PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO EM REDES WIFI

DIEGO MENDES RAMOS

GOIÂNIA
2020

DIEGO MENDES RAMOS

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO EM REDES WIFI

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciências da Computação.
Orientador (a):
Prof. (a) Me. Fernando Gonçalves Abadia
Banca examinadora:
Prof. Me. Max Gontijo de Oliveira
Prof. Dr. Gustavo Siqueira Vinhal

GOIÂNIA
2020

DIEGO MENDES RAMOS

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO EM REDES WIFI

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciências da Computação, em _____/_____/_____.

_____
Prof. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

_____
Orientador: Prof. Me. Fernando Gonçalves Abadia

GOIÂNIA
2020

RESUMO

As redes sem fio começaram a ser usadas nos anos 90, através de sinais da rádio frequência, tecnologia que foi criada no âmbito militar e com o passar dos tempos se tornou uma grande inovação tecnológica. Com o avanço das tecnologias, a sociedade passou a notar a vulnerabilidade das redes WI-FI e de qualquer outra tecnologia que faça o uso da conectividade sem fio e da internet, devido ao fato dessas tecnologias trafegarem vários tipos de informações sigilosas do cotidiano de cada usuário. Esse estudo teve como objetivo analisar a importância da segurança da informação em redes de Wi-Fi e descrever o papel da Tecnologia da Informação (TI) diante do processo de segurança em redes. Se trata de uma pesquisa bibliográfica, de caráter qualitativo, no qual foi realizado um levantamento bibliográfico, com os principais autores que demonstram a importância da Segurança da Informação em redes WI-FI. Foi possível observar, através deste estudo, as falhas de segurança nas redes Wi-FI, assim como também a importância da Tecnologia da Informação em segurança das redes.

Palavras-chave: Wi-FI; sistemas de redes; segurança da informação.

ABSTRACT

Wireless networks began to be used in the 1990s, using radio frequency signals, a technology that was created in the military sphere and over time has become a major technological innovation. With the advancement of technologies, society began to notice the vulnerability of WI-FI networks and any other technology that makes use of wireless connectivity and the Internet, due to the fact that these technologies travel various types of sensitive information in the daily lives of each user. This study aimed to analyze the importance of information security in Wi-Fi networks and describe the role of Information Technology (IT) in the face of the network security process. It is a qualitative bibliographic research in which a bibliographic survey was carried out with the main authors that demonstrate the importance of Information Security in WI-FI networks. It was possible to observe through this study the security flaws in Wi-FI networks, as well as the importance of Information Technology in network security.

Keywords: Wi-FI; network systems; information security.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Com o passar do tempo as pessoas começaram a notar as vulnerabilidades da segurança no uso de dispositivos e computadores com acesso sem fio. O uso da Tecnologia sem fio para os usuários se tornou prático e necessário, se tornando um grande facilitador no dia a dia. 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).

As redes sem fio hoje chamadas de WI-FI 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 a 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).

A Segurança de dados não era o foco, mas o avanço da tecnologia trouxe a necessidade de tê-la vinculada a seus dispositivos, no entanto com as empresas tendo problemas de segurança surgindo revela também que falta muito estrutura para conviver com esses problemas no dia-a-dia.

1.1 Justificativa do Trabalho

Nos tempos atuais, há 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 suas necessidades, onde se trafegam várias informações sigilosas da vida de cada indivíduo, seja de redes sociais, mensagens de texto, pesquisas na internet (CANCELA, GUIMARÃES et al,.2018).

Pessoas usufruem do lazer e entretenimento digital sem ao menos ter noção de sua vulnerabilidade e exposição, onde pode haver vários problemas, sendo vítimas de invasão e tendo dados acessados por invasores, desde então a segurança da informação se tornou uma necessidade para muitos.

Costa (2008), indaga que a Criptografia tem um grande papel de proteção sendo em conexões WLAN ou até mesmo em rede LAN, consistindo a maior importância em redes wireless por serem umas das mais fáceis de serem invadidas, é possível ter acesso em uma rede Wi-Fi e logo em seguida ter acesso a rede LAN.

Cancela e Guimarães (2018), “Destaca-se que, em uma organização, a informação pode valer até mais do que a própria infraestrutura da empresa”. Isso se destaca principalmente em redes sem fio ou até mesmo cabeadas lotadas em empresas e corporações que se pode ver no dia-a-dia.

Essas mesmas empresas que disponibilizam acesso à internet oferecem já o acesso sem fio que já utiliza um protocolo de segurança mais recente denominado WPA2 sucessor do WPA onde traz uma senha robusta que dificulta ainda mais o meio de invasão e que aumenta a segurança da informação em redes Wi-Fi para evitar a coleta de dados de qualquer gênero.

1.2 Objetivo Geral

Analisar a importância da segurança da informação em redes de Wi-Fi e descrever o papel da Tecnologia da Informação (TI) diante do processo de segurança em redes.

1.3. Objetivo Específico

- Descrever a contribuição da segurança da informação em redes Wi-Fi.
- Comparação de padrões de segurança em redes domésticas.
- Descrever o papel dos estudiosos da tecnologia da informação diante do processo de segurança em redes.
- Gerar Bibliografia Acerca do Tema Específico.

1.4. Metodologia

Este Trabalho terá como foco de metodologia a pesquisa bibliográfica, com classificação de um trabalho qualitativo.

Assim sendo, Goldenberg (1997), afirma que os estudiosos qualitativos rejeitam o molde positivista usado ao estudo da vida social, uma vez que o pesquisador não pode fazer julgamentos nem permitir que seus preconceitos e crenças contaminem a pesquisa.

Neste trabalho foi desenvolvido uma pesquisa embasada em livros, artigos científicos, endereços da internet afim de disponibilizar para o usuário como entender melhor sobre a segurança na internet vinculada a redes Wi-Fi.

1.5 Organização do Trabalho

Este trabalho terá o objetivo de apresentar os 4 tópicos dos objetivos específicos deste presente capítulo, desenvolvê-los e apresentar de uma maneira onde o usuário e leitor possam entender sem nenhuma dificuldade caso necessário será utilizado as tabelas dispostas ao trabalho para auxiliar caso julgue necessário.

O Desenvolvimento do trabalho dado como fundamentação teórica terá partida no capítulo dois trazendo uma explicação leve sobre os ambientes de rede Wi-Fi referente aos objetivos e uma forma de contornar certas situações para se manter com maior segurança em seus dispositivos pessoais, o capitulo três tem como objetivo apresentar os tipos de criptografia vinculada as redes Wi-Fi atualmente e mostrar meios de ter uma melhor segurança e privacidade de dados.

O capítulo quatro tem o foco de mostrar os materiais e métodos utilizados neste estudo, assim como também uma pequena explanação sobre a importância da pesquisa qualitativa. Em seguida o capítulo cinco trará a discussão dos principais autores utilizados na pesquisa assim como também análise dos resultados obtidos.

O capítulo seis tem o foco de mostrar o que foi concluído referente a pesquisa bibliográfica e suas informações, a coleta de todas as informações ao discorrer do tema, após isso se encontram as referências bibliográficas onde se apresenta todas as fontes da coleta de dados.

2 FUNDAMENTAÇÃO TEÓRICA

O uso da tecnologia sem fio Wi-FI 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, 2008).

2.1 A Valorização da Segurança da Informação na Sociedade

Beal (2005), em seus estudos nos traz que a segurança da informação, é o método de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Já Sêmola (2003) define segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. ”

Desta forma, pode-se conceituar segurança da informação como um campo do conhecimento que tem como objetivo a proteção da informação das intimidações a sua integridade, disponibilidade e confidencialidade a fim de certificar a ininterrupção do negócio e minimizar os riscos.

A proteção da informação, tem como objetivo defender as características e atributos de dados informativos de confidencialidade, integridade, disponibilidade, autenticidade preservando todas as fraquezas em relação a um indivíduo ou organização que queiram beneficiar-se por ameaças e que tenham probabilidades de atingir um negócio de uma organização afim de afetar e trazer perdas inquestionáveis, meio que não estão de nenhuma forma protegidos por meio de sistemas de computação nem a dados de formato eletrônico. (GORDON; LOEB, 2002; SÊMOLA, 2003; ABNT, 2006).

A informação é um meio importantíssimo para qualquer organização, seja de porte pequeno ou grande, independente do segmento de atuação. Os processos organizacionais funcionam através da geração de informações e o compartilhamento dela para determinados nichos. A gestão faz o uso da informação para tomar decisões assertivas, de forma que as organizações atinjam seus objetivos e aprimorem sua atuação no mercado. (BEAL ,2005).

Desta forma, segundo Posthumus e Von Solms (2004), a informação tem relevância estratégica e deve ser protegida de forma adequada e segura. Erros na segurança da informação podem comprometer a informação e podem gerar como consequências, grandes prejuízos financeiros assim como também, grandes danos à imagem das instituições

De acordo com a NBR ISSO/IEC 17799 (2005), conceitua a segurança da informação como:

> É a política de proteção existente sobre as informações de uma determinada organização de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades do negócio. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição (NBR ISSO/IEC 17799,2005).

Diante o exposto, é imprescindível determinar critérios para a elucidação do nível de segurança que se deseja alcançar, com análises diárias, permitindo o crescimento ou retrocessos no âmbito da segurança da informação na organização.

Ferreira (2003), indaga que aprimorar um sistema de segurança da informação, não se aplica somente em um grupo de computadores antivírus ou barreiras de proteção ligadas na rede de computadores de uma instituição. Para conseguir um sistema de segurança da informação e importante entender os princípios de segurança para poder criar e estabelecer políticas e soluções cabíveis de acordo com a necessidade de cada instituição.

Ferreira (2003), completa que é importante entender os princípios da segurança da informação para que possa conseguir executá-lo. Durante esse processo é relevante criar ferramentas que possam auxiliar o usuário para prevenção e suporte diante de qualquer tipo de falha que possa acontecer.

De acordo com Silva (2003), os pontos fundamentais para a introdução da segurança da informação devem seguir os cinco princípios básicos:

> 1. A relação custo e benefício: garantir investimentos para a implementação e a manutenção favoráveis, e o retorno que proporciona a prevenção e a proteção do sistema de informação. Tal situação só é lembrada pelos proprietários quando um grande desastre ou ataque ocorre e o custo de restauração das informações das bases de dados muitas vezes, é maior do que se tivesse investido meses em um sistema de segurança da informação seguro e estável.
> 2. O princípio da concentração: proporciona à possibilidade de se administrar as medidas necessárias de segurança da informação para atender necessidades de melhoramento de proteção de diferentes bases de dados sensíveis a alterações.

> 3. O princípio da proteção em profundidade: proporciona medidas de proteção de segurança (físicas ou lógicas) como câmeras de vigilância, biometria e reconhecimento de voz. A utilização deste princípio evita um conjunto de medidas de proteção distintas e avulsas para não se tornar uma soma ineficiente e lenta de obstáculos para um ambiente mais seguro.
> 4. O princípio da consistência: determina que as medidas de proteção da Segurança Informação possuam um nível de sensibilidade intercambiável para que reduzam as falhas dos programas de segurança das organizações. Sua utilização atinge a todos os níveis acessos do sistema de informação tanto como físico ou lógico, por exemplo, impedir que um filho de um sócio da organização instale jogos, acesse páginas indevidas com o servidor da empresa ou permitir pessoas não autorizadas ter acesso aos computadores da organização.
> 5. O princípio da redundância: determina a importância de se adotar mais do que uma forma de proteção da SI. Caso ocorra a falha do processo A de segurança será executado o processo B para que o sistema de informação continue em pleno funcionamento, Ex.: possuir servidores de contingência em locais diferentes replicando as informações entre as filiais efetuando *backups* automáticos diariamente com sistemas de espelhamentos de *hard disk* (SILVA,2003).

Para Silva (2003), estes princípios são dirigentes pela segurança da informação que deverá ser implementada de forma que venha estabelecer princípios para um âmbito mais seguro.

Dado que, a segurança da informação e a gestão de risco devem trabalhar lado a lado para que, desta maneira, seja admissível criar um plano de imprevisibilidade de segurança com o objetivo de resolver falhas e prever possíveis riscos para garantir a continua qualidade da segurança da informação.

2.2 Segurança da informação em redes sem fio

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.

Farias (2005) afirma que 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 Farias (2005), nos tempos atuais pode-se refletir em redes Wireless como uma opção bastante inovadora em relação as redes cabeadas. Suas aplicabilidades são variadas e tem como principal característica sua locomobilidade, fato que a torna mais aceita nos ambientes corporativos.

Devemos destacar a WPAN (Wireless Personal Area Network) ou rede pessoal sem fio, como uma rede que normalmente é utilizada para relacionar aparelhos eletrônicos fisicamente próximos. De acordo com Busch (2008), este tipo de rede é perfeito para extinguir os cabos utilizadas para interligar impressoras, teclados, telefones computadores, mouses e outros. Nos equipamentos atuais tem sido utilizado em grande escala o padrão Bluetooth para estabelecer esta comunicação assim como também, é utilizado o infravermelho.

Busch (2008), elucida também que 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.

2.2.1 Rede WI-FI

A Wi-Fi Alliance foi responsável em licenciar a marca Wi-Fi para representar a tecnologia de redes sem fio (WLAN) essa rede embarcada baseada no padrão IEEE (Institute off Electrical and Eletronics Engineers) 802.11.

As redes Wi-Fi como padrão consistem em faixas de frequência que as tornam chamativas por não possuírem uma certa necessidade de haver uma licença para se instalar ou uma operação do usuário, se o mesmo for usado comercialmente existe a necessidade de se ter a licença da Agência Nacional de Telecomunicações (Anatel). É necessário estar no alcance das redes WI-FI para ter acesso a internet por um ponto de acesso (modem, roteador, repetidor) utilizando dispositivos moveis como celular, notebook (MENDES, 2008).

Segundo Miranda (2013), os principais padrões de redes sem fio são:

802.11a: Alcançando velocidades de no máximo 54mb com o padrão IEEE e de 72 a 108 por outros fabricantes, suporta 64 dispositivos simultâneos e é compatível com redes 5 GHz onde tem uma banda maior de velocidade, sua vantagem é a velocidade e sua frequência pois tem várias faixas onde fica difícil de acontecer alguma interferência, sua desvantagem é a incompatibilidade com o Acess point 802.11 b e g, referente a clientes, pois a compatibilidade se dá com o padrão 802.11a sendo compatível com o padrão 802.11b e 802.11g padronizando assim a fabricação de dispositivos e facilitando seu uso.

802.11b: Tendo como padrão a IEEE consegue chegar aos seus 11Mbps e 22Mbps por outros fabricantes, aceita somente frequência 2.4 GHz ou seja com qualquer dispositivo Wi-Fi comum, tem suporte simultâneo para até 32 dispositivos em seu ponto de acesso, sua desvantagem é a alta interferência dada pelo baixa opção de canais disponíveis dada em transmissão como na recepção de sinais, porque sua frequência se assemelha com fornos de micro-ondas, dispositivos que tem suporte a Bluetooth, radio, dentre outros, mas acaba sendo financeiramente vantajoso pois os dispositivos que nela agrega tem custos mais baixos, por todo o mundo o padrão 802.11b é usado principalmente pela maioria dos fornecedores de internet sem fio do mundo.

802.11g: Possui compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 54 Mbps que funciona na frequência de 2,4 GHz, possui os mesmos inconvenientes do padrão 802.11b. Sua maior vantagem e a velocidade, pois usa a autenticação WEP estática. Entretanto, por vezes e difícil de configurar como Home Gateway por conta da frequência de rádio e outros sinais.

802.11n: Possui uma largura de banda de até 300 Mbps e tem alcance de 70 metros. Atua nas frequências de 2,4GHz e 5GHz.E considerado um padrão novo com uma recente tecnologia, MIMO (multiple input, multiple output), que usa diversas antenas para transferência de dados de um lugar para outro, tem como benefício principal o aumento da largura da banda e o alcance.

Rufino (2005), em seus estudos destaca que possui duas formas de funcionamento de redes sem fio: Infraestrutura e Ad-Hoc. Rufino (2005) explica que o funcionamento baseado na infraestrutura deve ter um aparelhamento central de rede que facilite para a topologia uma administração dinâmica e que concentre todos os dispositivos em um ponto só.

Já o funcionamento Ad-Hoc, e baseado em redes ponto-a-ponto onde que os dispositivos sem fio interatuam espontaneamente um com o outro, sem ter a obrigação de utilizar um ponto de acesso. A prerrogativa desse tipo de rede é a singeleza de se trocar arquivos sem a obrigação de ter especificação para utilizá-lo (RUFINO,2005).

Marques (2001) e Barrozo (2009), destaca alguns benefícios da rede 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 (MARQUES,2001; BARROZO,2009).

Barrozo (2009), cita em seus estudos 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.

3. CRIPTOGRAFIAS VINCULADAS AS REDES WI-FI.

Para que possa entender sobre criptografias relacionadas as redes WI-FI, primeiramente deve-se saber do que se trata o conceito de *Criptografia*. A palavra criptografia deriva do grego *kryptos = secreto e graphia = escrita,* com a junção das palavras temos *"*escrita secreta" (COSTA,2010*).*

De acordo com o dicionário Houaiss (2020):

> Criptografar significa cifrar um texto, reproduzi-lo em código não conhecido, tornando-o, desse modo, intencionalmente ininteligível para os que não têm acesso às suas convenções (HOUAISS,2020).

Costa (2010), afirma que a criptografia tem como objetivo ocultar o conteúdo da mensagem e torná-lo inelegível para qualquer pessoa que não tenha o conhecimento do método, impedindo que qualquer um possa inverter o processo.

3.1. Criptografias em redes WI-FI: WEP, WPA, WPA2, WPA-PSK, WPA2-PSK.

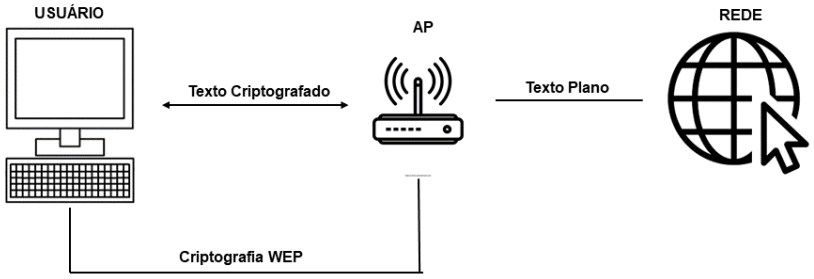
Como descrito anteriormente a criptografia de redes e a segurança dos dados transmitidos ou recebidos de uma determinada mensagem. Com base nisso será descrito neste estudo a seguir cincos tipos de criptografias em redes e explicar cada uma delas neste capítulo.

3.1.1 WEP

Wired Equivalent Privacy (Privacidade equivalente aos fios), foi o primeiro protocolo de segurança embutido no padrão IEEE 802.11 em 1999. Ele fornece dois tipos de autenticação de aparelhos, usa CRC-32 (Cyclic Redundacy Checks) para processar a integridade de dados e utiliza o algoritmo de criptografia RC4 (Ron`s Code #4) para precaver a interpretação de dados dos usuários que transitam na rede (LINHARES; GONÇALVES,2007).

O WEP pode ser usado entre o Ponto de Acesso (AP – Acess Point) e os usuários da rede (modo com infraestrutura), deste modo como na comunicação direta entre usuários (Modo AD-HOC). De acordo com a Figura 1, a criptografia WEP é inserida ao deslocamento do canal de comunicação sem fio, assim sendo, o deslocamento roteado para o lado de fora da rede sem fio não possui segurança WEP.

Figura 1 – WEP



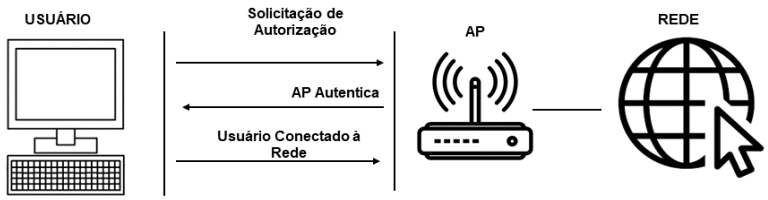
Fonte: (LINHARES; GONÇALVES,2007).

O padrão IEEE 802.11 estabelece dois tipos de autenticação WEP: Sistema Aberto (Open System) e chave compartilhada (Shared Key). O Sistema Aberto consente que algum dispositivo se conecte a rede. Para isto, é preciso comunicar o SSID (Service Set Identifier) da rede (i.e nome da rede). O SSID é capaz de ser adquirido por meio de pacotes do tipo BEACON (LINHARES; GONÇALVES,2007).

Gonçalves e Linhares (2007) afirmam que: “Estes pacotes não possuem criptografia e são enviados periodicamente em *broadcast* pelo Ponto de Acesso. Além do SSID, estes pacotes contêm outras informações sobre a rede como por exemplo, o canal de transmissão, a taxa de transmissão etc.”.

A figura 2 demonstra o processo de autenticação WEP sistema aberto. O aparelho solicita uma autenticação ao Ponto de Acesso, que envia uma mensagem autorizando a autenticação. Logo, o usuário se associa ao ponto de acesso, conectando-se com a rede.

Figura 2 - Sistema Aberto (Open System) – Autenticação WEP

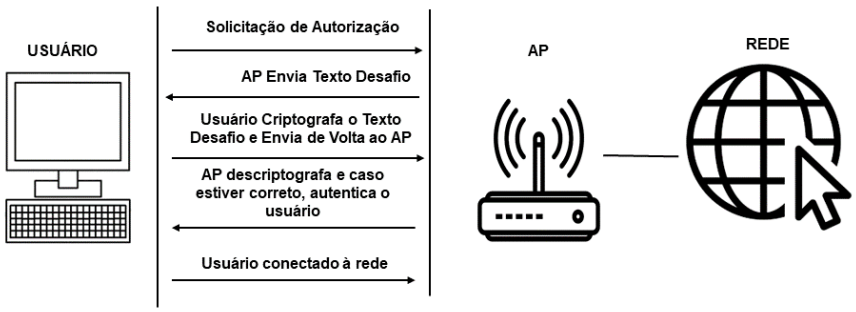


Fonte: (LINHARES; GONÇALVES,2007).

A autenticação por chave compartilhada solicita que o usuário e o ponto de acesso tenham uma mesma chave. O procedimento de autenticação por chave compartilhada será demonstrado na figura 3. O usuário manda um pedido de autenticação ao ponto de acesso, que logo envia ao usuário um texto-plano (sem criptografia). Esse texto é denominado de texto-desafio (Challenger Text) (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007), destaca que o usuário utiliza sua chave pré-configurada para criptografar o texto-desafio, retornado o resultado ao ponto de acesso. O AP o descriptografa com sua chave e equipara o texto obtido com o texto-desafio original enviado. Se o texto estiver correto, o usuário será autenticado na rede.

Figura 3 - Chave Compartilhada (Shared Key) – Autenticação WEP



Fonte: (LINHARES; GONÇALVES,2007).

Para a averiguação da inteireza das mensagens recebidas, o WEP acrescenta à mensagem a ser enviada um ICV (Integrity Check Value). O ICV consiste em um típico CRC acrescentado a mensagem original anterior a criptografia realizada. Ao

obter uma mensagem, um usuário ou AP a decodifica e computa o CRC- 32 da mensagem, aferindo- o com o CRC – 32 comunicando no campo ICV. Se acontecer de serem diferentes, a mensagem será descartada (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007) reiteram ainda que, para transformar as mensagens sigilosas, o WEP usa o algoritmo criptográfico RC4. Somente a mensagem e o ICV são criptografados. O começo 802.11 é passado em claro. O WEP usa um vetor de início (IV – Initialization Vector) sendo ele uma chave de 24 bits, no início, dinâmico.

De acordo com a norma IEEE 802.11, a chave WEP padronizada de 64 bits a ser usada pelo RC4 é aperfeiçoada pelo IV de 24 bits concatenado à chave estática de 40 bits (compartilhada pelos dispositivos). O RC4 é dividido em dois algoritmos: Key-Scheduling Algorithm (KSA) e Pseudo-Random Generation Algorithm (PRGA). O KSA consiste em inicializar um array de 255 posições com valores de 0 a 255 (LINHARES; GONÇALVES,2007).

Posteriormente, será executado uma serie de swaps, permutando o array. Esta permutação é realizada de acordo com a chave, chaves díspares permutam o array de formas desiguais. O PRGA executa um swap e cria um byte como saída que será usado na operação XOR (LINHARES; GONÇALVES,2007).

Borsc (2005), explica que a criptografia de cada mensagem com seu ICV deve gerar um novo IV, promovendo-o de um local para impedir repetição das chaves. Sendo que, o RC4 é um algoritmo de criptografia simétrico, a própria chave pode ser usada para o procedimento de decodificação. Por isso o IV é encaminhado em claro concatenado à mensagem criptografada, esse procedimento é também conhecido como encapsulamento WEP.

Boland (2004), destaca e lista em seus estudos as principais vulnerabilidades apresentadas pelo protocolo WEP, tais como:

- *Tamanho da chave*: Chave estática WEP originalmente era de apenas 40 bits. Chaves com esse tamanho de acordo com Boland (2004), podem ser quebradas pela força bruta das máquinas atuais;
- *Reuso de Chaves*: Os 24 bits do IV consiste em pouco mais de 16,7 milhões de vetores diferentes, número relativamente pequeno. Pois, de acordo com a quantidade de tráfego da rede os IVs irão se repetir de a cada momento e, por isso as chaves do RC4 também irão se repetir;

- *Gerenciamento de Chaves*: O WEP não utiliza de um protocolo para o gerenciamento de suas chaves. Por isso, as chaves usadas pelos dispositivos não conseguem ser trocadas dinamicamente, dificultando a manutenção das redes;
- *IV passado em claro*: Boland (2004), explica que o vetor de inicialização é decorrido em claro uma vez que ele é indispensável para o procedimento de decodificação. Como o IV é a primeira parte da chave, passa-se em claro uma porcentagem da chave que codificou o pacote;
- *Protocolo de autenticação ineficiente*: O modo de autenticação por Chave Compartilhada o invasor pode através de uma escuta de tráfego ter acesso a um pacote em claro e a sua cifra. Sendo possível achar os keystreams e utilizá-los para inventar uma resposta certa para qualquer texto-desafio;
- *Negação de Serviço (DoS – Deny of Service)*: é possível criar pacotes do tipo De-Authetication e encaminhá-los em broadcast ou espontaneamente para um determinado usuário utilizando o seu endereço MAC associado.

3.1.2 WPA

A fragilidade do WEP, foi necessário realizar um trabalho em conjunto para desenvolver um novo protocolo de segurança para as redes sem fio. A resultância desse incremento foi a criação do protocolo IEEE 802.11i, conhecido como WPA (DANTU, CLORHIER, ATRI;2005).

Para melhorar a aceitação do WPA, foi criado um consorcio de empresas do setor de redes sem fio, chamado de *WI-FI Alliance*. O objetivo do consorcio era realizar a criação de subconjuntos de protocolos de criptografia, para serem empregues sob esse novo protocolo de segurança, ainda em fase de desenvolvimento, o IEEE 802.11i (MEDEIROS,2017).

Enquanto os subconjuntos estavam sendo desenvolvidos, a *WI-FI Alliance*, para acalentar as críticas acendidas no meio corporativo em relação ao WEP, apresentou em 2003 um padrão denominado *Wifi Protected Access (WPA)* (LINHARES; GONÇALVES,2007).

O WI-FI Protected Access (WPA), foi elaborado para poder resolver os problemas do WEP. E capaz de ser utilizado com chaves compartilhadas, como no

WEP, ou usando o padrão 802.1x, e EAP (Extensible Authentication Protocol) que consegue achar usuários por meio de certificados digitais (STANGARLIN; FILHO,2014).

Linhares e Gonçalves (2007), afirma que o WPA é baseado no RC4 e em um subconjunto de particularizações exibidas em uma versão preliminar (draft) do IEEE 802.11i. O WPA tem capacidade de resolver diversos problemas de segurança associados ao WEP, tais como*: regras para o IV e IV estendido de 48 bits*, *novo código para verificação de mensagens*, *distribuição e derivação de Chaves etc.*

Em concordância aos benefícios do WAP de acordo com Linhares e Gonçalves (2007) são: faz o uso do conceito de chaves temporais, ao qual possui uma hierarquia de chaves. Possui uma chave principal, denominada de *Pairwise Master Key* (PMK), de onde se cria outras chaves como a chave de criptografia de dados; trabalha em dois modos diferentes de funcionalidade, um destinado a redes domésticas e micro escritórios, e outro destinado a rede de grandes instituições (redes corporativas); não possui suporte a redes do tipo ad hoc de maneira diferente ao WEP etc.

Conforme análise, possui dois tipos de autenticação no protocolo WPA. Um está voltado para redes corporativas que usa um servidor de autenticação 802.1x/EAP, ou seja, uma infraestrutura complementar, outro mais simplificado, criado para micros redes em escritório e para redes domésticas. Estes dois tipos de autenticação são conceituados como WPA Corporativo e WPA pessoal (LINHARES; GONÇALVES,2007).

O WPA Corporativo, o AP não é responsável por nenhuma autenticação. A autenticação do usuário e a do dispositivo é realizada por um servidor de autenticação. Ele usa uma infraestrutura complementar composta por um servidor que utiliza o protocolo de autenticação 802.1x em parceria com algum tipo de EAP (Extensible Authentication Protocol) (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007), explicam que quando um usuário requer uma autenticação, o servidor de autenticação confere em sua base de dados se as credenciais expostas pelo solicitante são verídicas, se forem válidas o usuário será autenticado e uma chave denominada de Master Session Key (MSK) será enviada.

Linhares e Gonçalves (2007), também explicam que no WPA Pessoal, somente um usuário comum não pode ser capaz de instalar e realizar a manutenção de um servidor de autenticação. Por isso, foi necessário criar o WPA-PSK (WPA-Pre Shared

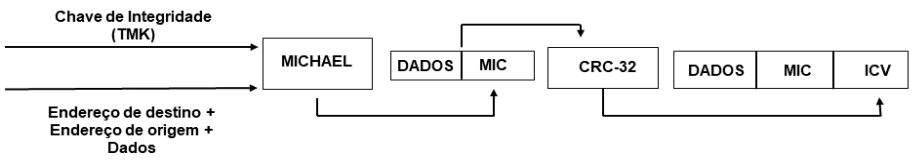
Key) que consiste em uma *passphrase* (frase senha) antecipadamente compartilhada entre os AP e o usuário. Sendo assim, a autenticação e realizada pelo AP, e a chave e configurada de forma manual em cada equipamento que pertence a rede, podendo variar de 8 a 63 caracteres ASCII.

Se tratando de integridade, a segurança do WPA consiste em dois valores. O ICV que também é utilizado no WEP e o MIC (Message Integrity Check). No MIC é implementado o algoritmo denominado Michael.

Segundo Linhares e Gonçalves (2007), a função do Michael se trata de uma função hash não linear, o que o difere do CRC-32. Para produzir o MIC é inserido no Michael o endereço de destino, de origem, a prioridade, os dados e uma chave integradora. Sua saída corresponde a 8 bytes que junto com o ICV constituem a integridade do protocolo WPA.

Sendo assim, sua integridade e formada por um total de 12 bytes, 8 gerados pelo Michael e 4 pelo CRC-32. A figura 4 demonstra o processo de integridade no WPA.

Figura 4 - Integridade WPA



Fonte: (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007), citam as principais desvantagens do WPA, tais como: *Fraqueza no algoritmo de combinação de Chave; PSK é suscetível a ataques de dicionário e Negação de serviço.*

3.1.3 WPA2

O padrão IEEE 802.1 li, foi validado em junho de 2004, com o objetivo de fornecer mais seguridade na comunicação (LINHARES; GONÇALVES,2007). O WPA2 é o padrão IEEE 802.1 li, na sua configuração final, sendo que o WPA é a

implementação de parte do padrão. Segundo Caixeta (2012), o WPA2 foi criado para adquirir um nível de segurança absoluto, ainda maior do que o WPA.

Caixeta (2012), afirma que a maior novidade do WPA2 é a substituição do método criptográfico do WPA pelo método AES-CCMP (Couter-Mode / CBC MAC Protocol). Esse modo consiste em cifragens de bloco. Ele não permite que a mesma chave seja utilizada para criptografia e autenticação.

A autenticação no WPA2 é, de forma resumida, o mesmo do WPA. Quando um indivíduo se autentica, há uma sequência de mensagens modificadas entre o AP e o usuário. Essa troca de mensagens adota um delongamento no processo de conexão (LINHARES; GONÇALVES,2007).

Para Linhares e Gonçalves (2007),

> Quando um usuário se desloca de um AP para outro, o atraso para estabelecer associação pode causar uma interrupção notória da conexão, principalmente em tráfego de voz e vídeo. Para minimizar este atraso de associação, o equipamento pode dar suporte a PMK *Caching* e *Preauthentication*. O PMK Caching consiste no AP guardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o AP, estas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já no *Preauthentication*, enquanto o cliente está conectado a um AP principal, ele faz associações com outros APs cujo sinal chega até ele. Desta forma, quando há uma mudança de AP não há perda de tempo com a autenticação (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007), se tratando sobre a integridade do WPA2, destaca que o protocolo CCMP (Counter -Mode/Cipher Block Chaining Message Authentication Code Protocol) é responsável por sua segurança e confidência. O CCMP é fundamentado no AES (Advanced Encryption Standard) que se trata de uma cifra de bloco. Suas chaves e os blocos são de 128 bits. Esse protocolo também é embasado no conceito de chaves temporais, como o TKIP no WPA.

Entretanto, no WPA2 há uma ordem de chaves, no qual as derivações da PMK criam as chaves temporais de criptografia de integridade. O algoritmo responsável pela segurança do frame é o AES Counter Mode (CTR). Possui chave de criptografia de dados simétrica e de tamanho de 128 bits, onde que seu vetor de inicialização permanece com 48 bits (LINHARES; GONÇALVES,2007).

Linhares e Gonçalves (2007), citam as principais desvantagens do WPA2, tais como: Negação de serviço e o PSK pequeno.

3.1.4 WPA-PSK

A versão doméstica do WPA pode ser chamada de WPA Personal ou WPA-PSK (Pre Shared Key). Nesta versão, cada usuário de rede wireless autentica com o ponto de acesso usando a mesma chave de 256 bits criada através de uma senha ou frase secreta. Essa função foi projetada para uso de redes pequenas e que não requer de um servidor para autenticação (LINHARES; GONÇALVES,2007).

De forma mais clara, o WPA-PSK se trata de uma criptografia forte, na qual as chaves de criptografia (TKIP) e constantemente alterada. Forma que garante a seguridade dos usuários, protegendo-os de ataques hackers (FERREIRA,2003).

3.1.5 WPA2-PSK

O WPA2-PSK (PSK acronym for Pre-Shared Key), é a evolução do protocolo WPA. Ele implementa um algoritmo baseado em uma chave de 8 a 63 caracteres, no qual de forma aleatória suas chaves são criadas e usadas para autenticação. Sua criptografia é extremamente forte e resistente a ataques (LÓPEZ,2015).

4. MATERIAIS E MÉTODOS

Esse estudo se trata de uma pesquisa bibliográfica de caráter qualitativo. A pesquisa Qualitativa é uma metodologia de caráter exploratório. Seu foco está no subjetivo do objeto analisado. Neste método as respostas costumam não ser objetivas e os resultados obtidos não são contabilizados em números exatos (ROCHA,2013).

Para Neves (2015), 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), diz que independente da maneira de como os dados foram colhidos, eles têm que ser investigados e examinados cautelosamente. 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).

Rossman e Rallis (1998, apud. Creswell, 2007), 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,1998 apud CRESWELL,2007).

A escolha da pesquisa qualitativa se deu pela forma investigativa do estudo, que tem como objetivo principal analisar a importância da segurança da informação em redes de Wi-Fi e descrever o papel da Tecnologia da Informação (TI) diante do processo de segurança em redes. Para tal, foi realizado um levantamento bibliográfico com os principais autores que permeiam sobre a Segurança da informação em redes WI-FI e descrito de forma clara e objetiva a ideia principal de cada autor assim como seus pontos de vistas.

Neste estudo não foi realizado a aplicação de questionários e sim a explanação e descrição das ideias principais de diversos autores que defendem a Segurança da Informação em redes WI-FI, assim como também, foi realizado a discussão dos resultados obtidos.

5. RESULTADOS E DISCUSSÃO

A Tecnologia da Informação perante a Segurança da Informação em redes, tem como prioridade a proteção da informação, visto que seus objetivos principais é garantir a segurança dos dados digitais, a integralidade, a confidencialidade, a disponibilidade e assim como também garantir a autenticidade das redes, de forma que preserve o usuário de possíveis ataques.

Beal (2005) e Sêmola (2003), conceituam a Segurança da Informação 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 (2005), 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 (2004), completa a fala de Beal (2005), 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.

A Segurança da Informação em redes WI-FI, 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.

É de suma importância que os profissionais de Segurança da Informação 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 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. 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.

De acordo com Linhares e Gonçalves (2007), 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.

Henriques (2019), destaca em seus estudos 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.

Assim sendo, foi possível destacar neste estudo a suma importância da Tecnologia da Informação (TI), assim como também a importância de profissionais capacitados e voltados para a Segurança da Informação em redes Wi-Fi, com o objetivo de monitorar constantemente a rede, detectando possíveis ameaças antes que elas possam causar danos dolosos às Instituições e aos usuários.

6. CONSIDERAÇÕES FINAIS

Após estudar mais afundo sobre a Importância da Segurança da Informação, podemos concluir que a Tecnologia da Informação (TI), tem uma grande responsabilidade em relação a Segurança. A segurança da Informação surgiu com a necessidade de evitar ataques e perda de dados informacionais dos usuários domésticos e corporativos. Cujo seu objetivo é garantir a veracidade da segurança dos dados, a integridade, a confidencialidade e a disponibilidade de toda a informação.

As informações contidas em instituições são de extrema importância e devem ser guardadas rigorosamente, mesmo não tendo acesso direto aos dados, um breve acesso nas redes wireless já disponibiliza para indivíduos mal-intencionados uma grande oportunidade de se aproveitar das informações ali contidas. Foi possível observar durante este estudo que os profissionais da Segurança da Informação devem se ater constantemente nos dispositivos de redes WIFI, aperfeiçoando a segurança deles através da criptografia de redes, com o intuito de evitar perdas de informações sigilosas como possíveis invasões.

Para evitar essas situações, foi demonstrado no estudo a importância do uso de protocolos de segurança como a criptografia, onde se pode proteger os dados com maior eficácia e garantir uma maior segurança. Sendo o protocolo WPA2 o mais seguro até o momento e é usado nas instituições corporativas porque sua quebra de senha e praticamente impossível devido ao fato que sua certificação seja AES.

Após avaliar cada tipo de tecnologia, podemos concluir que existem várias formas de se fornecer segurança em ambientes wireless. Cada procedimento deve ser estudado e analisado para se ter certeza de qual atenderá ao tipo de ambiente. Não existe o método exato, e sim aquele que calha melhor ao tipo de necessidade.

Regras básicas devem ser seguidas em qualquer tipo de ambiente, seja ele corporativo ou doméstico. Cabe a equipe de Segurança da Informação se manter atenta a qualquer situação de vulnerabilidade da informação e buscar cada vez mais métodos inovadores para a proteção da informação.

6.1 Trabalhos futuros

Podemos abordar melhor em trabalhos futuros os estudos da criptografia AES tendo em vista outros modelos que irão surgir futuramente em meio ao ramo

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 podemos esperar outros avanços da criptografia para evitar que esse tipo de ação seja aceito facilmente no intuito da coleta de dados informacionais.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 17799:2005 – **Tecnologia da Informação – Técnicas de Segurança — Código de prática para a gestão da segurança da informação**. Requisitos. ABNT, 2005.

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

BARROZO, Leandro Lavagnini. **Segurança nas redes sem fio: Wireless e Wimax**. 2009. 56 Trabalho de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2009.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

Boland, H.e Mousavi, H., 2004. **Security issues of the IEEE 802.11b wireless LAN. Electrical and Computer Engineering**, 2004. Canadian Conference on. Vol. 1, pp 333 – 336.

Borsc, M.e Shinde, H., 2005. **Wireless security & privacy. Personal Wireless Communications**, 2005. ICPWC 2005. 2005 IEEE International Conference on. pp 424 – 428.

BUSCH, **Jade, Wired ou Wireless, 2008**, disponível em: http://jaderedes.blogspot.com.br/2008/11/wired-ou-wireless.html - Acessado em 13/10/20.

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.

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

CRESWELL, J. W. **Projetos de pesquisa: métodos qualitativo, quantitativo e misto**. 2. ed. Porto Alegre: Bookman, 2007.

DANTU, R.; CLOTHIER, G.; ATRI, A. **EAP methods for wireless networks**. Elsevier, p. 13, 2005.

FARIAS, Paulo César Bento. **Rede Wireless**. 2005, Disponível em: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp -Acessado em 20/10/2020.

FERNANDES, Guilherme Augusto; PINHO, João Gilberto et al., **A IMPORTÂNCIA DA SEGURANÇA DE REDES NO CENÁRIO ATUAL: ESTUDO COM O MÉTODO DELPHI**. XXXV ENCONTRO NACIONAL DE ENGENHARIA DE PRODUCAO Perspectivas Globais para a Engenharia de Produção Fortaleza, CE, Brasil, 13 a 16 de outubro de 2015.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003. 162 p.

Goldenberg, M. (1997) **A arte de pesquisar - como fazer pesquisa qualitativa em Ciências Sociais**.R.J.- S.P.: Ed. Record.

GORDON, L. A.; LOEB, M. P. **The economics of information security investment**. ACM Transactions on Information and Systems Security, v. 5, n. 4, p. 438–457, nov. 2002.

HENRIQUES, Pedro. **A segurança da informação e a proteção da rede wifi. Indicca.com**. Rua Santo Antônio, 990, sala 603, Centro, Juiz de Fora, MG, CEP 36016-210. 2019. Disponível em: https://indicca.com.br/a-seguranca-da-informacao-e-a-protecao-da-rede-wifi/. Acessado 25/10/2020.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro, Ed. Objetiva, 2020.

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,2007.

López, H. A., Marques, E. R. B., Martins, F., Ng, N., Santos, C., Vasconcelos, V. T., and Yoshida, N. (2015). **Protocol-based verification of messagepassing parallel programs**. In OOPSLA, pages 280–298, New York, NY, USA. ACM.

MARQUES, Alexandre Fernandez. **Segurança em rede IP. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados**. Londrina: ASIT, 2001. MENDES, Douglas R. Redes de Computadores: Teoria e prática. SP: Novatec Editora.

MEDEIROS, Roger Casagrande de. I**mplementação de um Modelo de Segurança para Rede Sem Fio WPA2-EAP**. Universidade Regional do Noroeste do Estado do Rio Grande do Sul – Santa Maria, 2017.

MENDES, Osvane. **Wi-Fi, 2008**. Disponível em: http://osvanewireless.blogspot.com.br/2009_08_01_archive.html - Acessado em 23/10/2020.

MIRANDA, Antônio. **Redes Wi-Fi 802.11 o que é?** 2013, Disponível em: http://antoniomjf.wordpress.com/2013/08/24/redes-wi-fi-802-11-o-que-e-e-seuspadroes/ - Acessado em 26/10/2020.

NEVES, Miranilde Oliveira. **A importância da Investigação Qualitativa no Processo de Formação continuada de professores: Subsídio ao Exercício da Docência**. Revista Fundamentos, V.2, n.1, 2015. Revista do Departamento de Fundamentos da Educação da Universidade Federal do Piauí. ISSN 2317-2754.

POSTHUMUS, Shaun; VON SOLMS, Rossouw. **A Framework for the Governance of Information Security**. Computers & Security, v.23, n.8, p.638-646, dez.2004.

ROCHA, Hugo. **O que é Pesquisa Qualitativa, tipos, vantagens, como fazer e exemplos.** Disponível em: https://klickpages.com.br/blog/o-que-e-pesquisa-qualitativa/. Acessado 10/11/2020.

Rossman, G. B., & Rallis S. F. (1998). **Learning in the field: An introduction to qualitative research**. Thousand Oaks, CA: Sage Publications.

RUFINO, Nelson Murilo de O**. Segurança em redes sem fio**. 2. Ed. São Paulo: Novatec, 2005.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

SILVA, Pedro Tavares Silva; CARVALHO, Hugo; TORRES, Catarina Botelho; **Segurança em sistemas de informação: gestão estratégica da segurança da empresa real**. Portugal: Centro Atlântico: s.n., 2003.

STANGARLIN, Douglas Pegoraro; FILHO, Walter Priesntz. **Análise de Desempenho de Redes sem Fio com diferentes protocolos de criptografia**. Universidade Federal de Santa Maria – 2014.

YIN, R. Estudo de Caso: **Planejamento e Métodos**. Porto Alegre: Bookman, 2015.