ESCOLA DE SARGENTOS DAS ARMAS
ESCOLA SARGENTO MAX WOLF FILHO
CURSO DE COMUNICAÇÕES

Emanuel Luan Bronze Costa
Felipe Rodrigues dos Santos
Gabriel Leão Fernandes Júlio
Humberto Faria Guedes
Matheus Freitas
Nícolas Antônio Fonseca dos Passos
Tiago Henrique Guedes Menezes
Weslley Cunha Lima

A IMPORTÂNCIA DA CRIPTOGRAFIA PARA O SIGILO DAS INFORMAÇÕES NOS APLICATIVOS

TRÊS CORAÇÕES – MG
2022

Emanuel Luan Bronze Costa
Felipe Rodrigues dos Santos
Gabriel Leão Fernandes Júlio
Humberto Faria Guedes
Matheus Freitas
Nicolas Antônio Fonseca dos Passos
Tiago Henrique Guedes Menezes
Weslley Cunha Lima

A IMPORTÂNCIA DA CRIPTOGRAFIA PARA O SIGILO DAS INFORMAÇÕES NOS APLICATIVOS

Projeto de pesquisa do Curso Superior de Tecnologia em Gestão de Comunicações Militares apresentado à Escola de Sargentos das Armas como requisito para a obtenção do título de Tecnólogo em Ciências Militares

Orientador: Capitão **Fábio** Henrique **Rodrigues**

Área de concentração: Ciências Militares

TRÊS CORAÇÕES – MG
2022

ESCOLA DE SARGENTOS DAS ARMAS
ESCOLA SARGENTO MAX WOLF FILHO
FOLHA DE APROVAÇÃO

Emanuel Luan Bronze Costa
Felipe Rodrigues dos Santos
Gabriel Leão Fernandes Júlio
Humberto Faria Guedes
Matheus Freitas
Nicolas Antônio Fonseca dos Passos
Tiago Henrique Guedes Menezes
Weslley Cunha Lima

A IMPORTÂNCIA DA CRIPTOGRAFIA PARA O SIGILO DAS INFORMAÇÕES NOS APLICATIVOS

Projeto de Pesquisa do Curso Superior de Tecnologia em Gestão de Comunicações Militares apresentado à Escola de Sargentos das Armas como requisito para a obtenção do título de Tecnólogo em Ciências Militares.

DATA: _____/_____/_____ APROVADO ( ) REPROVADO ( )

BANCA EXAMINADORA

_____

Orientador: Capitão **Fábio** Henrique **Rodrigues**

RESUMO

Este trabalho aborda um tema muito discutido tanto no contexto civil como militar, pois ao explanar sobre o Sistema Criptográfico e Segurança das Comunicações, deseja-se apresentar a importância para aqueles que não possuem conhecimento, bem como reforçar a relevância para quem detém domínio deste assunto. Este trabalho visa dissertar a maneira como o sistema criptográfico contribui para a confidencialidade das informações. A criptografia é de extrema importância para o sigilo e segurança das informações e comunicações de aplicativos, sistema computacionais, empresas, organizações militares, tendo em vista a possibilidade de vazamentos de dados feito por cibercriminosos e de algum inimigo interno ou externo. A metodologia utilizada foi a de revisão bibliográfica, junto ao estudo exploratório, para isso foi adotado como apoio, alguns autores: Gil (2008); Vergara (2009); entre outros. Este trabalho, tendo como tema "Sistema Criptográfico e Segurança das Comunicações", faz conexão à Segurança da Informação que está diretamente relacionada à proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou coletivo. Para isso, deve oferecer confidencialidade, integridade, sigilo, disponibilidade, autenticidade e legalidade. Tendo em vista a constante evolução da Tecnologia da Informação e Comunicação, percebe-se que o uso da criptografia, um mecanismo de segurança, é extremamente necessário para a proteção das informações e das comunicações no âmbito civil e militar.

Palavras-chave: Criptografia. Segurança. Informação.

ABSTRACT

This work addresses a topic much discussed both in the civil and military context, because when explaining the Cryptographic System and Communications Security, it is desired to present the importance for those who do not have knowledge, as well as reinforce the relevance for those who have mastery of this subject. This work aims to discuss the way in which the cryptographic system contributes to the confidentiality of information. Encryption is extremely important for the secrecy and security of information and communications from applications, computer systems, companies, military organizations, in view of the possibility of data leaks made by cybercriminals and an internal or external enemy. The methodology used was the bibliographic review, together with the exploratory study, for which some authors were adopted as support: Gil (2008); Vergara (2009); among others. This work, with the theme "Cryptographic System and Communications Security", makes connection to Information Security that is directly related to the protection of a set of data, in the sense of preserving the value they have for an individual or collective. For this, it must offer confidentiality, integrity, secrecy, availability, authenticity and legality. In view of the constant evolution of Information and Communication Technology, it is clear that the use of cryptography, a security mechanism, is extremely necessary for the protection of information and communications in the civil and military scope.

Keywords: Encryption. Safety. Information.

LISTA DE FIGURAS

LISTA DE SIGLAS

LGPD	Lei Geral de Proteção de Dados
IOT	*Internet Of Things* – Internet das Coisas
DES	*Data Encryption Standard* - Padrão de Criptografia de Dados
EB	Exército Brasileiro
IBM	*International Business Machines Corporation* - Corporação Internacional de Máquinas para Negócios
AES	*Advanced Encryption Standard* - Padrão de Criptografia Avançada
ECMP	*Encrypted Mobile Content Protocol* - Protocolo de Conteúdo Móvel Criptografado
LAN	*Local Area Network* - Rede local
WEP	*Wired Equivalent Privacy* - Privacidade Equivalente com Fio
WAP	*Wi-fi Protected Access* - Acesso Protegido por Wi-Fi
WPA2	*Wi-fi Protected Access 2* - Acesso Protegido Wi-Fi 2
TKIP	*Temporal Key Integrity Protocol* – Protocolo de Integridade de Chave Temporal
NIST	*National Institute of Standards and Technology* -Instituto Nacional de Padrões e Tecnologia
RSA	Rivest, Shamir e Adlema

SUMÁRIO

INTRODUÇÃO

Este trabalho tem como tema o Sistema Criptográfico e Segurança das Comunicações, tendo em vista seu vasto contexto. Por isso, esta pesquisa foi delimitada para: A Importância da Criptografia para o Sigilo das Informações nos Aplicativos, um assunto de suma importância para o meio militar, uma vez que um dos objetivos do Exército Brasileiro (EB) é manter os sistemas de proteção contra-ataques virtuais atualizados, utilizando como estratégia essencial para a sobrevivência das corporações.

Criptografar é criar um método que possibilite transformar uma mensagem em código (cifra) que, caso seja interceptada, fique difícil a interpretação da informação contida na mensagem. A partir da codificação e decodificação de dados, é possível estabelecer uma comunicação segura, confidencial, que garanta a autenticidade do emissor e a integridade do receptor. Esse sistema permite que os dados transmitidos sejam armazenados sem sofrer alterações e sem serem expostos, a não ser por quem detenha a chave de acesso seguro.

Dessa forma, esta pesquisa é uma Revisão Bibliográfica, conectada ao estudo qualitativa, em que tem como objetivo geral: ressaltar a necessidade do sistema criptográfico para a segurança das comunicações, tendo em vista que com o avanço da tecnologia da informação, a questão da privacidade, anonimato e segurança de transmissões de dados aumentou a importância da criptografia. O seu impacto na esfera social, econômica e cultural tem dado situações sem precedentes e que serão discutidas neste projeto.

Além disso, este trabalho tem a finalidade de responder a seguinte questão norteadora: como o sistema criptográfico contribui para a confidencialidade das informações? Com o intuito de responder esta questão, no decorrer desta investigação, será abordada a grande importância da criptografia para a proteção de dados e documentos confidenciais, visando alguma tentativa de invasão ou roubo de informações, assim o sistema criptográfico tem a finalidade de os proteger, não só no âmbito militar, mas também no meio civil.

O primeiro relato que se tem da criptografia é datado de 1900 a.C e foi encontrado no Egito. Para demonstrar a importância histórica da criptografia no meio militar, vale-se destacar a Cifra de Cesar, a qual foi nomeada por conta do General Romano Júlio Cesar que foi fundamental na transformação de Roma em um império em 50 a.C. Esta era uma Cifra de Substituição cujo modo de criptografia consistia em substituir cada letra da mensagem pela letra que se encontrava três posições depois dela. Dessa maneira, essa cifra era utilizada para proteger as informações militares do Império Romano.

Já no meio civil, a importância da criptografia torna-se evidente com o advento da internet. Após vazamentos de dados nos meios sociais, em 2018 foi aprovada a Lei Geral de Proteção de Dados (LGPD) lei nº 13.709, entrando em vigência em agosto de 2020, que foi criada para manter o controle e proteção de dados pessoais, garantido ao cidadão a privacidade de informações particulares como nome, endereço, e-mail, idade, estado civil, obrigando os sites a informar como os dados serão tratados, armazenados e a finalidade da coleta de dados.

Desse modo, a razão principal do uso de criptografia está relacionada à segurança da informação, tendo em vista que cada vez mais os dados sigilosos de pessoas e empresas são alvos de ataques orquestrados por criminosos cibernéticos. Por isso, como forma de se proteger dessas investidas, usa-se a criptografia para “embaralhar” uma mensagem como forma de preservá-la em diversas situações.

JUSTIFICATIVA

A justificativa tem por finalidade refletir sobre a importância do sistema criptográfico e sobre a segurança das comunicações e é de suma relevância para o entendimento no que tange à importância da criptografia para o sigilo das informações nos aplicativos. Com o objetivo de abordar e explicar o trabalho apresentado, o tema retrata um relevante assunto para a proteção cibernética no seu expecto relativo ao uso de aplicativos.

O objeto de estudo traz grande relevância para o meio civil visto que, atualmente, o uso de aplicativos é muito presente nas empresas, escolas e outras instituições civis e tem-se a importância da criptografia no uso das informações desse meio. Ademais, no espectro militar, tem-se grande relevância a utilização desse meio como medida de coordenação e de controle da tropa no terreno, tendo como exemplo os aplicativos como “Zimbra”, “Sistema C2” e “SPED” de combate.

Para o âmbito acadêmico, os estudos apresentados mostram-se de grande relevância para o desenvolvimento de novas pesquisas acerca do assunto apresentado, pois a globalização revolucionou a forma de se comunicar e a proteção das informações se faz bastante crucial. Logo, estudar sobre Criptografia é um passo enorme para o desenvolvimento científico dessa área.

DESENVOLVIMENTO

Neste capítulo será abordado o desenvolvimento do Trabalho Científico, o qual leva em consideração o item 2.1 representando os Objetivos de forma clara e objetiva, em seguida o 2.2 Referencial Teórico, composto por citações diretas de pesquisadores nas quais fundamentam esta pesquisa, com finalidade de responder à questão norteadora qual foi trabalhada: A importância da criptografia para o sigilo das informações nos aplicativos. Posteriormente, o item tipo de pesquisa: revisão bibliográficas; e a trajetória Metodológica da Pesquisa: A primeira etapa desta investigação é buscar ressaltar e interpretar a importância do tema abordado e consolidar a pesquisa através de fontes, por meio do uso de artigos científicos, manuais, e livros de acervos virtuais e físicos, nos quais foi observada a importância da criptografia para a segurança dos softwares, sendo possível reduzir vazamentos, a perda e o roubo de dados e informações. Logo após, foi elaborada a segunda etapa, a qual consiste na coleta de dados, abordados através da leitura exploratória. E, para absorver o máximo de conteúdo, foi realizada a leitura analítica na terceira e na última etapa. Por fim, a pesquisa apresentou atributos descritivos por expor detalhadamente sobre: a importância da criptografia para o sigilo das informações nos softwares e permitir o entendimento mais aprofundado de um assunto pouco conhecido, mas bastante importante para a confidencialidade de dados.

OBJETIVOS

Objetivo geral:

- Ressaltar a necessidade do sistema criptográfico para a segurança das comunicações.

Objetivos específicos:

- Identificar os sistemas criptográficos disponíveis para utilização nas comunicações;
- Analisar as diversas maneiras que a segurança pode favorecer no emprego das comunicações;
- Verificar de que forma os invasores de rede podem acessar dados de comunicações caso o sistema criptográfico seja ineficaz.

REFERENCIAL TEÓRICO

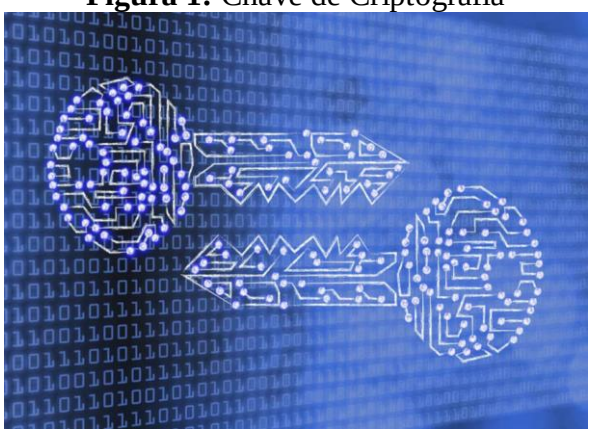
Criptografia é um conjunto de processos examinados para proteger uma informação que é trocada em um meio físico ou digital, para que somente o emissor e receptor consigam entender. Ela também pode ser entendida como uma ciência, de forma que esconda o assunto de pessoas indesejadas, fazendo com que somente o destinatário da mensagem consiga ler e compreender o conteúdo de maneira íntegra. Em outros termos, a criptografia transforma um texto original, também conhecido como *plaintext* (texto claro), em um texto cifrado, ou *cyphertext* (texto cifrado), que irá parecer informação randômica e ilegível. Para tal, é usada uma técnica de encriptação, chamada de cifra ou sistema criptográfico. Além disso, o processo de converter o texto claro no texto cifrado é chamado de cifração ou encriptação. O caminho contrário recebe o nome de decifração ou decriptação. (NICOLAU, 2003).

Conforme Coelho (2011), a criptografia pode ser entendida como "arte ou ciência de codificar informações, de modo a esconder o conteúdo original de pessoas indesejadas, permitindo que somente o destinatário da mensagem consiga lê-la e compreendê-la de forma íntegra", ou seja, ela transforma o *plaintext* (texto claro ou original) em *cyphertext* (texto cifrado), e assim a informação se tornará ilegível. Essa técnica é chamada de encriptação, comumente conhecida como cifra ou sistema criptográfico, já o caminho contrário tem o nome de decifração ou decriptação (NICOLAU, 2003; COELHO, 2011).

De forma sintetizada, a criptografia consiste em ocultar informações, convertendo dados em códigos que dificultam o entendimento e a leitura por pessoas não autorizadas. Desse modo, apenas quem envia e quem recebe a informação em uma determinada mensagem tem acesso ao que está escrito, ou então apenas quem tem a "chave" pode realizar a leitura de um documento.

A seguir, será apresentada a Figura 1, a qual representa a Chave de Criptografia.

Figura 1: Chave de Criptografia



Fonte: *Evaltec*, 2022

A Figura 1 é uma foto retirada do *site Evaltec*, a qual mostra duas chaves que fazem referência à criptografia (uma emissora e outra receptora). Assim, tal ilustração mostra a seguridade desse sistema, o qual surge para a proteção da identidade e dos dados do usuário, pois, havendo alguma tentativa de invasão, o sistema de criptografia protege todas as informações importantes: tanto os dados pessoais dos usuários, quanto o conteúdo de arquivos e de mensagens trocadas.

Levando em conta os recentes casos de vazamento de dados que promoveram escândalos na internet (*Netflix, Linkedin e MySpace*) e a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor a partir de agosto de 2020, torna-se notória a importância em aplicar a criptografia como medida de segurança no cenário corporativo.

Contudo, os usuários também estão expostos em ambiente doméstico, isso se tornou ainda mais recorrente após a Quarta Revolução Industrial- *Internet Of Things* (IOT)- que é a Internet das coisas. No cenário da sociedade atual, vive-se constantemente procurando ou compartilhando informações online, e, por isso, nossos dados estão sendo armazenados em servidores locais ou em sistema de nuvens. Tendo em vista que, em alguns casos, não se pode ter certeza de que a zona de armazenamento é segura, deve-se reforçar a importância de se proteger com criptografia e de aumentar sua segurança e sua privacidade no uso doméstico.

Nesse contexto, a necessidade de uso da criptografia está relacionada diretamente à proteção da identidade e dos dados do usuário. Havendo alguma tentativa de invasão, o sistema de criptografia protege todas as informações importantes: tanto os dados pessoais dos usuários, quanto o conteúdo de arquivos e de mensagens trocadas (ADIL, 2019). Sob esse aspecto, com a crescente quantidade de informações disponibilizadas pelo usuário, ocorreu que:

> No ano de 2018, cerca de 87 milhões de usuários pelo *Facebook*, rede social famosa na época pela divulgação de *fake news* eleitorais, foi afetada pelo repasse de informações ao *Cambridge Analytica* (empresa de consultoria política britânica) sem o devido consentimento e essas informações foram manipuladas incorretamente. Além disso, o *Facebook* se tornou uma das redes sociais menos confiável em questão de termos de privacidade, após expor fotos de mais de 6,8 milhões também no ano de 2018 (PINHEIRO, 2018).

Destarte, após esses casos, em 2020 entrou em vigor a Lei Geral da Proteção de Dados (LGPD), ressaltando a importância em aplicar a criptografia como medida de segurança no cenário corporativo. Logo, “em muitos casos não é possível ter certeza se o ambiente de armazenamento é seguro” (ADIL, 2019). Sendo assim, é importante reforçar o uso da

criptografia, aumentando a segurança das suas informações e a sua privacidade no uso doméstico.

2.1 OS SISTEMAS CRIPTOGRÁFICOS DISPONÍVEIS PARA UTILIZAÇÃO NAS COMUNICAÇÕES

Cipriano (2020) aponta que existem dois tipos de criptografia, que são nomeadas de simétrica e assimétrica. A simétrica tem o algoritmo e chave iguais, ou seja, o remetente e o destinatário usam a mesma chave. Algoritmo de chave única, isto é, para criptografia simétrica, mais difundido é o DES (*Data Encryption Standard*). Esse algoritmo foi desenvolvido pela IBM (*International Business Machines Corporation*) e é adotado como um padrão nos Estados Unidos desde 1977.

O algoritmo DES trabalha codificando blocos de 64 *bits*, usando uma chave de 56 *bits* mais 8 *bits* de paridade. Para quebrar o DES pela força bruta, isto é, tentar todas as combinações possíveis de chave, como é uma chave de 56 *bits*, temos um total de 2 elevado a 56 chaves possíveis.

A respeito da criptografia assimétrica, Cipriano (2020) explica que:

> A criptografia assimétrica utiliza uma chave (pública) para encriptar e outra (privada) para decriptar. Podemos dizer que, ao invés de compartilhar uma chave secreta, utiliza-se duas chaves matematicamente relacionadas. [...] Criptografia assimétrica é usado com maior frequência na Internet, pois é mais viável tecnicamente, pois não sabemos previamente onde serão enviados os dados (CIPRIANO, 2020, p.15).

O algoritmo de chave pública, para criptografia assimétrica mais difundido é o RSA (significa o nome dos autores: Rivest, Shamir e Adleman). Sua segurança se baseia na intratabilidade da fatoração de produtos de dois números primos. Se fosse usado a criptografia simétrica, poderíamos ter grandes problemas, pois, para distribuir a chave para todos os usuários autorizados, teríamos um problema de atraso de tempo e possibilitaria também que a chave chegasse a pessoas não autorizadas, logo, teria redução da segurança e do processamento de dados.

No caso dos aparelhos como celulares e *tablets*, há um perigo maior de vazamento de dados, já que é bastante comum as pessoas fazerem uso de conexão *Wi-Fi* abertas. Nestes casos, qualquer usuário mal-intencionado pode reter dados navegando nestas conexões. É justamente por esta razão que é totalmente impróprio acessar aplicativos de bancos ou compras online

conectado em uma rede de *Wi-Fi* aberta. Também existe um grande uso de plataformas *mobile* e armazenamento de dados em nuvem através de data centers terceirizados e de servidores.

A criptografia de dados também é capaz de proteger as informações e trabalhos criados através de aplicativos como os de vazamento de dados de pessoas e companhias (MADE IN WEB, 2018). Em celulares e *tablets,* o vazamento de dados é bem comum de acontecer, pois é comum o uso de conexão em redes de *Wi-Fi* abertas, e qualquer usuário com más intenções pode reter dados navegando nestas conexões. O *site Made In Web* (2018) aponta que, por esse motivo, é impróprio o acesso a aplicativos de bancos ou de compras *online* nessas redes abertas.

2.2 FERRAMENTAS QUE A SEGURANÇA PODE FAVORECER NO EMPREGO DAS COMUNICAÇÕES

Tratando-se de criptografia de dados a nível militar, é utilizado o AES, a abreviação de *Advanced Encryption Standard* (Padrão de Criptografia Avançado), pois a criptografia de 256 *bits* tem um comprimento de chave de criptografia de 2^{265} (lê-se dois elevado a duzentos e sessenta e cinco).

Há 1.2×10^{77} (lê-se dez elevado a setenta e sete) possíveis combinações para que seja decifrada em uma única chave de criptografia. Após essa criptografia ter sido certificada pela *US National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia dos EUA) como uma proteção viável para defender os dados dos usuários, passou a ser comumente utilizada entre as Forças Armadas e os governos como forma de proteger as informações nacionais sigilosas.

No uso de chamadas por voz, em mensagens instantâneas e em outros conteúdos de dispositivos móveis, também pode ser utilizado o ECMP (*Encrypted Mobile Content Protocol*), o qual é responsável por otimizar a entrega de conteúdo criptografado em tempo real.

O sistema *Dual Cipher* da *Cellcrypt* usa o dobramento para maior segurança. Por exemplo, as chamadas de voz são primeiro criptografadas, usando RC4 com uma chave de 384 *bits* e, em seguida, criptografado novamente, usando AES com uma chave de 256 *bits*. (PROTECTSOFTWARE, 2021, p.1)

A seguir, será apresentada a Figura 2, a qual representa a Criptografia Militar:

Figura *2*: Criptografia Militar

Fonte: *The FastCode*, 2020.

A figura 2 é uma foto retirada do *site The FastCode*, a qual mostra dois militares programando um servidor com criptografia militar. Vale ressaltar que:

> No ano de 2001, o órgão Americano NIST, Instituto Nacional de Padrões e Tecnologia, (National Institute of Standards and Technology) recomendou um novo algoritmo de criptografia conhecido como *Advanced Encryption Standard* (AES), substituindo o algoritmo DES. O algoritmo AES suporta uma combinação de dados de 128 *bits* e chaves com o comprimento de 21 128, 192 e 256 *bits* (SINGH, 2013).

Utilizando o conceito de chave simétrica, se um terceiro interceptar a chave durante a transmissão, ele tem acesso às instruções para criptografar novas mensagens e descriptografar a informação cifrada enviada, inutilizando qualquer segurança que o algoritmo traria (KIM; SOLOMON, 2014).

No ano de 2001, o órgão Americano NIST recomendou um novo algoritmo de criptografia conhecido como *Advanced Encryption Standard* (AES), substituindo o algoritmo DES. O algoritmo AES suporta uma combinação de dados de 128 *bits* e chaves com o comprimento de 21 128, 192 e 256 *bits* (SINGH, 2013). (SILVA, 2019, p.21)

Esse algoritmo suporta um comprimento de 128 *bits* e pode ser dividido em até 4 blocos operacionais básicos, organizados como uma matriz de *bytes* de ordem 4x4, chamado de "estado". Igualmente ao anterior, os processos de encriptar e de decriptar uma informação passa por dez passos, e cada um desses passos decorre em quatro etapas (SILVA, 2019).

Retomando o conceito de chave simétrica, Silva (2019) especifica que se um terceiro interceptar a chave durante a transmissão, ele tem acesso às instruções para criptografar novas mensagens e descriptografar a informação cifrada enviada, inutilizando qualquer segurança que o algoritmo traria (KIM; SOLOMON, 2014). (SILVA, 2019, p.21)

Logo, tratando- se da segurança que a chave simétrica proporciona aos seus usuários, essa vulnerabilidade poderá incorrer da inutilização dos algoritmos gerados para proporcionar o princípio de confidencialidade. Essa ação afetaria diretamente a proteção dos sistemas de informação contra desastres, erros e manipulações de usuários mal-intencionados.

2.3 USO DE CRIPTOGRAFIA EM APARELHOS MÓVEIS

A necessidade do uso de medidas de proteção de dados não se limita aos dispositivos de uso corporativo; com a evolução da tecnologia e com a criação dos dispositivos móveis, houve um aumento exponencial da utilização da internet através desses aparelhos, ocorrendo a criação de uma série de medidas de segurança nesse tipo de rede.

A principal rede desse ramo é a *Wireless Fidelity* (WiFi), e ela segue as especificações do padrão *Institute of Electrical and Electronics Engineers* 802.11 (IEEE 802.11). Porém, o uso delas diminui a segurança do tráfego de informação, pois não é fisicamente possível garantir a preservação dos dados.

Quando se utiliza uma *Local Area Network* (LAN), é possível restringir o acesso dos seus usuários, algo de extrema relevância no meio corporativo [Moretti e Bellezi 2014]. Bine e Kuk (2016) explicam que, ao utilizar uma *Local Area Network* (LAN), é possível restringir o acesso dos seus usuários, o que é bastante importante no meio corporativo. No que diz respeito ao *Wi-Fi*, temos o *Wired Equivalent Privacy* (WEP), Privacidade Equivalente a Rede Cabeada, que utiliza uma senha compartilhada para criptografar os dados e funciona de forma estática.

Além de fornecer apenas um controle de acesso e de privacidade de dados na rede sem fio; *Wi-fi Protected Access* (WAP) e o *Wi-fi Protected Access 2* (WPA2), sendo wi-fi de acesso protegido, a principal diferença entre o WPA e o WPA2 é a forma com a qual ele criptografa os dados. Enquanto o WPA utiliza o (Temporal Key Integrity Protocol – Protocolo de Integridade de Chave Temporal (TKIP), Protocolo de Integridade da Chave Tempora, como algoritmo de criptografia, o WPA2 utiliza o algoritmo *Advanced Encryption Standard* - Padrão de criptografia avançada (AES).

Para a garantia dos dados dos usuários *Wi-Fi*, foram criados alguns protocolos de segurança, como o WPA e WPA2. A diferença entre os dois é a forma com que é feita a criptografia dos dados. Por um lado, o WPA usa o Temporal Key Integrity Protocol – Protocolo

de Integridade de Chave Temporal (TKIP) como algoritmo de criptografia, e, por outro lado, o WPA2 utiliza o algoritmo AES (*Advanced Encryption Standard* - Padrão de criptografia avançada).

Observa-se, então, que o algoritmo AES é consideravelmente mais pesado que o TKIP, em contrapartida, oferece uma segurança de dados mais aprimorada, pois permite uma quantidade maior de combinações, dificultando a sua decriptografia.

TIPO DE PESQUISA

Para o desenvolvimento deste trabalho, foi utilizado o procedimento de Revisão Bibliográfica junto ao estudo exploratório, o qual visa a aprofundar o tema e a aumentar a interação com um assunto pouco conhecido e explorado no meio civil que, para implementar o conhecimento, segundo Gil (2008, p. 58), ‘‘é desenvolvida a partir de material já elaborado, constituído de livros e artigos”. Por ser uma pesquisa que precisa ser fundamentada e organizada, Vergara (2009, p. 47) explica que pesquisas exploratórias aplicam-se em situações ‘‘nas quais há pouco conhecimento acumulado e sistematizado”.

Por fim, a pesquisa apresentou atributos descritivos por expor detalhadamente sobre: a importância da criptografia para o sigilo das informações nos *softwares* e permitir o entendimento mais aprofundado de um assunto pouco conhecido, mas bastante importante para a confidencialidade de dados. Dessa forma, os estudos apresentados denotam grande importância e servirão de acervo para futuras pesquisas a respeito da temática abordada.

TRAJETÓRIA METODOLÓGICA DA PESQUISA

A primeira etapa desta investigação é buscar compreender e interpretar a importância do tema abordado e consolidar a pesquisa por meio de fontes, por meio do uso de artigos científicos, manuais, e livros de acervos virtuais e físicos, nos quais foi observada a importância da criptografia para a segurança dos *softwares,* sendo possível reduzir vazamentos, a perda e o roubo de dados e informações. Logo após, foi elaborada a segunda etapa, a qual consiste na coleta de dados, abordados mediante da leitura exploratória. E, para absorver o máximo de conteúdo, foi realizada a leitura analítica na terceira e na última etapa.

DISCUSSÕES

Entende-se que o presente artigo respondeu com êxito os pontos levantados acerca da Importância da Criptografia no que tange aos aspectos evolutivos, gerais e positivos.

É notório, também, que o tema é bastante relevante não só para a segurança das informações do Exército Brasileiro, como também para empresas e pessoas do âmbito civil. Dessa forma, todos aqueles que obtém um entendimento maior sobre o assunto possam ressaltar a importância dele para outras pessoas ou instituições, com a finalidade de aumentar o

conhecimento sobre criptografia e proteger-se contra crimes e golpes cibernéticos que causam prejuízos na sociedade

Logo, trabalhos como este qualificam-se como auxílio para propagar informações sobre o tema, pois por ser algo bastante atual e tecnológico, há a necessidade de maior difusão não apenas no meio militar, mas também para futuros trabalhos no meio civil.

CONSIDERAÇÕES FINAIS

No término desta pesquisa, tivemos a certeza de que o Sistema criptográfico garante uma maior segurança e assegura o sigilo das comunicações, respeitando a integridade das informações nos diversos aspectos. Os diversos métodos de criptografia implementados nos aplicativos no meio civil e principalmente nas Forças Armadas, as quais estão se modernizando, visando aumentar a segurança na transmissão de informações que necessitem um maior nível de sigilo com o uso dos diversos tipos de criptografias.

As ferramentas de apoio utilizadas para a aplicação das tecnologias de criptografia oferecido pelos diversos sistema criptográficos existentes, garante a segurança dos dados em nível altamente aprimorado que permite a maior confidencialidade possível, dificultando a decriptografia por indivíduos não autorizados.

Os Sistemas criptográficos mostram-se, cada vez mais, de fundamental importância nas manobras e operações evitando que informações importantes sejam interceptadas, modificadas ou até mesmo falsificadas, construindo assim, conhecimento estratégico, e buscando resultados satisfatórios nos diversos âmbitos da comunicação, desde o planejamento, a análise dos erros e acertos obtidos durante o planejamento, e, por fim, a execução.

REFERÊNCIAS

ADIL, Josué. Entenda a importância da criptografia para a segurança dos seus dados na internet. **Academia Inovadora de Ti**. 2019. Disponível em: https://acaditi.com.br/entenda-a-importancia-da-criptografia-para-a-seguranca-dos-seus-dados-na-internet/
Acesso em: 27 mar. 2022.

ADIL, Josué. Entenda a importância da criptografia para a segurança dos seus dados na internet. **Academia Inovadora de Ti**. 2020. Disponível em: https://acaditi.com.br/entenda-a-importancia-da-criptografia-para-a-seguranca-dos-seus-dados-na-internet/#:~:text=A%20grande%20necessidade%20de%20uso,arquivos%20e%20de%20mensagens%20trocadas
Acesso em: 28 mar. 2022.

A IMPORTÂNCIA: da Criptografia De Dados Em Aplicativos. Made In Web, 2018. Disponível em: https://www.madeinweb.com.br/importancia-da-criptografia-de-dados-em-aplicativos/#:~:text=No%20caso%20dos%20aparelhos%20como,reter%20dados%20navegando%20nestas%20conex%C3%B5es
Acesso em: 03 abr. 2022.

BINE, Jamilson; KUK, Josiel Neumann**. Estudo de segurança em dispositivos móveis.** Departamento de ciência da computação. Semana acadêmica. Universidade do centro-oeste. UNICENTRO. Guarapuava, 2016. Disponível em: https://semanaacademica.org.br/system/files/artigos/jamilson_bine-estudo_de_seguranca_em_dispositivos_moveis.pdf
Acesso em: 5 mar. 2022.

CHIAVENATO, I. **Introdução à teoria geral da administração**. São Paulo: Makron Books, 2004.
Acesso em: 01 abr. 2022.

CIPRIANO, Wellington Ferreira. **A segurança da informação com o advento da internet das coisas em ambientes hospitalares: uma abordagem bibliográfica.** Escola de Formação Complementar do Exército / Centro Universitário do Sul de Minas – UNISMG. Salvador, 2020. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/9237/1/CGAEM_2021_1_majcipriano.pdf
Acesso em: 02 abr. 2022.

COELHO, Arthur Prieto. **Mecanismo De Criptografia Para Comunicação Via Bluetooth.** Centro Universitário De Brasília -UniCEUB .Brasília, 2011. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/3145/2/20564741.pdf
Acesso em: 03 abr. 2022.

CRIPTOGRAFIA: de Nível Militar Para Comunicação Segura. ProtectSoftware, 2021. Disponível em: https://www.protectsoftware.com.br/criptografia

Acesso em: 3 abr. 2022.

CRIPTOGRAFIA: e confidencialidade das informações. **MGITECH.** 2015. Disponível em: https://blog.mgitech.com.br/blog/criptografia-e-confidencialidade-das-informacoes
Acesso em: 20 mar 2022.

CRIPTOGRAFIA: e Criptoanálise. GTA.UFRJ, 2010. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/hist.htm#:~:text=Criptografia%20e%20a%20Criptoan%C3%A1lise&text=A%20primeira%20mensagem%20criptografa%20que,atrav%C3%A9s%20de%20um%20mensageiro%20privado
Acesso em: 17 mar. 2022.

CRIPTOGRAFIA: tipos, exemplos e importância nas empresas. **Equipe Totvs.** 2022. Disponível em: https://www.totvs.com/blog/negocios/criptografia/#:~:text=Uma%20maneira%20de%20proteger%20a,por%20um%20terceiro%20n%C3%A3o%20autorizado
Acesso em: 22 mar. 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2008. Disponível em: https://wp.ufpel.edu.br/ecb/files/2009/09/Tipos-de-Pesquisa.pdf
Acesso em: 29 mar. 2022.

GREEN, P. C. **Desenvolvendo Competências Consistentes – Como Vincular Sistemas de Recursos Humanos a Estratégias Organizacionais.** Rio de Janeiro Qualitymark, 2000.
Acesso em: 7 abr. 2022.

LGPD: o que é, objetivos e como sua empresa pode se adequar. **Equipe Totvs.** 2021. Disponível em: https://www.totvs.com/blog/adequacao-a-legislacao/lgpd/
Acesso em: 25 mar. 2022.

ORLANDINI, L. **Administração de Empresas - Teoria x Prática: o que o mercado procura?** Paraná: Web Portal Paraná LTDA. Disponível em: http://www.bonde.com.br
Acesso em: 29 mar. 2022.

PINHEIRO, Jéssica. **Retrospectiva 2018: Os 10 maiores escândalos tech de 2018.** Canal Tech, 2018. Disponível em: https://canaltech.com.br/internet/retrospectiva-2018-os-10-maiores-escandalos-tech-de-2018-129873/
Acesso em: 14 mar 2022.

RABAGLIO, M. O. **Seleção por Competências.** São Paulo: Educator, 2001.
Acesso em: 03 abr. 2022.

RESENDE, E. **O Livro das Competências – Desenvolvimento das Competências: a Melhor Auto-Ajuda para Pessoas, Organizações e Sociedade.** Rio de Janeiro: Qualitymark, 2000.
Acesso em: 03 abr. 2022.

SALES, E. Como aumentar a segurança de dados através da criptografia. **Esales.** 2020. Disponível em: https://esales.com.br/blog/como-aumentar-seguranca-de-dados-atraves-da-criptografia/
Acesso em: 20 mar. 2022.

SEGURANÇA: da informação e criptografia são temas de evento nacional realizado no comando militar do planalto. **EBMIL.** 2016. Disponível em: https://www.eb.mil.br/web/haiti/noticias-braengcoy/-/asset_publisher/uIeNJ9eDHugv/content/seguranca-da-informacao-e-criptografia-sao-temas-de-evento-nacional-realizado-no-comando-militar-do-planalto-/8032597
Acesso em: 21 mar. 2022.

SILVA, Willian Wallace de Matteus. **A Evolução Da Criptografia E Suas Técnicas Ao Longo Da História.** Instituto Federal Goiano, 2019. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf
Acesso em: 14 mar. 2022.

THIOLLENT, Michel. Metodologia da pesquisa - ação. 2. ed. São Paulo: Cortez, 1986. Disponível em: https://wp.ufpel.edu.br/ecb/files/2009/09/Tipos-de-Pesquisa.pdf
Acesso em: 29 mar. 2022.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2009. Acesso em: 05 abr. 2022

VIEIRA, V. A. **As tipologias, variações e características da pesquisa de marketing.** Revista da FAE, Curitiba, v. 5, n. 1, p. 61-70, janabr 2002.
Acesso em: 08 abr. 2022.

YOSHIDA, Elias Yoshiaki**. Informação, Comunicação e a Sociedade do Conhecimento. Segurança, Criptografia, Privacidade e Anonimato Fase 2.** MAC 339, 2001. Disponível em: https://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/elias/
Acesso em: 17 mar. 2022.

ZOGBI, Paula. **Netflix, LinkedIn e YouPorn têm vazamento de 1,4 bilhão de dados sigilosos. InfoMoney** 2017. Disponível em: https://www.infomoney.com.br/consumo/netflix-linkedin-e-youporn-tem-vazamento-de-14-bilhao-de-dados-sigilosos/
Acesso em: 15 mar. 2022.