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

Cleisson Fernando Fernandes Souza Daniel de Sousa Farias
Fabiano Gomes de Almeida Junior Marcos Wendell Venegeroles Silva Mota Rafael Carvalho Bento Júnior
Raul André da Conceição de Souza Thiago Silva Campos
Vinícius Luiz Duarte Gomes

ANÁLISE SOBRE AS POSSÍVEIS UTILIZAÇÕES DA CRIPTOGRAFIA POR HARDWARE NO EXÉRCITO BRASILEIRO

TRÊS CORAÇÕES – MG
2022

Cleisson Fernando Fernandes Souza
Daniel de Sousa Farias
Fabiano Gomes de Almeida Junior
Marcos Wendell Venegeroles Silva
Mota Rafael Carvalho Bento Júnior
Raul André da Conceição de Souza
Thiago Silva Campos
Vinícius Luiz Duarte Gomes

ANÁLISE SOBRE AS POSSÍVEIS UTILIZAÇÕES DA CRIPTOGRAFIA POR HARDWARE NO EXÉRCITO BRASILEIRO

Projeto de pesquisa de 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: Ten. Israel Soares de Oliveira
Área de concentração: Segurança

TRÊS CORAÇÕES – MG
2022

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

Cleisson Fernando Fernandes Souza Daniel de Sousa Farias
Fabiano Gomes de Almeida Junior Marcos
Wendell Venegeroles Silva Mota Rafael Carvalho Bento Júnior
Raul André da Conceição de Souza Thiago Silva Campos
Vinícius Luiz Duarte Gomes

ANÁLISE SOBRE AS POSSÍVEIS UTILIZAÇÕES DA CRIPTOGRAFIA POR HARDWARE NO EXÉRCITO BRASILEIRO

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

_____
Membro: Thamara Marques Rodrigues - Ten

_____
Membro: Enói Maria Miranda Mendes – Tem

_____
Orientador: Israel Soares de Oliveira - Ten

RESUMO

Este trabalho titulado: “Análise sobre as possíveis utilizações da criptografia por *hardware* no Exército Brasileiro” - aborda uma temática discutida com frequência, tanto no âmbito civil quanto militar. Isso, porque, existe a necessidade de expandir o conhecimento na área de proteção de dados, tanto por *hardware* como por *software*. Dessa forma, este projeto tem por finalidade de explanar a importância da criptografia como meio essencial de proteção de dados, principalmente em relação à área de defesa cibernética militar utilizando os meios físicos, conhecidos como hardware. As instituições militares necessitam de mecanismos para protegerem suas informações contra invasões ou ataques, visto que elas são detentoras de conhecimentos e dados sensíveis que são essenciais para a defesa nacional. A aplicação desse tipo de proteção nos equipamentos utilizando ferramentas externas, como *pen drives* e outros tipos de *hardware* de armazenamento de dados, tornam quase inexistentes o acesso de invasores. Dessa forma, a criptografia desse material manterá restrita as informações contidas no equipamento. Na sociedade, em geral, a ideia de que a proteção dos dados pessoais ou empresariais é necessária é bastante difundida. A metodologia adotada foi a revisão bibliográfica, juntamente com a pesquisa exploratória, usando como fundamentação o autor Antônio Carlos Gil (2008). O tema visa analisar sobre esse sistema de segurança de informações, evidenciando as vantagens de ser feito através de dispositivos físicos aos quais denominamos *hardwares.* Nesse viés, é necessário que esses conhecimentos sejam disseminados e colocados em prática, reduzindo os problemas com interceptações de informações.

Palavras-chave: Criptografia por Hardware. Informação. Proteção.

ABSTRACT

This work entitled: “Analysis of the possible uses of hardware encryption in the Brazilian army” - addresses a frequently discussed topic, both in the civil and military spheres. This is because there is a need to expand knowledge in the area of data protection, both by hardware and software. Thus, this project aims to explain the importance of encryption as an essential means of data protection, especially in relation to the area of military cyber defense using physical means. Military institutions need mechanisms to protect their information against intrusions or attacks, as they hold knowledge and sensitive data that are essential for national defense. The application of this type of protection on equipment using external tools, such as pen drives and other types of data storage hardware, makes remote access by intruders almost non-existent, preventing any contact that is not physical. In this way, the encryption of this material will keep the information contained in the equipment restricted. In society, in general, the idea that the protection of personal or business data is necessary and still not widespread. The methodology adopted was the bibliographic review, together with exploratory research, using as a basis the author Gil (2008). The theme aims to explain about this information security system, highlighting the advantages of being done through physical devices which we call hardware. In this bias, it is necessary that this knowledge be disseminated and put into practice, reducing problems with information intercepts.

Keywords: Hardware Encryption . Information. Protection

LISTA DE FIGURAS

LISTA DE SIGLAS

EB	Exército Brasileiro
IME	Instituto Militar de Engenharia
DES	Data Encryption Standart
RSA	Rivest-Shamir-Adleman
CI’s	Circuitos integrados
PLD	Programable Logical Devices

SUMÁRIO

1 INTRODUÇÃO

O tema deste trabalho é “A Importância da Criptografia por *Hardware* no Sigilo das Transmissões”, e tem como título delimitador “Análise sobre a possível utilização da criptografia por hardware no Exército Brasileiro”, não obstante, a delimitação do tema da pesquisa restringiu-se à criptografia como medida de proteção nos sistemas de Transmissão. Isso porque a criptografia, que é a codificação de um texto, é amplamente utilizada para proteger, dificultar e impedir que pessoas não autorizadas tenham acesso a determinadas informações. No contexto da globalização, governos e grandes empresas mundiais utilizam a criptografia como meio seguro para a troca de mensagens. Na abordagem da origem da criptografia ela faz parte da sociedade há muitos anos, sendo inserida no meio militar e associada às suas práticas.

O tema foi escolhido com o intuito de analisar informações sobre a criptografia por *hardware* e incentivar futuros estudos sobre tal tipo de criptografia, dado a importância que novas informações sobre o assunto agregaria a sociedade brasileira. Existe também a finalidade de apresentar os equipamentos militares que utilizam a criptografia por *hardware* em operações das forças armadas, como os *pen-drives* utilizados como *tokens* por comandantes para obter acesso a informações restritas, considerando que o tipo de criptografia por *hardware* é mais seguro que o sistema criptográfico por *software*.

Desta forma, esta investigação tem como objetivo geral apresentar a criptografia como medida de proteção dos Sistemas de Transmissão. Para iniciarmos esta abordagem, vamos começar expondo as questões orientadoras, são elas: Qual a origem da criptografia? O que é *hardware*? O que é *software*? Qual a diferença de criptografia por *software* para criptografia por *hardware*? Na intenção de solucionar essas dúvidas, serão expostas de forma sucinta as possíveis respostas para tais perguntas.

Segundo o autor (ORDONEZ; PEREIRA; CHIARAMONTE, 2005) a criptografia é um método de segurança de mensagens muito antigo, usado até mesmo na antiga forma de escrita egípcia, um método de proteção a qual o meio militar dependia – para a sua defesa – de mensagens secretas, sendo utilizados algoritmos específicos para a descriptografia da mensagem.

Essa fase clássica da criptografia vai desde os povos romanos, egípcios e mesopotâmicos há 3500 anos até antes da Segunda Guerra Mundial, tendo dentro dela alguns períodos específicos e que angariaram uma notoriedade dentro da criptografia, como a Cifra de César, na qual uma letra era substituída e rotacionada por um determinado número de posições, tanto para a esquerda quanto para a direita.

Durante a Segunda Guerra Mundial, surgiu a criptografia moderna, pois, naquele momento de instabilidade tornava-se essencial manter as informações em sigilo. Sendo assim, a fim de evitar possíveis ataques, os alemães desenvolveram uma máquina chamada “Enigma”, invenção do engenheiro Arthur Scherbius na qual se baseou na invenção do holandês Hugo Alexander Kock. Tal máquina assemelhava-se a uma máquina de escrever, em que era usada uma chave em sua estrutura para cifrar e decifrar uma mensagem, onde rotores eletrônicos eram sua base que alteravam conforme a necessidade. Não obstante, no século XXI a criptografia teve uma acentuada evolução, principalmente na computação em que são utilizados sistemas de chaves criptográficas, conjuntos de bits baseado em algoritmo capaz de decodificar a informação e são divididas em chaves simétricas e assimétricas. (BATITUCCI, 2020)

O *hardware* é todo componente físico, externo ou interno de um computador ou celular, que determina do que um dispositivo é capaz e como pode ser utilizado. De modo englobante, é toda máquina, ferramenta ou utensílio que passa por um celular ou computador é um *hardware*. (GOGONI, 2019)

Por conseguinte, o *software* é um conjunto de instruções que devem ser seguidas e executadas por um mecanismo, seja ele um computador ou um aparato eletromecânico. Dessa maneira, é usado para descrever programas, *apps, scripts*, macros e instruções de código embarcado diretamente, de modo em que ordene o que uma máquina deve fazer. (GOGONI, 2019)

A criptografia por *software* é uma abordagem de segurança para proteger os dados confidenciais usando ferramentas de *software* para criptografar os dados. A única maneira de criptografar ou dcsriptografar esses dados é por meio de uma senha.

Dessa maneira, a criptografia por *hardware* designa-se às unidades de armazenamento, que suportam criptografia de *hardware* que vêm com um chip pequeno na placa de circuito impresso - Printed Circuit Board (PCB) - um processador que lida com criptografia de dados com uma chave pública ou privada, que consiste em uma chave para cifrar a mensagem, que seria a chave pública e uma chave para decifrar a mensagem, que seria a chave privada. Dessa maneira, esse processador dedicado abriga as funções matemáticas necessárias para executar o algoritmo de criptografia e desscriptografia de dados.

O processador exclusivo é acompanhado por uma pequena memória dedicada para armazenar a chave segura e é isolado do restante das funções do dispositivo para garantir a melhor segurança e o menor impacto no desempenho do dispositivo (isso significa que ele pode acessá-lo apenas e exclusivamente ao processador dedicado).

Ademais, é necessário ressaltar que, no âmbito da utilização das duas criptografias, a criptografia por *hardware* se torna a melhor, pois além de ser muito

rápida, a sua memória e o seu processador não afetam o desempenho do sistema, tornando-se muito mais seguras, porque são utilizadas em circuitos e sistemas isolados, sendo menos vulneráveis a ataques, dessa forma, torna-se um ótimo meio de criptografia que o Exército Brasileiro (EB) pode utilizar em seus sistemas confidenciais.

2 DESENVOLVIMENTO

Neste capítulo será abordado o desenvolvimento do Trabalho Científico, o qual leva em consideração os Objetivos de forma clara e objetiva, em seguida o Referencial Teórico, composto por citações diretas de pesquisadores, imagens e contextos históricos os quais fundamentam esta pesquisa, com finalidade de responder à questão norteadora qual foi trabalhada: As possíveis utilizações da criptografia por Hardware no Exército Brasileiro? Posteriormente, o Tipo de pesquisa e a Trajetória Metodológica da Pesquisa.

2.1 Objetivos

- Apresentar a criptografia por hardware como possível utilização para a segurança das informações no Exército Brasileiro.
- Compreender a importância da criptografia por
- *hardware*; Analisar diversos fatores referentes a
- criptografia;

  Apresentar sugestões de sua utilização no Exército Brasileiro.

2.2 Referencial Teórico

O referencial teórico desta investigação tem por objetivo apresentar a criptografia como importante meio de proteção de dados e sua forma de utilização, seja ela nos diversos aplicativos contidos no celular ou em redes corporativas, sendo apresentado primeiramente a história da criptografia moderna onde se começou[1] a utilizá-la na forma de proteção das transmissões, passando pelos dias atuais na sua existência nos diversos programas. Logo depois, abordando a criptografia por *hardware*, que consiste no enfoque principal, como ela funciona e sua utilização. Passando por último aos equipamentos que utilizam a criptografia por *hardware* em uso no Exército Brasileiro.

A seguir, será apresentada a Figura 1, na qual representa o Rádio Harris RF 7800 V-HH.

Figura 1: Rádio Harris RF 7800 V-HH

Fonte: Semiee[1]

A figura 1, retrata o rádio RF 7800 V-HH, utilizado em operações do Exército Brasileiro (EB). Ele possui um sistema de criptografia que é utilizado para manter o sigilo das transmissões realizadas em operações militares.

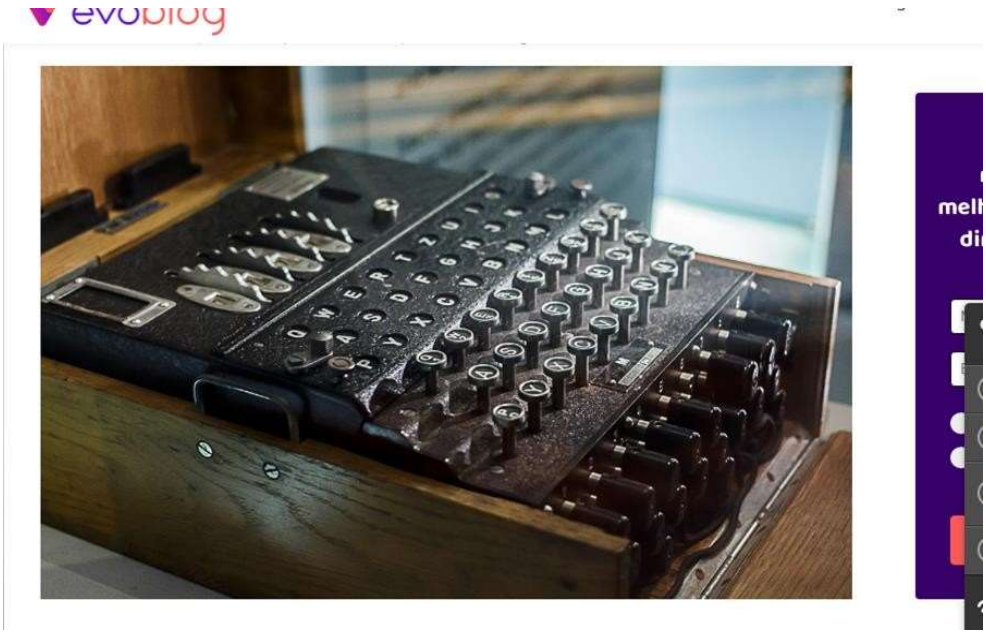
2.2.1 História da criptografia moderna até os dias atuais

A Criptografia moderna surgiu durante o período em que se abrangeu a Segunda Guerra Mundial, (BATITUCCI, 2020) época em que se fazia de extrema necessidade a segurança das transmissões, onde os integrantes do Eixo e os Aliados buscavam, a todo momento, informações um sobre o outro, a fim de garantir vantagens no campo de batalha. Com o pensamento de proteger suas transmissões, os alemães desenvolveram uma máquina chamada “Enigma” (BATITUCCI, 20200).

1A Figura 1 foi retirada do site Semiee. Disponível em: https://www.semiee.com/file/backup2/HARRIS- RF-7800V-HH.pdf. Acessado em: 18 mar. 2022

A seguir, será apresentada a Figura 2, na qual referencia a máquina criada pelos alemães, conhecida por Máquina Enigma.

Figura 2: Máquina Enigma



Fonte: Mastermaq (2020).

A Figura 2 apresenta a máquina Enigma, criada na Segunda Guerra Mundial, meados dos anos 1939 – 1945. Ela tem semelhança com uma de escrever e utilizava como chave em sua estrutura para cifrar/decifrar, que tinha como base rotores eletrônicos que eram alterados conforme necessidade.

Hoje em dia, com a evolução da tecnologia e a facilidade de acesso da mesma, tornou-se de grande importância a proteção de dados, tendo em vista a vulnerabilidade destes na rede, se tornando um assunto sensível. Com a combinação de algoritmos para a proteção de diversos dados e maior segurança na circulação de informações em rede, a criptografia é amplamente utilizada, um exemplo dessa utilização está na proteção das contas bancárias e dados de usuários na internet, principalmente em ferramentas as quais são armazenadas informações sigilosas.

2.2.2 Utilização da criptografia

A criptografia é um recurso utilizado para a proteção de dados, evitando assim a perda de dados e a invasão dos mesmos por indivíduos mal intencionados. Para realizar a criptografia é usado o sistema de chaves criptográficas, na qual é dividida em chave

simétrica e chave assimétrica, as simétricas utilizam uma única chave para criptografar e decifrar dados, enquanto a assimétrica faz uso de duas chaves, uma pública, para cifrar a mensagem e uma privada para decifrar a mensagem (KIM, SOLOMON, 2014)

A criptografia é muito utilizada na sociedade, mas muitas vezes nem percebemos sua aplicação, como em aplicativos de celular, em sites de instituições e redes governamentais. Tudo isso visando a proteção das informações contidas nesses sistemas. É importante saber que a criptografia não é apenas utilizada na circulação das informações, mas também em seu armazenamento, como discos rígidos e *pen drives.*

A obtenção de dados, sejam eles pessoais ou de empresas, é algo que, utilizado por indivíduos de má índole, se tornou uma forma de ganhar vantagens ou prejudicar o próximo, então cresce em demasia a importância da criptografia para a proteção dos mesmos.

> Eu estou falando a vocês do Vale do Silício, onde algumas das mais proeminentes e bem-sucedidas companhias vem construindo seu negócio convencendo seus clientes a serem complacentes sobre suas informações pessoais. Elas estão engolindo tudo que podem aprender sobre vocês e estão tentando monetizar isso. Nós achamos que isso é errado. E não é o tipo de empresa que a Apple quer ser. (COOK, TIM, 2015[2])

Com isso, pode-se perceber que a criptografia deve ser ainda mais utilizada, reforçando a população a importância da mesma e levando em conhecimento geral a sua existência nos diversos aplicativos e meios de programação, e da importância de manter os dados pessoais bem protegidos.

2.2.3 Criptografia por *Hardware* (Equipamentos que utilizam)

A criptografia por hardware pode ser encarada como uma alternativa que protege sistemas computacionais, onde a autenticação ocorre por meio do hardware. Ela está ligada a um dispositivo específico, logo cada dispositivo contém sua própria chave criptográfica. Considerada um excelente meio de proteção de dados contra invasões utilizando o próprio equipamento, que de alguma forma possa ter sido furtado e está sendo utilizado para obtenção de informações. Seria uma solução para a proteção dos

[2]A citação foi retirada do site Correio do Estado. Disponível em: https://correiodoestado.com.br/tecnologia/nossa-privacidade-esta-sendo-atacada-diz-chefe-da-apple/248629. Acesso em: 18 mar. 2022

equipamentos nacionais, uma vez que seu desenvolvimento precisa ser inteiramente do país, a fim de saber as vulnerabilidades e procurar sempre corrigir, caso contrário, se fosse feito em parceria com outra nação, poderia ficar à mercê do mesmo, podendo virar um possível adversário.

> Quanto a implementação física, define-se por criptografia via hardware aquela em que o algoritmo criptográfico é processado por um ou alguns circuitos integrados (CI's) dedicados ou especialmente programados. As principais vantagens da criptografia via hardware são a velocidade e irreprodutibilidade. (BRUNAZO; TING, 1989, p.1).

Os sistemas criptográficos - Data Encryption Standart (DES) e Rivest-Shamir-Adleman (RSA) - são os mais conspícuos, apesar de que grande, se não toda a exportação é de controle do governo dos Estados Unidos. A diferença de ambos é que o DES usa uma chave assimétrica para obter informação virtual e o RSA é uma chave pública utilizado para uma segura transmissão de dados.

No entanto, há uma ideia de utilizar os Circuitos Integrados (CI's) do Programable Logical Devices (PLD), os quais, a sua produção não é controlada e não se sabe ao certo a forma de que eles são programados. Além de seu suporte ser original, pode-se fazer infinitos algoritmos com diferentes graus de segurança.

No mundo, existem diversos equipamentos que utilizam este tipo de criptografia, como por exemplo o *pen drive*, os computadores, entre outros. Dessa forma, para uma melhor segurança nas transmissões realizadas pelo Exército Brasileiro, pode-se ser realizado pesquisas, pelas diversas instituições militares, como o Instituto Militar de Engenharia (IME), que visem um maior emprego da criptografia por *hardware* no teatro de operações. Um modelo dessa utilização seria um *pen drive* com esse molde de criptografia utilizado pelos mensageiros e em caso de interceptação do inimigo, não seria possível o acesso às informações contidas nele, ou até mesmo conduzi-lo a uma série de informações falsas que levaria o oponente a sua completa desinformação, tendo em vista que um dos princípios da segurança das comunicações é a negação da informação.

2.3 Tipo de Pesquisa

Esta investigação seguiu parâmetros da revisão bibliográfica, que consiste na realização de um estudo para a familiarização com o tema, por meio desses parâmetros que, segundo Gil (2008,p.58), "é desenvolvida a partir de material já elaborado, constituído de livros e artigos científicos" ou documentos no âmbito

virtual que contribuíram para angariar conhecimentos sobre o objeto de estudo. O trabalho apresentou um ponto de vista descritivo, por transmitir ideias do tema "A Importância da Criptográfica por *Hardware* no Sigilo das Transmissões" no âmbito do Exército, apresentando um contexto lógico para contribuir no estudo mais aprofundado do tema e mostrar um meio mais seguro de criptografia.

2.4 Trajetória Metodológica da Pesquisa

Segundo o pensamento de Gil (2008), a fase inicial do projeto contemplou o estudo de uma série de pesquisas, dando o conhecimento necessário para a explanação do assunto e divulgação deste conhecimento para os não familiarizados com o conteúdo.

Sendo assim, foi apresentado as definições e objetivos deste trabalho. Foram explanadas de forma aprofundada e simples, a fim de que pessoas sem conhecimento sobre o tema leiam e entendam a criptografia por *hardware* e a sua utilização nos sistemas de transmissão e armazenamento de informações. Dessa maneira, foi elaborada a segunda parte, a qual foi de suma importância a utilização da coleta de dados, utilizando-se a leitura seletiva e exploratória. Na terceira parte, foi elaborada uma leitura analítica.

.

3. Discussões

É entendido que este artigo respondeu com êxito todos pontos citados sobre A Análise sobre as Possíveis Utilizações da Criptografia por Hardware no Exército Brasileiro no que se refere aos aspectos evolutivos, gerais e positivos.

É visto com notoriedade, também, que ao estimular os estudos sobre o tema, o Exército Brasileiro tem a possibilidade de obter tal meio de criptografia para assim agir de forma que informações sigilosas não caiam nas mãos de um possível inimigo e que seja mantido o sigilo das transmissões.

Sendo assim, trabalhos como este constituem-se como benefício para ramificar informações acerca do tema, pois por ser algo que mudaria o sistema de criptografia e muito tecnológico, deve ter maior propagação não apenas no meio militar, como dito neste artigo, mas também para trabalhos vindouros no meio civil.

4. Considerações Finais

A Análise sobre as Possíveis Utilizações da Criptografia por Hardware com suas propostas e inovações assegura um maior envolvimento no desempenho da construção do conhecimento, respeitando individualidades em relação ao ritmo e características de aprendizado. Esse método implementado tanto no meio civil, quanto no meio militar, está sendo modernizado de forma contínua por meio de possíveis projetos que têm visado desenvolver competências referentes ao sigilo das transmissões.

O Exército Brasileiro necessita manter suas informações em sigilo e para isso, utiliza da criptografia por software, porém, com as ponderações apresentadas neste trabalho é evidente que a criptografia por hardware é mais eficaz e segura. A explanação das melhorias que a implementação dessa tendência em sua comunicação, focada no aperfeiçoamento, é a intenção desse trabalho.

REFERÊNCIAS

ASSURED COMMUNICATIONS. Harris. **Handheld VHF Radio**. 2009. Disponível em: https://www.semiee.com/file/backup2/HARRIS-RF-7800V-HH.pdf. Acessado em: 18 mar. 2022.

BATITUCCI, Manuela. **Criptografia: quando, como surgiu e onde é usada**. 2 set. 2020. Disponível em: http://blog.mastermaq.com.br/como-surgiu-a-criptografia/. Acessado em: 18 mar. 2022.

COOK, Tim. **"Nossa privacidade está sendo atacada"**. 3 jun. 2015. Disponível em: https://correiodoestado.com.br/tecnologia/nossa-privacidade-esta-sendo-atacada-diz- chefe-da-apple/248629. Acesso em: 18 mar. 2022.

FILHO, Amílcar Brunazo; TING, Daniel Kao Sun. **Hardware Criptográfico, uma solução nacional.** 1997. Disponível em: http://www.brunazo.eng.br/tn/hardnac.html#:~:text=Quanto%20a%20implemente%C3%A7%C3%A3o%20f%C3%ADsica%2C%20define,s%C3%A3o%20a%20velocidade%20e%20irreprodutibilidade. Acesso em: 18 mar. 2022.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6ª. ed. São Paulo: Atlas, 2008.

GOGONI, Ronaldo. **O que é hardware?** Disponível em: https://tecnoblog.net/responde/o-que-e-hardware/ Acesso em: 18 mar. 2022.

_____**O que é software?** Disponível em: https://tecnoblog.net/responde/o-que-e-software/ Acesso em: 18 mar. 2022.

Nossa privacidade está sendo atacada', diz chefe da Apple Disponível em: https://correiodoestado.com.br/tecnologia/nossa-privacidade-esta-sendo-atacada-diz-chefe-da-apple/248629 Acesso em: 18 mar. 2022.