply	930,00	3.720,00	
Tax	1	Tax + Freight + Dollar Rating (12 %)			10.769,28	
USD Amount					100.513,28	
BRL Amount						234.195,94

Fonte: própria

Figura 13 - Orçamento X Investimento - detalhe do valor do projeto

Project Name on ITMS	Account Code	Budget Plan	Used	Request	Balance
EAZ - Wireless N/W Extension: Access Point (AZ)	15231303	R$ 48.930,00	R$ 0,00		
EAZ - Wireless N/W Extension: WLC Implementation (AZ)	15231303	R$ 186.400,00	R$ 0,00		
Total		**R$ 235.330,00**	R$ 0,00	**R$ 234.195,94**	**R$ 1.134,06**

CISCO 2602I AP

QTY	PRODUCT	DESCRIPTION	UNIT PRICE	TOTAL PRICE	Dolar Rate
11	AIR-SAP2602I-T-K9	802.11n SAP w/CleanAir; 3x4:3SS; Mod; Int Ant; T Reg Domain	697,00	7.667,00	2,33
11	CON-CNT-C262IK	SmartNet 8x5x NBD 802.11n CAP w/CleanA	58,00	638,00	
11	AIR-PWRINJ4=	POWER INJECTOR 2600 SERIES	105,00	1.155,00	
11	AIR-AP-BRACKET-2=	CISCO AIR AP Universal Mounting Bracket	10,00	110,00	
3	WS-C2960S-48TS-L	CISCO CATALYST 2960-S 48 PORT GIGE 4XSFP LAN BASE	2.685,00	8.055,00	
3	CON-SNT-2960S4TS	SmartNet 8x5x NBD CATALYST 2960-S 48 PORT	323,00	969,00	
1	Tax + Freight + Dollar Rating (12 %)			2.231,28	
Total USD				**20.825,28**	
Total BRL					**48.522,90**

WLC IMPLEMENTATION

QTY	PRODUCT	DESCRIPTION	UNIT PRICE	TOTAL PRICE	Dollar Rate
2	AIR-CT5508-50-K9	Cisco 5508 Series Controller for up to 50 APs	14.215,00	28.430,00	2,33
2	CON-SNT-CT5508	SmartNet 8x5x NBD 5508 Series Controller	3.455,00	6.910,00	
2	AIR-CT5508-HA-K9	Cisco 5508 Series Wireless Controller for High Availability	12.950,00	25.900,00	
2	CON-SNT-CT5508HA	SmartNet 8x5x NBD Cisco 5508 Series	3.095,00	6.190,00	
4	AIR-PWR-5500-AC	Cisco 5500 Series Wireless Controller Redundant Power Supply	930,00	3.720,00	
1	Tax + Freight + Dollar Rating (12 %)			8.538,00	
Total USD				**79.688,00**	
Total BRL					**185.673,04**

Fonte: própria

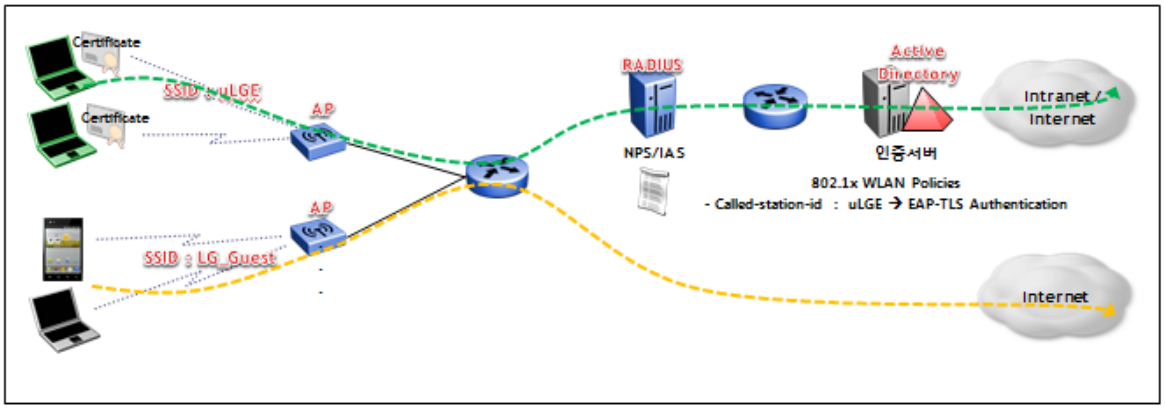
Figura 14 - Ponto de acesso - AIR-SAP2602I-T-K9

Fonte: própria

Figura 15 - WLC 5508 Series

Fonte: própria

Figura 16 - Implementação NW do convidado - criar NW Wireless Guest



Fonte: própria

Faça NW para Mobiles para conectar apenas a Internet e o escritório de aplicativos da LGE. Se o circuito tiver um problema, pode ser bloqueado Mobile NW primeiro e outros tráfegos da Internet serão bloqueados, consulte o uso do circuito.

Sempre recebemos visitantes na LG (especialmente LG display para fábrica BM) e eles não podem acessar a internet de acordo com nossas regras (AD Account e Waterwall Client). Sempre que precisamos solicitar exceção pelo CSR para todos os visitantes acessarem a Internet, o gerenciamento de IP é muito difícil, a aprovação do CSR demora muito (3 ou 5 dias).

5 TRABALHOS FUTUROS

Pode-se abordar melhor em trabalhos futuros os estudos da tecnologia wireless redes sem fio, sendo observado outros modelos que irão surgir futuramente em meio a área tecnológica tecnológico que atualmente consiste em aplicações institucionais que estão sendo usadas nesse momento, visto que ataques para obtenção de dados são cada vez mais frequentes pode-se esperar outros avanços para evitar que esse tipo de ação seja aceito facilmente no intuito da coleta de dados informacionais.

6 CONCLUSÃO

Como todo ambiente lógico não é totalmente seguro, as redes sem fio têm suas vulnerabilidades, atualmente existem vários processos que ajudam a tornar um ambiente Wireless seguro, mesmo não garantindo que a rede seja totalmente segura.

Uma rede como wireless sem fio, elas são versáteis e úteis em muitos casos, desde que se faça uso de seus métodos e ações para garantir a privacidade e qualidade das informações transitadas e aumentar a sensação de que o ambiente sem fio é seguro.

REFERÊNCIAS

ARTHAS, Kael. **Tutorial wireless.** 2014. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=269602 . Acessado em: 25/09/2022.

BABOO, Fórum. **Ataques às redes sem fio**. 2015. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=335352 . Acessado em: 14/10/2022.

BANDWIDTH place, 2010. http://www.bandwidthplace.com/.

BARROZO, Leandro Lavagnini. **Segurança nas redes sem fio:** Wireless e Wimax. 2019. 56 Trabalho de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2019.

BOLAND, H.E MOUSAVI, H. **Security issues of the IEEE 802.11b wireless LAN. Electrical and Computer Engineering**. Canadian Conference on. Vol. 1, 2014, pp. 333 – 336.

BOLOT, J.C. "**End-to-end packet delay and loss behavior in the Internet,**" ACM SIGCOMM '93, pp. 289-298, San Francisco, 2013.

BORSC, M.e Shinde, H. **Wireless security & privacy. Personal Wireless Communications**, ICPWC 2015. 2015 IEEE International Conference on, 2015, pp. 424 – 428.

CAIXETA, P. C.; CAIXETA, P. C. **A evolução das Redes Sociais**. Revista Observatório Patense, Patos de Minas, 07 jul. 2012.

CANCELA, Lucas Borcard; GUIMARÃES, Karlos Eduardo; SOUZA, Flávio Eduardo De., et al. **A Importância da Segurança da Informação em Redes WI-FI**. XV Encontro Virtual de Documentação em Software. v. 7, n. 1 VII Anais do Evidosol/Ciltec Edição 2018.

CARTER, R.L; M.E. Crovella, "**Measuring bottleneck link speed in packet-switched networks,**" TR-96-006, Boston University, Mar. 2016, http://www.cs.bu.edu/techreports/pdf/1996-006-measuring-bottlenecklink.pdf.

CERT. **Práticas de Segurança para Administradores de Redes *Internet*,** 4.13.6. Monitoração da Rede *Wireless*. 2003. Disponível em: http://www.cert.br/docs/seg-admredes/seg-adm-redes.html#sec1. Acessado em: 10/11/2022.

CHENG, L and I. Marsic, "**Accurate bandwidth measurement in Xdsl service networks,**" Computer Communications 25, pp. 1699-1710, Feb.2012.

COSTA, Jorge Procópio Da. **Softwares de segurança da informação**. Centro de Educação Tecnológica do Amazonas – CETAM. Manaus, 2010.

DOWNEY, A. B. **“Using pathchar to estimate Internet link characteristics**,”Proceedings ACM SIGCOMM ’99, pp. 241-250, Aug/Sep. 2009.

ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio:** O guia prático sobre redes *Wi-Fi* para Windows e Macintosh. São Paulo: Pearson Makron Books, 2015

FARIAS, Paulo César Bento. **Rede Wireless**. 2015, Disponível em: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp -Acessado em 10/10/2022.

JACOBSON, V. “**Pathchar-A tool to infer characteristics of Internet paths**.” 2012.

LAI, K; Baker, M. **“Measuring bandwidth**,” IEEE INFOCOM ’99, pp. 235-245, New York, Mar. 2019.

LAKSHMINARAYANAN, K; V.N. Padmanabhan and J. Padhye. **“Bandwidth Estimation in Broadband Access Networks**” IMC ’04, 8 Pages, Taormina, Sicily, Italy, Oct. 2014.

LINHARES, André Guedes;GONÇALVES,Paulo André Da. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11:WEP, WPA, WPA2 e IEEE 802.11w**. Universidade Federal de Pernambuco (UFPE) - Centro de Informática (CIn)Av. Professor Luís Freire s/n – Cidade Universitária - Recife – PE – Brasil{agl., pasg}@cin.ufpe.br,2017.

PATRICK. **História e Perspectivas, O Início da Tecnologia Wireless**. 2016. Disponível: em http://www.mundowifi.com.br/forum/thread63.html . Acessado em 26/10/2022

PAXSON, V. **“Measurement and Analysis of End-to-end Internet Dynamics**,” PhD Thesis, University of California, Berkeley, Apr. 2017.

._____ “**End-to-end Internet packet dynamics**,” ACM SIGCOMM ’97 pp. 139-152, Cannes France, 2018.
POSTEL, J. **“Internet Control Message Protocol**.” RFC 792, Sep. 2011.

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP.** 2005. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp. Acesso em: 04/10/2022.