UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ)
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS (CCJE)
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS (FACC)
CURSO DE BIBLIOTECONOMIA E GESTÃO DE UNIDADE DE INFORMAÇÃO (CBG)

PHIAMA HIVERA SILVA DE ALMEIDA

O SEGREDO DA COMUNICAÇÃO SECRETA: A CRIPTOGRAFIA COMO MÉTODO DE SEGURANÇA DA INFORMAÇÃO

Rio de Janeiro
2019

PHIAMA HIVERA SILVA DE ALMEIDA

O SEGREDO DA COMUNICAÇÃO SECRETA: A CRIPTOGRAFIA COMO MÉTODO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de bacharel em Biblioteconomia e Gestão de Unidades de Informação.

Orientador (a): Prof. Dr. Andre Vieira de Freitas Araujo

Rio de Janeiro

2019

CIP - Catalogação na Publicação

AA447s

Almeida, Phiama Hivera Silva de
O segredo da comunicação secreta: a criptografia como método de segurança da informação / Phiama Hivera Silva de Almeida. -- Rio de Janeiro, 2019.
61 f.

Orientador: Andre Vieira de Freitas Araujo.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Administração e Ciências Contábeis, Bacharel em Biblioteconomia e Gestão de Unidades de Informação, 2019.

1. Segurança da Informação. 2. Criptografia. I. Araujo, Andre Vieira de Freitas, orient. II. Titulo.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

PHIAMA HIVERA SILVA DE ALMEIDA

O SEGREDO DA COMUNICAÇÃO SECRETA: A CRIPTOGRAFIA COMO MÉTODO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de bacharel em Biblioteconomia e Gestão de Unidades de Informação.

Rio de Janeiro, 02 de Julho de 2019.

_____

Prof. Dr. Andre Vieira de Freitas Araujo
Orientador

_____

Prof. Dr. Danilo Pestana de Freitas
Membro interno

_____

Prof. Dr. Raimunda Fernanda Santos
Membro interno

Aos meus pais, meus maiores críticos e apoiadores.

Agradecimentos

Agradeço primeiramente a Deus, por me dar não o que eu queria, mas tudo o que eu precisava durante esses anos na universidade. Foram bons anos, apesar de achar que poderia ter aproveitado mais algumas oportunidades, chego ao fim de mais uma etapa com sentimento de satisfação por tudo que fiz.

Devo toda minha vida acadêmica aos meus pais, que me sustentaram de todas as formas possíveis, não sou mais uma na estatística de evasão em universidades públicas graças a eles. E quando no fim do meu projeto 1 depois de dois ataques de pânicos que tive sozinha e uma crise de ansiedade, que eu não tive como esconder por ter afetado minha integridade física, eu encontrei esperança no consolo e apoio deles. Foram minha força quando eu estava fraca e eu acreditei que poderia porque eles acreditaram em mim. Sou grata. Amo vocês.

Agradeço a minha irmã Monique, pelas conversas sobre a vida, sobre minhas disciplinas, por ouvir minhas ideias sobre trabalhos que eu nunca cheguei a apresentar e resumos que eu nunca submeti e achá-los incríveis. Por ser minha cobaia em testes, por me emprestar seu notebook por tempo integral e indeterminado para que eu pudesse escrever minha monografia, a lista é bem grande, mas um ‘obrigada por tudo’ resume bem.

Agradeço aos meus colegas de turma por fazerem da 2014.2 uma turma agradável e me trazer boas lembranças para posteridade.

Meu grupinho do canto, como eu fui feliz com vocês! Poderia escrever uma outra monografia só com nossas histórias. Cada uma de vocês me ensinou muito e estão tatuadas no meu coração. Espero tê-las sempre comigo, obrigada por cada momento.

Agradeço aos professores, que com sua grandeza honraram o título de mestres e contribuíram para que meu crescimento fosse além do ensino. Em especial meu orientador, professor Andre, por aceitar o desafio de me ajudar nessa etapa final do curso mesmo o tema escolhido não sendo da sua área de atuação, pela dedicação e por todos os “vai dar tudo certo!”, ao meu ex-orientador, Danilo por ser um professor bem acima da média e a todas as

professoras mulheres com as quais eu tive contato por me inspirarem e me fazerem enxergar as possibilidades.

Por fim, agradeço a todos que contribuíram de alguma maneira para minha permanência e conclusão na UFRJ.

Got a secret, can you keep it? Swear this one you'll save (The PIERCES, 2007).

RESUMO

A presente pesquisa propõe introduzir o estudo da Criptografia enquanto método de Segurança da Informação. Durante milhares de anos, governantes dependeram do estabelecimento de métodos seguros e eficientes para se comunicar, de modo a governar suas nações e comandar seus exércitos. Ao mesmo tempo todos estavam cientes das consequências caso suas mensagens caíssem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para força inimigas. Foi a ameaça da intercepção pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas como a criptografia para mascarar uma mensagem de modo que só o destinatário possa ler o conteúdo. A partir deste contexto, esta pesquisa é conduzida pelo seguinte questionamento: quais são as características da criptografia enquanto método de segurança da informação? Este trabalho objetiva identificar e caracterizar a criptografia como método de Segurança da Informação apresentando suas mais marcantes evoluções, técnicas e aplicações ao longo da história. Como ponto de partida definimos Segurança da Informação e exploramos seus aspectos, seguindo para o conceito de criptografia e posteriormente atender o objetivo central do trabalho. Para tanto, foi desenvolvida uma pesquisa qualitativa e exploratória que mescla os métodos bibliográfico e documental para o embasamento teórico. A partir da pesquisa realizada, compreendemos que a criptografia está posicionada como método eficiente e mais recomendado para assegurar a informação, sendo essencial no contexto atual para a troca de informações no ambiente cibernético, por tornar a comunicação ilegível, ainda que interceptada.

Palavras-chave: Segurança da informação. Criptografia. Tecnologia da Informação. História da Tecnologia.

Abstract

The present research proposes to introduce the study of Cryptography as an Information Security method. For thousands of years, rulers depended on establishing safe and efficient methods for communicating in order to rule their nations and command their armies. At the same time everyone was aware of the consequences if their messages fell into the wrong hands, revealing precious secrets to rival nations or spreading information vital to enemy forces. It was the threat of the interception by the enemy that motivated the development of codes and ciphers, techniques like encryption to mask a message so that only the recipient can read the content. From this context, this research is driven by the following question: what are the characteristics of cryptography as an information security method? This work aims to identify and characterize cryptography as a method of Information Security presenting its most remarkable evolutions, techniques and applications throughout history. As a starting point, we defined Information Security and explored its aspects, following the concept of encryption and later meeting the central objective of the work. For that, a qualitative and exploratory research was developed that mixes the bibliographical and documentary methods for the theoretical foundation. Based on the research carried out, the understanding of cryptography is positioned as an efficient and appropriate way of maintaining information, and it is essential in the current context for an information exchange in the cybernetic environment to make communication illegible, although intercepted.

Keywords: Information security. Encryption. Information Technology. History of Technology.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A expressão em latim *scientia potentia est* quer dizer: conhecimento é poder. Essa frase popularmente conhecida de Francis Bacon, em sua obra *Meditationes Sacrae* (1597), dá margem para reflexões de ângulos diferentes. Neste trabalho vamos refletir da seguinte forma: ao adquirirmos conhecimento através da informação nos tornamos arbitrariamente mais capazes pelo fato de a termos, sabermos seu uso e aplicação, sendo capazes de manipulá-la a nossa vontade. O detentor da informação certa tem impacto direto no processo de tomada de decisão, portanto, tem poder.

Desde os primeiros habitantes da Terra as relações sociais se deram visando o poder, e a informação tem sido o principal objeto de poder durante todos esses anos.

Dessa maneira os seres poderosos da terra como reis, rainhas, imperadores, presidentes e generais vem aprimorando não só suas técnicas de captação de informação e desenvolvimento de conhecimento, mas também de segurança da informação, como forma de assegurar informações vitais para manterem seu poderio.

Durante milhares de anos esses mesmos governantes dependeram de meios de comunicações eficientes para governar seus países e comandar seus exércitos. Ao mesmo tempo todos estavam cientes das consequências caso suas mensagens caíssem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da intercepção dessas informações por possíveis inimigos que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa decifrar e ler o conteúdo. A partir daí podemos identificar o fator gerador da necessidade de segurança da informação.

Com o passar dos anos as técnicas usadas para assegurar a informação foram evoluindo à medida que as técnicas para as desvendar foram obtendo sucesso, sendo a criptografia a técnica mais explorada e

desenvolvida dentre as outras, que apesar de estarem em vigor até hoje, não tem a mesma adesão da criptografia.

Durante muito tempo a Segurança da Informação não possuiu um conceito definido, quase sempre foi apresentada como um conjunto de práticas que se executadas corretamente acarretariam a segurança de suas informações. Alcoforado diz que:

> Segurança da Informação não é uma ciência exata. Se fossemos classificá-la, ela estaria no campo da Gestão de Riscos. E para gerir riscos é preciso conjugar vários verbos: conhecer, planejar, gerir, auditar, educar, monitorar, aprender e gerenciar são apenas alguns deles. (2014, p. 2).

Quando se trata de segurança da informação a princípio pensamos pelo viés tecnológico, automaticamente nos vem à cabeça sistemas de informação modernos e computadorizados. Entretanto, de acordo com o próprio manual de boas práticas de Segurança da Informação do Tribunal de Conta da União (2013), a segurança da informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas por uma instituição. Essa constatação não limita o suporte em que uma informação deve ser assegurada e sim do conjunto de características objetivadas pela segurança da informação.

Apesar disso a segurança da informação se configura atualmente apenas no ambiente eletrônico e digital, apresentando métodos de segurança que se aplicam somente nesses ambientes, não abrindo espaço para a perspectiva histórica da segurança da informação e seus métodos o que como visto anteriormente, não é uma preocupação recente e sim milenar.

Entendendo que método é uma ferramenta para alcançarmos um objetivo, podemos correlacionar a criptografia descrita por Singh (2003) como modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções, como um contundente método de segurança da informação que nem sempre é caracterizado e apresentado dessa forma na literatura, ainda que tenha um conceito bem definido a criptografia assim como outras técnicas da ciência do sigilo não está atrelada a história da segurança da informação e nem listada como método de segurança da informação que inclusive independe do meio digital.

Com esse trabalho busca-se identificar, exemplificar e explicar os principais métodos utilizados para assegurar a informação ao longo da história mencionados em registros bibliográficos, em especial a criptografia, que dentre outros métodos evoluiu e é utilizado até hoje em uma escala superior em relação aos outros. Evidenciando sua relevância no estudo e desenvolvimento da segurança da informação.

Para entender a persistência da criptografia desde seu primeiro registro na história até hoje e legitimar seu lugar como método de segurança da informação nossa questão de pesquisa é: quais são as características da criptografia enquanto método de segurança da informação?

Saindo um pouco do pensamento óbvio e senso comum sobre segurança da informação onde antivírus, firewall e criptografia quântica estão sempre elencados, pensar na origem de tudo isso e em como chegamos no momento de vigilância global que temos hoje, onde não existe privacidade e precisamos assegurar a mais simples das informações.

É importante ressaltar que em diferentes momentos da história outros métodos de segurança da informação foram surgindo de acordo com o avanço tecnológico, assim como ameaças a seguridade das informações, de acordo com Mitnick (2005) sempre haverá esse jogo de gato e rato entre especialista em segurança e invasores.

Na segunda seção, posterior a Introdução, nomeada de “Segurança da Informação” abordamos primeiro os aspectos conceituais de Segurança da Informação. Em seguida apresentamos como a Segurança da Informação tem sido gerida e regulamentada no Brasil. Por fim abordamos os aspectos políticos e sociais da Segurança da Informação no mundo.

Na terceira seção “Criptografia” a princípio abordamos os aspectos conceituais da criptografia, desenvolvemos uma perspectiva histórica estabelecendo uma base a partir da evolução da criptografia descrita por Simon Singh em seu livro[1].

Na quarta seção, “Criptografia enquanto método de Segurança da Informação” procuramos apresentar autores que corroborassem a concepção

[1] O livro dos códigos

da criptografia como método indispensável para o estabelecimento de comunicação segura atualmente, em especial na internet.

Na seção, “Considerações finais” é dissertado de forma geral os temas abordados no texto e inclui reflexões pessoais da autora do trabalho.

1.2 JUSTIFICATIVA

O ano de 2013 foi um ano marcante pra a história da segurança da informação ou a falta dela, por conta das informações divulgadas por Edward Snowden sobre os Estados Unidos estarem espionando não só diversos países e grandes empresas com a Petrobras aqui no Brasil, como também informações de cidadãos comuns por meio dessa grande rede chamada internet.

Apesar da Segurança da informação ser uma preocupação antiga como falamos anteriormente, foi a partir desse momento que se tornou mais evidente a maneira com que as informações podem ser interceptadas facilmente na atual sociedade da informação, e em como alguns países principalmente os de terceiro mundo e não tão evoluídos no quesito tecnologia, estão vulneráveis em relação às grandes potências no contexto atual com a internet e produção em massa de informação.

Com esse e outros casos de espionagem vindo à tona, a privacidade e a Segurança da Informação estão sendo debatidas de maneira não vista antes.

A ciências do sigilo e seus métodos sempre foram mantidos em segredo, de acordo com Singh (2001) departamentos e documentos secretos só vem a conhecimento da sociedade após muitos anos de obsolescência. Esse fato torna as pesquisas na área mais complexas e faz com que se atenham sempre a fatos já descobertos.

> A codificação é o único meio de proteger nossa privacidade e garantir o sucesso do mercado digital. A arte da comunicação secreta também conhecida como criptografia fornecerá os fechos e as chaves da era da informação. (SINGH, 2001, p.12)

Viver na chamada sociedade da informação é um desafio, e trabalhar com a gestão da informação é um desafio maior ainda que compete aos profissionais da ciência da informação.

> Sendo um bem, a informação pode e deve ser gerenciada, e é a base da administração dos recursos de informação, que consiste na visão integrada de todos os recursos envolvidos no ciclo de informação. Isso inclui a informação propriamente dita (conteúdo), os recursos tecnológicos e recursos humanos. (TARAPANOFF apud CARVALHO; ARAUJO JUNIOR 2001, p. 44).

Conforme Burnett, Steve e Paine (2002, p. XVII) “A ferramenta mais importante da segurança é a criptografia”. Através dos estudos sobre conceitos, características e aplicabilidades da criptografia em instituições, é possível vislumbrar a importância de o profissional da informação desenvolver competências para a gestão da segurança da informação e colaborar com a criação de políticas voltadas para essa perspectiva, considerando três pilares: tecnologia, processos e pessoas.

Entender a evolução da criptografia como método de segurança da informação e seu impacto histórico na sociedade é importante para entender esse contexto atual onde a informação ganhou ainda mais importância devido ao avanço tecnológico e a dinâmica das mudanças nos mercados de produtos e serviços.

A reflexão sobre a perspectiva histórica da Segurança da Informação tem sido negligenciada, não permitindo que certas lacunas históricas fossem preenchidas e o presente mais bem compreendido.

A Segurança da Informação e a criptografia são investigadas, sobretudo, no contexto da Ciência da Computação[2] e têm se estendido de maneira exponencial devido ao fato de, hoje, grandes massas informacionais serem produzidas e armazenadas em ambientes computacionais. A Segurança da Informação tem sido estudada pela Ciência da Computação sob uma perspectiva mais técnica, desconsiderando, normalmente, perspectivas históricas e sociais. Já a literatura acadêmica sobre este tema, no âmbito da Ciência da Informação, é reduzida; a preocupação com a proteção da informação existe, quase sempre abordando questões éticas sobre os modelos de busca, armazenamento, apropriação e uso da informação digital no contexto da web inteligente. Mas é necessária a

[2] A partir da produção científica de grupos de pesquisa como: Criptografia e Segurança da Informação (http://dgp.cnpq.br/dgp/espelhogrupo/277004); GTSeg - Gestão e Tecnologia em Segurança da Informação (http://dgp.cnpq.br/dgp/espelhogrupo/29604); Segurança da Informação, Redes e Sistemas (http://dgp.cnpq.br/dgp/espelhogrupo/208306)

capacitação dos profissionais da informação em Segurança da Informação em sentidos mais amplos para associá-la, principalmente, com a Gestão da Informação. Deste modo, é possível fortalecer a cultura da Segurança da Informação na sociedade, fomentando distintas atividades de pesquisa científica, de desenvolvimento tecnológicos e de inovação a partir do tratamento de informações secretas e com restrição de acesso.

1.3 OBJETIVOS

Objetivo geral

Identificar e caracterizar a criptografia como método de segurança da informação.

Objetivos específicos:

a) Conceituar segurança da informação;
b) Explorar os aspectos institucionais, legais, normativos, políticos e sociais globais
c) Conceituar criptografia;
d) Mapear a evolução da criptografia ao longo da história;
e) Apresentar os principais métodos e técnicas da criptografia.

1.4 METODOLOGIA

Trata-se de pesquisa teórica qualitativa e exploratória, pois preocupa-se com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais entre a criptografia e a sociedade proporcionando maior proximidade com o tema histórico e atual.

> Os pesquisadores que utilizam os métodos qualitativos buscam explicar o porquê das coisas, exprimindo o que convém ser feito, mas não quantificam os valores as trocas simbólicas nem se submetem à prova de fatos, pois os dados analisados são não-métricos e se valem de diferentes abordagens. (GERHARDT; SILVEIRA, 2009, p. 31).

O campo limita-se a uma pesquisa bibliográfica e documental, pois recorre a fontes mais diversificadas que podem apresentar referências relevantes para o tema.

A técnica de coleta de dados implementada nesta pesquisa se deu a partir do levantamento de referências exaustivas já analisadas, escritos

eletrônicos, livros, artigos científicos, websites que contenham relatos sobre Criptografia, Segurança da Informação e Gestão da Informação como palavras-chave, assim como filmes e documentários que abordem a mesma temática. Utilizando como fontes de coleta de dados Google Acadêmico, Biblioteca Digital de Teses e Dissertações (BDTD) e Brapci.

A população desta pesquisa é composta pela bibliografia encontrada como uso das palavras chaves da pesquisa já mencionadas acima e outros temas correlatos que pudessem enriquecer a discussão estabelecida. Foi dada preferência a fontes recentes para a amostra, em sua maioria escritas a partir dos anos 2000 até os dias atuais, com autores em sua maioria nacionais e algumas fontes internacionais.

2 SEGURANÇA DA INFORMAÇÃO[3]

Nesta seção citaremos alguns conceitos de Segurança da Informação, mencionaremos instituições responsáveis por introduzir propostas, leis e normas no campo a fim de situar a condição da Segurança da Informação nesses aspectos. Discutiremos questões globais e alguns desdobramentos baseados nas denúncias de espionagem sofridas pelo Brasil no ano de 2013.

2.1 CONCEITOS

Para a Ciência da Informação, dados são símbolos escritos que por si só não tem nenhum significado, e informação é conjunto de dados que juntos constroem um significado podendo ser encontrado em diferentes tipos de suporte. Fontes (2017), afirma que transformar esses dados em informação é tornar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional.

Para Terada (1988), a informação pode ser entendida como um conjunto de dados que quando colocados num contexto útil e de grande significado, têm um valor real e percebido nas ações ou decisões de quem o utiliza. A Associação Brasileira de Normas Técnicas (ABNT), através da NBR ISO/IEC 27002 afirma que:

> A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenado eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendável que ela seja sempre protegida adequadamente. (2005, p. x).

Atualmente informação representa o recurso mais precioso para uma organização, e garantir a sua segurança é um dos maiores desafios com que uma organização têm de lidar afirmam Pimenta e Quaresma (2016), embora anteriormente reconhecida apenas por seu papel como redutora de

[3] A produção científica sobre Segurança da informação no contexto da Ciência da computação pode ser consultada a partir dos grupos de pesquisa mencionados na nota anterior. Para a Ciência da Informação a Segurança da informação faz parte do escopo da Gestão da Informação e do Conhecimento. Ainda não possui um grupo de pesquisa sobre o tema que seja cadastrado na plataforma do CNPQ (plataforma utilizada para consultar a respeito dos grupos), no entanto no contexto de trabalho publicados em eventos como o ENANCIB (GT4- GIC) alguns trabalhos a respeito de Segurança da Informação começam a demonstrar de maneira gradativa o aumentos de estudos na área.

incertezas, a informação é cada vez mais vista como um recurso transformador do indivíduo e da sociedade, cabendo-lhe papel essencial no contexto socioeconômico vigente, não por acaso denominado de era da informação.

> O fato de que, cada vez mais, os recursos de tratamento da informação sejam apresentados sobre uma base tecnológica indo a que se de elevada ênfase aos aspectos tecnológicos da segurança. De fato, esta ênfase não é recente, entretanto não se deve ser a tecnologia a única nuance contemplada nem mesmo a principal. (MARCIANO; LIMA-MARQUES, 2006, p. 44).

Para Laureano e Moraes (2005), o domínio da informação sempre teve fundamental importância. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente.

A informação sempre foi importante, não é um bem adquirido com o advento da tecnologia. Nas literaturas analisadas os autores apesar de sempre se referirem a informação como um bem valioso independente da esfera, suporte e área em que ela está contida, sempre se referem a ela no contexto tecnológico ou sua relevância no ambiente organizacional de uma empresa.

E não há absolutamente problema nenhum com isso, é apenas mais uma maneira de enxergar o fenômeno da informação e gerir seus desdobramentos à medida que as necessidades aparecem.

Para Marciano e Lima-Marques (2006) os ativos da informação estão sujeitos a diversos eventos e potencialidades nocivos a sua segurança divididos em três categorias: ameaças, vulnerabilidades e incidentes, os quais compõem as caracterizam os riscos.

Ameaça é um evento ou atitude indispensável que potencialmente remove desabilita danifica ou destrói um recurso.

Vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado a informação que é passível de ser explorado por alguma ameaça.

Incidentes são eventos em que envolve uma violação de segurança.

Por sua vez, um ataque corresponde a concretização de uma ameaça, não necessariamente bem-sucedida mediante uma ação deliberada e por vezes meticulosamente planejada.

O risco pode ser definido como as perdas, incluindo perdas em vidas humanas que podem ocorrer mediante a adoção de determinado curso de ação.

> A disseminação de meios maciços de acesso à informação, com a integração organizacional por meio da informática e posteriormente com a proliferação da internet e de redes corporativas, ao qual mesmo tempo em que introduz formas de fácil e rápida utilização os recursos computacionais, expõe ainda mais a fragilidade e os riscos a que estão sujeitos os usuários, os sistemas e os dados armazenados e tratados por tais sistemas. (MARCIANO; LIMA-MARQUES, 2006, p. 47).

Para Silva e Stein (2011), o uso de senhas para obter acesso à informação envolve 2 mundos, o tecnológico e o humano, interação que naturalmente gera muitos problemas.

O elo mais fraco de um processo de segurança é a pessoa (usuário), que por sua vez é responsável por garantir a fidelidade da informação. Laureno e Moraes (2005) garantem ainda que para o planejamento estratégico da informação é de suma importância a participação de um gestor que possua as competências necessárias para avaliar o valor da informação.

> No sentido científico administrativo, estratégias têm por fim vantagens que não são apenas momentâneas, com vistas a um objetivo particular, mas que determina a possibilidade de benefício direto em cada posição que a instituição assuma ao longo de sua história. (LAUREANO; MORAES, 2005, p. 1).

De acordo com os autores, presentemente o papel dos gestores é de uma maneira geral promover os produtos e/ou serviços de uma instituição zelando por seus ativos. E que para tanto o gestor necessita de informações confiáveis que auxiliem no processo de tomada de decisão a partir de uma análise interna e externa.

> A gestão estratégica de informação e dados é fundamental para as organizações uma vez que “possibilita tomadas de decisão que sustentam outros processos de gestão e outros processos de gestão e outros processos estratégicos”. (GIMENEZ; PELISSON; KRUGER; HAYASHI, 1999 apud LAUREANO; MORAES 2005, n.p).

Para Maciano e Lima-Marques (2006), o conceito de Segurança da Informação ainda é muito abstrato e a literatura especializada é pródiga nas apresentações do conceito do que a segurança da informação faz e de quais são os domínios de sua atuação, mas não do que ela de fato é, diz ainda que muito se fala sobre a perspectiva funcional da segurança, mas são escassas as análises descritivas da segurança da informação.

> A segurança da informação objetiva a preservação da confidencialidade, integridade e disponibilidade da informação, adicionalmente, outras propriedades tais como autenticidade, responsabilidade, não repúdio e confiabilidade. ‘A segurança compreende, assim a proteção das informações em relação aos diversos tipos de ameaças para garantir a continuidade do negócio’. (FERREIRA; ARAÚJO, 2008, p. 12).

Sêmola (2014), afirma que não há uma ciência exata quando se trata de Segurança da Informação e sim uma série de ações que visam a prevenção de possíveis riscos que a informação pode correr, reiterado por Bugs (2010), que apresenta Segurança da Informação como um conjunto de princípios, técnicas, protocolos, normas e regras que visam garantir um melhor nível de confidencialidade da informação.

Silva e Stein (2011, p.4) resumem Segurança da informação como a “proteção contra o uso ou acesso não autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas ”.

“A segurança da informação não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados em qualquer ferramenta.” (GUEDES, 2015, p. 30).

> Entretanto, as formas correntes de implementação de mecanismos de segurança em sistemas de informação, como a criptografia, que é utilizada como prevenção ou solução para falhas em segurança na ampla maioria dos casos, são notadamente técnicas, e tendem a ser em grau cada vez maior, haja vista o fato de que as iniciativas apresentadas se basearem em atualizações e sofisticação da tecnologia. (MARCIANO; LIMA-MARQUES, 2006, p. 22).

Ferreira e Araújo (2008) definem Segurança da Informação como a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive a segurança dos recursos humanos.

Para Fontes (2017) Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

Apesar da elaboração de políticas, regulamentos, métodos e várias ferramentas que visam a segurança da informação sejam importantes, é necessário que todos os envolvidos no processo de proteção da informação estejam cientes do assunto.

Como Laureno e Moraes (2005) disseram anteriormente, o usuário é o ponto mais fraco do processo de Segurança da Informação, por conta de toda subjetividade e influência a que está sujeito, diferentes de atividades não humanas, que se realizam por meio de um padrão invariável, como o código binário de um computador.

Logo, para nós usuários da informação, tomar ciência da segurança da informação e seus desdobramentos torna-se fundamental para anularmos essa fragilidade, já que somos os gestores do processo e temos a informação como matéria prima no dia-a-dia e precisamos desenvolver competências para gerenciar a informação em diferentes níveis e esferas inclusive o modo como assegurá-las.

2.2 ASPECTOS INSTITUCIONAIS, LEGAIS E NORMATIVOS

Já falamos da preciosidade da informação e da evidente necessidade de protegê-la por seu grande potencial valorativo. Com esse cenário, a Segurança da Informação torna-se peça fundamental no processo de gestão da informação em qualquer organização, e a elaboração regulamentos, leis e o estabelecimento de padrões é uma necessidade subsequente.

Tanto Fontes (2008) quanto Sêmola (2014) apontam a informação como o sangue de uma organização e ativo mais importante de uma empresa. Evidentemente, necessitam mais do que a elaboração de políticas internas para gerir e proteger suas informações, precisam de órgãos que estabeleçam diretrizes que sirvam como referências legais e normativas para seus processos.

No Brasil, a Segurança da Informação é tratada pelo Gabinete de Segurança Institucional da Presidência da República (GSI), que existiu em várias formulações desde sua criação em 1999. Na sua composição atual, aprovada pelo decreto nº 9.668 de 02 de Janeiro de 2019, tem entre outras responsabilidades planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela

incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamentos de segurança e o tratamento de informações sigilosas. O GSI a briga o Departamento de Segurança da Informação e Comunicações (DSIC) que, de acordo com Monclaro (2008), foi criado para ser o braço executivo do GSI nas ações de coordenação de segurança da informação e comunicações.

O decreto nº 9.637 de 26 de dezembro de 2018 que institui a Política Nacional de Segurança da Informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Nessa política podemos sumarizar como principais responsabilidades:

> A. Acompanhar em âmbito nacional e internacional a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação.
> B. Estabelecer norma sobre a definição dos requisitos metodológicos para implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal;
> C. Aprovar diretrizes e estratégias normas e recomendações;
> D. Elaborar apoiar a elaboração dos planos nacionais vinculados a estratégia nacional de segurança da informação;
> E. Estabelecer critérios que permitam monitoramento e avaliação da execução das políticas nacionais de segurança da informação e seus instrumentos.
> F. Elaborar e implementar programas sobre segurança da informação destinados a conscientização e capacitação de servidores públicos federais e da sociedade. (BRASIL, 2018, n.p.)

Para ajudar o GSI no cumprimento de seus objetivos, foi criada a Rede Nacional de Segurança de Informação e Criptografia (RENASIC), que é uma iniciativa do Centro de Defesa Cibernética do comando do Exército para promover avanços científico-tecnológico na segurança das informações, criptografia e defesa cibernética do país.

De acordo com a Agência Brasileira de Inteligência (ABIN) [4]o principal objetivo do RENASIC é elevar a competência brasileira nesse campo tecnológico por meio da cooperação entre órgãos públicos, universidades, institutos de pesquisa e instituições privadas. O RENASIC é composto por um

[4] Disponível em: http://www.abin.gov.br/atuacao/cooperacao/cooperacao-nacional/

comitê diretor, comitês técnico-científico, laboratórios de pesquisa e grupos de trabalho.

O RENASIC organiza um seminário (SENASIC) anual que objetiva apresentar aos participantes e membros da comunidade segurança informação e criptografia a estrutura da RENASIC, discutir as várias tecnologias consolidadas e outras que estão surgindo no ambiente científico e tecnológico mundial.

No decorrer dos anos o Brasil foi percebendo a necessidade de assegurar a informação e além de estabelecer organizações dentro do governo que se responsabilizassem pela segurança da informação em específico, desenvolveu leis que garantissem essa seguridade em âmbito nacional.

> Os códigos penais especiais foram afetados por essa nova realidade, porque o direito penal tradicional é fortemente ligado a questões da soberania nacional enquanto a internet por sua vez, não conhece Estados por ser manifestação de uma verdadeira “aldeia global”. (TOMASEVICIUS FILHO, 2016, p. 272).

À medida que o tempo foi passando e com a troca de presidentes a legislação foi sendo alterada, e leis pertinentes a segurança da informação foram revogadas por outras, as principais leis remanescentes no tocante ao tema se encontram abaixo:

A lei nº 12.965/2014 mais conhecida como Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. Para Bragatto; Sampaio e Nicolás (2015) o Marco Civil da internet foi evidenciado como uma lei de vanguarda no que tange à proteção da privacidade de usuários, liberdade de expressão e neutralidade

A lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais foi a lei mais recente implementada no que e refere a Segurança da Informação no Brasil, atualizando alguns artigos da lei do Marco Civil da Internet. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

No âmbito normativo a *International Organization for Standardization* (ISO), uma organização internacional que desenvolve e publica documentos responsáveis por estabelecer padrões internacionais em diversas áreas de atuação, lançou guias que tratam de vários aspectos da segurança com a finalidade de padronizar a gestão da Segurança da Informação definindo o caminho a ser seguido para a obtenção da segurança da informação. Abaixo estão listadas as principais publicações da ISO a respeito do tema:

ABNT NBR ISO IEC 17799: 2005. Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005a)

ABNT NBR ISO/IEC 27001:2005. Esta Norma fornece diretrizes para o processo de gestão de riscos de segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005b)

ABNT NBR ISO/IEC 27001:2013. Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013)

ABNT NBR ISO/IEC 27002:2013.Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013)

2.3 ASPECTOS POLÍTICOS E SOCIAIS GLOBAIS

Tanto Snowden (2014) quanto Assange (2015) mencionam que o 11 de Setembro contribuiu de maneira singular para que a vigilância fosse aplicada de modo maciço com a justificativa de agir em prol da segurança

nacional estadunidense e fazer com que o fenômeno que Bauman (2014) chama de “regime de vigilância” fosse implementado no cotidiano de milhões de pessoas nos EUA e posteriormente no mundo todo.

Bauman (2014) diz que “os olhos eletrônicos sempre abertos nas ruas, a coleta de dados abrangente, os fluxos de informações pessoais com sua pressão cada vez mais alta são vistos como reações racionais aos riscos da vida”. Pouco a pouco estamos abrindo mão da nossa liberdade em função de uma suposta segurança.

> Esse é o paradoxo de nosso mundo saturado de dispositivos de vigilância, quaisquer que sejam esses pretensos propósitos: de um lado, estamos mais protegidos da insegurança que qualquer geração anterior, de outro, porém, nenhuma geração anterior pré-eletrônica vivenciou os sentimentos de insegurança como experiência de todos os dias. (BAUMAN, 2014, p. 73).

Julian Assange (2015) em seu livro diz que o Google se tornou uma corporação que integra sistema de controle, a vigilância e expansão do poder do Estado estadunidense, onde o poder não se exerce apenas por meio da tecnologia, mas está embutido na própria tecnologia e que as “redes digitais e seus dispositivos não são neutros” (SILVEIRA, 2015, n.p). O autor continua afirmando que os arranjos e limites dessas redes digitais “em protocolos e códigos são programados para cumprir determinações, muitas vezes de ordem geoestratégica, política e econômica”.

O autor afirma que os algoritmos do Google e do Facebook não funcionam de maneira aleatória ou subjetiva, ele faz exatamente aquilo que foi programado para fazer.

Uma experiência de que a tecnologia não está ausente por exemplo da política que podemos citar as eleições para presidência dos EUA do ano de 2016. Em uma reportagem da BBC de 2017 que apresentou o relatório divulgado pela inteligência dos EUA que constatou não haver provas concretas sobre a interferência do presidente russo Vladimir Putin na campanha contra Hillary Clinton, mas afirma que as ações da Rússia incluíram: Hackear e-mails de contas do Comitê Nacional Democrata e de membros da alta cúpula do partido; Usar intermediários como WikiLeaks, DCLeaks.com e Guccifer 2.0 para publicar informações adquiridas no

hackeamento; Usar propaganda financiada pelo Estado e pagar usuários de mídia sociais ou "trolls" para fazer comentários desagradáveis sobre Hillary.

Para o jornal El País em o Facebook reconheceu que até 126 milhões de seus usuários foram expostos a uma empresa alemã chamada Internet Research Agency, ligada ao Kremlin e o Twitter identifico 3.814 contas com a finalidade de emitir propagandas contra a candidata Hillary Clinton durante as eleições presidenciais estadunidenses de 2016 e com a conclusão do relatório a inteligência dos EUA disse: “Nós entendemos que o presidente russo solicitou uma campanha para interferir na eleição americana de 2016”.

Podemos concluir que os usuários desses sistemas inteligentes e seus aparelhos que podem ampliar, limitar e moldar nossa maneira de nos comunicar e como interagimos com ela que quem programa esses sistemas obtêm controle de nós que fazemos uso deles.

Essas tecnologias fechadas, onde programador tem controle total do que é desenvolvido e que são disseminadas em larga escala por organizações de grande porte são de acordo com Assange (2014) a base da espionagem e vigilância massiva executadas por agências de inteligência do EUA e seus aliados.

No ano de 2013, o ex-agente da Agência de Segurança Nacional (NSA) dos Estados Unidos da América, Edward Snowden denunciou a existência de um programa de espionagem chamado PRISM usado pela NSA para coletar informações, como histórico de pesquisa, e-mails, arquivos, fotos, chamadas de vídeo e voz e muito mais de qualquer usuário. Segundo Snowden a NSA tinha 3 maneiras de coletar os dados de vigilância, eles eram: Através de da cooperação entre empresas de telecomunicações (dados dos usuários fornecidos por essas empresas); Cooperação entre agências de inteligência (como o MI6 britânico) e interceptando os dados ainda nos cabos da internet.

Segundo Assange (2014), no caso denunciado por Snowden, a NSA tinha acesso a servidores de empresas como Google, Facebook e Microsoft, podendo invadir o computador de qualquer pessoa que utiliza-se um sistema operacional da Microsoft (windows). O autor afirma ainda que tais empresas além de terem ciência desse acesso ainda cooperam declaradamente com iniciativas como esta, afirmativa que podemos comprovar com a declaração dos diretores destas empresas (Facebook e Oracle) em colaboração com a

lei “*Cyber Intelligence Sharing de Protection Act*” (CISPA), que visa legalizar a vigilância através do compartilhamento de informações cibernéticos dos usuários com as agências de inteligência estadunidenses com a justificativa de que é uma medida de segurança das redes de informação tornando lícito a parceria corporativa de compartilhamento de dados.

Segundo Bridi (2014) Snowden entregou documentos ultrassecretos para jornalistas conceituados, entre eles Glenn Greenwald de redes renomadas de comunicação como o jornal *The Guardian*, que provavam que agências de inteligência estadunidenses espionavam e mantinham vigilância sobre empresas como a Petrobras aqui no Brasil, a Huawei (empresa de tecnologia) na China, além de mensagens de texto e telefonemas de chefes de Estado como a então presidente do Brasil Dilma Rousseff e a chanceler alemã Angela Merkel.

Logo depois a divulgação desses fatos a então presidente Dilma em seu discurso na Assembleia Geral Organização das Nações Unidas (ONU) em 2013 ressaltou que as informações obtidas pela “espionagem colaborativa com entre Canadá e Estados Unidos não tinham relação com ameaças terroristas, mas sim dados pessoais de cidadãos comuns e informações estratégicas empresariais e de valor econômico” (ASSANGE, 2015, n.p.) e que era necessário a elaboração de políticas que assegurassem as informações e que os direitos humanos como privacidade e liberdade de expressão fossem respeitados e garantidos.

Enquanto isso, aqui no Brasil a presidente Dilma pediu celeridade no desenvolvimento da lei que ficou conhecida como Marco Civil da Internet que tem como objetivo efetivar a neutralidade da rede, a liberdade de expressão, criação e navegação, bem como a privacidade online. Para Silveira (2015) o Brasil com seus inúmeros coletivos culturais, defensores da liberdade de expressão e dos direitos humanos contribuiu para a resistência à vigilância global e tornasse possível a existência de uma lei colaborativa como o Marco Civil da Internet que conseguiu envolver diferentes setores da sociedade e do governo.

Em entrevista a jornalista Sônia Bridi da Globonews em 2014, Edward Snowden declarou que as autoridades estão tão blindadas do público por níveis de acesso, sigilo e por não precisarem prestar contas, que podem

cometer um erro ou até mesmo algum crime e nunca ter que responder por isso. Isso é extremamente perigoso, principalmente quando se trata de uma organização poderosa, como foi o caso, uma decisão ruim pode afetar milhões de pessoas, é necessário responsabilidade. Para ele a questão é a liberdade, e convida a reflexão: até que ponto um indivíduo deve ser livre? Até que ponto podemos ligar para amigos, namorados, andar de ônibus, comprar um livro, assistir a um filme, sem que isso seja gravado?

De acordo com Snowden (2014), esse tipo de invasão só seria justificável caso a pessoa tivesse um envolvimento com atividades criminosas, e ainda assim seria necessária uma autorização judicial para tanto.

Ele ainda afirma que a vigilância é tão massiva que até mesmo videogames, jogados online, em todo o mundo são monitorados pelas inteligências com a justificativa de ser utilizada por terroristas e espiões, o que em sua visão não é verdade por não ser um meio de comunicação seguro, nem mesmo criptografado, o que é de extrema preocupação para organizações como essas.

Para Snowden (2014) não há explicação para que agências de inteligência estadunidenses espionem empresas de petróleo no Brasil e muito menos e-mails de sua então chefe de Estado, ainda mais sendo países que são aliados. Que tipos de benefícios os EUA poderiam obter com essa vigilância se não políticos? Esses programas como Snowden diz: “[...] não salvam vidas, não evitaram crimes e nem promovem interesses” dos seus respectivos países (2014).

Ele diz que a solução para que nós estejamos protegidos é que os governos invistam em educação e pesquisas que permitam proteger as comunicações não de pessoa A ou organização B, mas o mundo todo. Isso é possível por meio de avanços tecnológicos e padrões internacionais de comunicação que abranjam o mundo todo já que a internet é uma rede global. Já que a melhor lei não pode ser plenamente eficaz por não se aplicar a redes além fronteira.

O jornal *The Washinton Post* (2014) publicou em respostas as revelações de Edward Snowden sobre a vigilância global feita pela NSA, que o então presidente dos EUA Barack Obama criou um grupo presidencial para revisão em inteligência e tecnologia de comunicações para avaliar os

resultados da NSA a respeito do programa Prism. Esse grupo concluiu que o programa de vigilância da NSA não era essencial para a prevenção de ataques terroristas, e que as informações necessárias em caso de terrorismo poderiam ser recolhidas por meios convencionais. O que contrariava as palavras do então diretor da NSA Keith Alexander, que até aquele momento afirmava que o programa tinha prevenido uma série de ataques terroristas. A equipe chegou à conclusão que o programa PRISM não foi relevante na prevenção de nenhum ataque terrorista, Obama então entendeu que por tanto não havia razão para que houvesse manutenção do programa e também não havia justificativa para as ações tomadas durante a execução do programa e decidiu suspender o programa.

> Somente quando as pessoas conhecem os verdadeiros planos e comportamentos de seus governos que podem escolher significativamente apoiá-los. Historicamente as formas as mais resilientes de governo aberto são aquelas em que a publicação e a revelação são protegidas. Onde essa proteção não existe é a nossa missão fornecê-la. (ASSANGE, 2015, n.p.)

A Wikipédia define Wikileaks[5] como uma organização sem fins lucrativos, que realiza em sua página na internet postagens anônimas de documentos com conteúdo confidencial, vazadas de governos ou empresas, sobre diversos assuntos, que geralmente são ocultados do conhecimento da sociedade.

Fundada por Julian Assange em 2006 a Wikileaks visa garantir que os governos sejam transparente com a população de uma maneira ou de outra, e tem uma plataforma colaborativa e anônima, que permite que qualquer pessoa publique informações anonimamente, sem que sejam identificadas e acusadas de traição ou algo do tipo.

O site é totalmente criptografado e extremamente seguro de acordo com seus colaboradores. Assim esperam encorajar cidadãos conscientes de comportamentos consequentemente antiéticos de seus governos e passem a denunciá-los, deste modo podem prestar contas de suas ações a sociedade, os órgãos competentes podem aplicar as punições cabíveis de acordo com a lei e as pessoas podem decidir que posicionamento tomar e cobrar por aquilo que acham correto.

[5] Disponível em: https://pt.wikipedia.org/wiki/WikiLeaks

Quanto a autenticidade das informações, a Wikileaks conta com uma equipe de colaboradores especialistas em diversas que examinam e realizam uma análise forense nos documentos.

A constante busca por um método de segurança como a criptografia entra em conflito com as necessidades de manutenção de leis e da segurança nacional, em especial no âmbito da internet. Apesar do grande avanço que é o surgimento de leis como o Marco Civil da Internet, é importante lembrar que a internet é uma rede mundial que vai além de qualquer fronteira. Leis territoriais não são eficientes quando se tratam de atividades que ocorrem na internet, é necessário que sejam elaboradas leis que tenham validade mundial, que podem partir de organizações internacionais como a ONU, que tem representantes de diversas nações.

À medida que nos aprofundamos nesse nem tão novo século XXI, defensores das liberdades civis como Wikileaks (na figura muitas vezes de seu criador Julian Assange) e Edward Snowden começam a pressionar pelo uso generalizado da criptografia para proteger a privacidade dos indivíduos. Trazendo a tona fatos como os narrados acima para que as pessoas possam se tornar conscientes e escolham a sociedade em que querem viver.

3 CRIPTOGRAFIA

Nessa seção abordamos alguns conceitos a respeito da criptografia, além de apresentarmos suas mais marcantes evoluções, técnicas e aplicações ao longo da história. Partindo do primeiro relato registrado até o princípio da utilização em computadores

3.1 CONCEITOS[6]

Derivada da palavra grega *Kriptos,* que significa oculto e *graphein*, que significa escrever, a criptografia de acordo com Revivest (1990), é o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros.

O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado.

> Criptografia é a ciência ou a arte de escrever mensagens em forma cifrada ou em códigos. Basicamente, é o método utilizado para alterar os caracteres originais de uma mensagem por outros caracteres, ocultando a mensagem. É parte de estudos que trata das comunicações secretas. (BUGS, 2010, p. 3).

Uma mensagem codificada deve ser sigilosa, ou seja, somente aquele que enviou a aquele que recebeu devem ter acesso ao conteúdo da mensagem. (BUGS, 2010).

Um código envolve a substituição de uma palavra ou frase por uma palavra, um número ou um símbolo. Uma alternativa ao código é a cifra, uma técnica que age no nível mais fundamental onde as letras, no lugar das palavras, são substituídas.

Singh explica e conceitua os principais termos utilizados na composição da criptografia básica:

---

[6] A criptografia tem sido desenvolvida ao longo dos anos por predominantemente matemáticos. O avanço de seus estudos e técnicas contribuiu de maneira determinística para o surgimento dos computadores e a maneira como eles funcionam, como veremos na subseção a seguir, contribuindo para que a criptografia também se tornasse um estudo da Ciência da Computação. Nessa seção os estudos encontrados e analisados são predominantemente de matemáticos, físicos e profissionais da computação.

> Um **código** é definido como uma substituição de palavras ou frases, enquanto **cifra** é definida como uma substituição de letras. Por esse motivo, o termo **cifrar** significa misturar uma mensagem usando uma cifra, enquanto, enquanto **codificar** significa ocultar usando código. De modo semelhante, a palavra decifrar se aplica à tradução de uma mensagem cifrada e decodificar a tradução de uma mensagem codificada. (2003, p. 47).

Ainda de acordo com o autor os termos encriptar e decriptar são gerais e servem tanto para códigos quanto para cifras.

A Wikipédia [7]afirma que criptografia vai além de cifragem e decifragem. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento, incluindo autores como Maquiavel, Sun Tzu e Karl von Clausewitz.

Para Marcacini (2010), criptografia é definida como a arte de escrever em cifra ou em código, de modo a permitir que somente quem conheça o código possa ler a mensagem essa é uma definição que remonta e suas origens artesanais.

> Atualmente a criptografia é considerada uma ramificação da criptologia, que por sua vez, dado o grau de sofisticação e de embasamento teórico que envolve o seu estudo, é hoje considerada uma ciência no campo das ciências exatas. E ao lado de técnicas criptográficas para cifrar a mensagem, o estudo dos métodos para decifrá-la, sem conhecer a senha, é chamado de criptoanálise, constituindo-se em outra subdivisão da criptologia. (MARCACINI, 2010, p. 19).

O uso da criptografia não é recente e ao longo dos tempos teve larga aplicação estratégica e militar (GROENWALD; FRANKE; DE ASSIS, 2012), a necessidade de enviar mensagem às tropas, que não pudessem ser compreendidas pelo inimigo, caso o mensageiro caísse em suas mãos, desenvolver a arte de escrever em código e, evidentemente, fez crescer paralelamente a criptoanálise artes de quebrar o código e decifrar a mensagem alheia.

Em um trecho de seu livro Steven Burnett (matemático e engenheiro criptográfico) e Stephen Paine (engenheiro de sistemas) dizem que a criptografia é a ferramenta mais importante de segurança e que deve ser de conhecimento de todos que participam do processo de segurança:

> Desenvolvedores e engenheiros precisam entender a criptografia a fim de construir eficazmente seus produtos. O pessoal de marketing e de vendas precisa entender a

[7] Disponível em: https://pt.wikipedia.org/wiki/Criptografia

> criptografia a fim de provar que seus produtos são seguros. Os clientes compram esses produtos, sejam eles usuário finais ou a gentes de empresas, precisam entender a criptografia, para que possam tomar a melhor decisão e assim utilizar esses produtos corretamente. Os profissionais de TI precisam entender criptografia a fim de distribuí-la adequadamente entre seus sistemas. Mesmo advogados precisam entender de criptografia, visto que os governos locais, estaduais e federal estão aprovando novas leis que definem as responsabilidades das entidades que detêm as informações privadas do público. (2002, n. p.)

A principal vantagem da criptografia é que se a informação cair em mãos de terceiros a mensagem é ilegível por conta da cifragem tornando-o incompreensível.

Marcacini (2010), considera que a criptografia seja tão antiga quanto a própria escrita. Há indícios de que, na antiguidade foi conhecida no Egito, Mesopotâmia, Índia e China, mas não se sabe bem qual foi a sua origem, e pouco se sabe acerca de seu uso nos primórdios da história.

3.2 HISTÓRIA DA CRIPTOGRAFIA[8]

O primeiro relato sobre criptografia mencionado por Singh (2003) em seu livro traz a cifra de César, uma cifra de substituição monoalfabética, em que uma letra é substituída por outra, a chave é definida pelo alfabeto cifrado, que pode ser um rearranjo qualquer do alfabeto original. Utilizada com frequência pelo imperador romano Júlio César para fins, entre outros, militares. Os detalhes da cifra de César encontram-se em “As Vidas dos Césares” escrito no século II por Suetônico. Nesta cifra ele substituía todas as letras na mensagem por outra letra que estivesse três casas a frente no alfabeto. Veja como funcionava no exemplo a seguir:

Alfabeto original: A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-X-Z

Alfabeto cifrado: D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-X-Z-A-B-C

texto original: recuem as tropas

texto cifrado: uhfzhj dv xursdv

[8] Esta subseção aborda de maneira resumida os relatos sobre a evolução da história da criptografia reportadas por Simon Singh em seu livro “O livro dos códigos”. Obviamente outros materiais foram consultados, mas em sua maioria serviram como checagem para fatos relatados no livro de Singh (2003).

Esse tipo de cifragem apesar de simples e fácil, para época fornecia um alto nível de segurança. Pois para decifrar essa mensagem o decifrador teria que verificar todas as possibilidades.

Avançando, o autor disserta sobre as contribuições dos árabes para a criptografia. Destaca que a próspera civilização islâmica dependia de uma eficiente administração e administradores que por sua vez dependiam de comunicações seguras por meio de códigos. Além dos segredos de Estado, os registros de impostos também eram codificados, demonstrando um amplo e rotineiro uso da criptografia, incluindo manuais administrativo, como o *adab al-kuttab* do século XX (manual do secretário), que inclui uma seção específica sobre criptografia. Esses administradores além da cifra de César que faz uso apenas de letras do alfabeto, acrescentavam outros tipos de símbolos. Por exemplo, substituir a letra P no alfabeto original por % ou a letra A por # e por aí vai. Apesar disso a maior contribuição dos estudiosos árabes nessa ciência foi a capacidade de quebrar as cifras, chamada de criptoanálise, a ciência que permite decifrar uma mensagem sem conhecer a chave para desencriptá-la. Técnica resumida da seguinte forma por al-Kindi:

> Um meio de ser decifrar uma mensagem codificada, quando conhecemos seu idioma, e encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página. Então contamos a frequência com que cada letra aparece. A letra que aparecer com maior frequência chamamos de primeira, enquanto a segunda mais frequente recebe o nome de segunda e assim por diante, até contarmos todas as letras diferentes no texto.[...] Descobrindo qual o símbolo que aparece com maior frequência e o transformamos na primeira letra do texto que usamos como amostra [...] e assim por diante, até convertemos todos os símbolos do criptograma que desejamos decifrar. (2003, p. 34).

Essa técnica é conhecida como análise de frequência, desenvolvida entre os anos 800 e 1200 pelos árabes e posteriormente utilizada por todo o mundo para decifragem.

Durante esse mesmo período na Europa o estudo da escrita secreta era incentivado apenas nos mosteiros, onde os monges se dedicavam a pesquisar a bíblia na busca por significados oculto.

O primeiro fato histórico sobre criptografia mencionado por Singh em seu livro traz a trágica história da rainha Maria I da Escócia (1542-1586). Na época a Inglaterra era governada pela rainha Elizabeth I que não era bem

aceita pela nobreza por ser protestante. Um grupo de nobres católicos conspirava contra ela e tinha o objetivo de substituí-la Maria I rainha da Escócia, católica e prima de segundo grau de Elizabeth I. Presa acusada por traição, Maria se correspondia com os conspiradores através de cartas cifradas, o que a deixava segura de que ainda que as cartas fossem interceptadas os agentes de Elizabeth não teriam provas que justificassem seu envolvimento com os conspiradores, logo, não seria executada. No entanto Sir. Francis Walsingham secretário de Elizabeth era também o chefe da espionagem inglesa e encaminhou as cartas para Thomas Phelippes, o maior especialista em quebra de códigos no país, que decifrou as cartas dando as provas necessárias para a execução de Maria e dos outros conspiradores (Fig. 1). Com isso, claramente era necessário o desenvolvimento de uma nova cifra, mais forte que dificultasse a criptoanálise, pois a cifra de substituição monoalfabética já não era mais eficiente.

Figura 1 - Execução de Maria Stuart, rainha da Escócia

Fonte:https://rainhastragicas.com/2016/02/08/o-ultimo-ato-de-uma-rainha-a-execucao-de-mary-stuart/ (2016)

Por volta do ano 1562 o diplomata francês Blaise de Vigenère(Fig. 2). tomou conhecimento dos estudos criptográficos de Johannes Trithemius, Giovanni Porta e Leon Battista Alberti em uma visita diplomática a Roma, que após ter acumulado dinheiro suficiente abandonou a carreira para dedicou-se ao desenvolvimento de uma nova cifra.

Figura 2- Blaise Vigenère

Fonte: https://pt.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re (2012)

Juntando as ideias dos criptógrafos anteriores mencionados, Vigenére desenvolveu sua cifra (Fig. 3), que consiste em um quadro que contém 26 alfabetos distintos para criar uma mensagem cifrada.

Figura 3 – Quadro cifra Vigenére

Tabela 3 O quadrado de Vigenère.

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: (SING, 2003, p.66)

A diferença entre esta cifra e a de César é que uma linha diferente do quadro é usada para codificar letras diferentes da mensagem e para o destinatário é necessário o acordo de uma palavra chave para que ele saiba a mudança das linhas. Por exemplo: supondo que a mensagem a ser criptografada é “ataque ao amanhecer” e a palavra-chave seja “morte”

palavra-chave M O R T E M O R T E M O R T E M O

Texto original A T A Q U E A O A M A N H E C E R

texto cifrado M H R J Y Q M F T Q M B Y X G Q F

A palavra-chave é escrita e repetida acima da mensagem para que cada letra da mensagem fique associada a uma letra da palavra. Para cifrar a primeira letra, A, identificamos a letra da palavra chave acima, que é M, que define a letra do quadro Vigenère que será usado, no caso a linha 12 e assim por diante como demonstrado no exemplo acima. A enorme vantagem da cifra

de Vigenère é que ela é imune à análise de frequências por isso, ficou conhecida por quase dois séculos, como a cifra indecifrável.

Apesar de ser muito mais segura, essa cifra desestimulou a muitos por ser muito trabalhosa e demorada. As pessoas preferiam utilizar a cifra de César para garantir sua privacidade em níveis menores como por exemplo em diários, já em casos de segurança mais sérios como em assuntos de governo, os criptógrafos tentavam desenvolver uma cifra intermediária que não fosse fácil de decifrar e que também não demorasse para ser codificada.

Mesmo sendo tão mais complexa, a cifra de Vigenère foi quebrada pelo matemático inglês Charles Babbage, por volta de 1850, que fez um estudo do padrão que a palavra-chave criava ao ser repetidamente utilizada, ao longo do texto.

Em seguida o autor relata sobre a Grande Cifra Luís XIV, inventada por pai e filho, Antoine e Bonaventure Rossignol. Se tornaram famosos após em 1626 receberem uma carta codificada interceptada de um mensageiro na cidade sitiada de Réalmont e decifrá-la antes do fim do dia, o exército de huguenotes que havia tomado a cidade estava à beira de um colapso, sabendo disso o exército francês retomou a cidade. A relevância dessa quebra de cifra foi tão importante que os Rossignol se tornaram membros da corte e serviram a Luís XIII e posteriormente Luís XIV como criptoanalistas. Eles inventaram a Grande Cifra que era tão segura que desafiou os esforços de todos os criptoanalistas inimigos para tentar roubar as informações, o que nunca aconteceu. No entanto com a morte de pai e filho a Grande Cifra caiu em desuso e muitas informações foram perdidas por ainda estarem cifradas e ninguém mais além dos Rossignol saberem como decifrar. Esse conhecimento que ficou perdido até o século XIX, quando em 1890 cartas cifradas pela a Grande cifra foram encontradas e entregues a Étienne Bazaires (membro do Departamento Criptográfico do Exército francês) que dedicou longos anos para a quebra dessa cifra utilizando a análise de frequência da sílabas comuns no idioma francês e não apenas nas letras mais frequentes. Com os documentos finalmente decifrados depois de mais de 200 anos Bazaires foi o primeiro a encontrar evidências da verdadeira identidade de uma das lendas mais antigas da França, O Homem da Máscara de Ferro.

Nos anos 1700 o autor aponta a industrialização da criptoanálise com a organização de equipes governamentais trabalhando para decifrar cifras complexas. De acordo com ele as potências europeias tinham um centro para decifrar mensagens e guardar informações chamadas de Câmaras negras. A câmara mais famosa ficava em Viena era uma espécie de correio e nela eles interceptavam todas as cartas que chegavam com destino às embaixadas em Viena, faziam uma cópia em no máximo 3 horas e as selavam novamente para que fossem entregues ao destinatário. A cada dia, centenas de cartas passavam pela câmara negra de Viena e as cópias depois de decifradas além de fornecer informações aos imperadores da Áustria, a câmara também vendia informações colhidas para outras potências.

Já nos anos 1800 na América do norte Samuel Morse construíra a primeira linha telegráfica, um sistema cobrindo uma distância de 60 quilômetros entre Baltimore e Washington. Usou um eletromagneto para amplificar o sinal, de modo que ao chegar ao receptor realizava uma série de marcas curtas e longas no papel, com pontos e traços conhecidos hoje como código Morse que criou um receptor acústico, assim o receptor da mensagem poderia ouvir bips que representassem cada letra.

Tanto o telégrafo quanto o código Morse não são formas de criptografar a informação, o código Morse é uma espécie de alfabeto alternativo que representa letras para a transmissão telegráfica, logo não há segurança uma vez que o telegrafista tem acesso à informação e algumas mensagens são mais delicadas do que outras.

O desenvolvimento do telégrafo despertou o interesse comercial pela criptografia popularizando o interesse do público pelo assunto. As pessoas escreviam suas mensagens e passavam para o telegrafista que passava a conhecer, mesmo que sem querer, o conteúdo das mensagens, mensagens essas que poderiam ter conteúdos extremamente pessoais. Logo, o povo se tornou consciente da necessidade de proteger suas informações e passou a fazer o uso de cifras nos telegramas. As cifras usadas pelo povo não eram de alta complexidade, um criptoanalista poderiam facilmente desvendar a mensagem, mas era o suficiente para evitar curiosos. A partir daí as pessoas se habituaram com o uso de cifras e as habilidades criptográficas apareciam de diversas maneiras, não só pelo telégrafo.

Singh conta a história de uma jovem casal inglês da era vitoriana que impedidos de se comunicarem pelos pais trocavam mensagens cifradas por meio da colunas de jornais dedicadas às mensagens dos leitores, uma dessas mensagens na qual os jovens planejavam fugir foi decifrada por criptoanalista, que usando a mesma cifra na coluna de jornal desencorajou os jovens a não fugirem obtendo a seguinte resposta sem cifragem: “querido Charlie, não escreva mais. Nossa cifra foi descoberta.” (SINGH, 2003, p. 98).

No século XIX a popularização da criptografia fez com que técnicas criptográficas começassem a aparecer em livros de literatura, o autor cita obras como, ‘Viagem ao centro da Terra’ e ‘Mathias Sandorff’ de Júlio Verne, as aventuras de ‘Sherlock Holmes’ de Sir Arthur Conan Doyle e também o ‘Besouro dourado’ de Edgar Allan Poe como ficções criptográficas de sucesso.

No final do século XIX o telégrafo já era o meio de comunicação muito bem difundido, no entanto a necessidade de fios para o seu funcionamento limitava sua utilização. Na virada do século o físico Guglielmo Marconi desenvolveu um aparelho que não dependeria de fio algum, apenas sinais transmitidos pelo ar através de correntes elétricas, nascia então o rádio. Os militares ficaram fascinados com a possibilidade de uma comunicação direta à longa distância, entretanto nada impedia que inimigos também captassem os sinais do rádio, logo, era necessária uma forma de encriptar as mensagens para assegurar as informações, no entanto não houve nenhuma técnica de cifragem eficiente entre os anos 1914 e 1918.

Durante esse tempo as cifras utilizadas eram apenas variações das utilizadas no século XIX que já haviam sido decifradas anteriormente, elas até ofereciam um nível de segurança, mas eram facilmente quebradas.

Com o surgimento do rádio o volume das mensagens interceptadas aumentou exponencialmente, o que trouxe um novo desafio para os criptoanalistas. Singh diz que durante a Primeira Guerra Mundial os franceses levaram a melhor nessa questão do volume de informações por terem construído uma equipe de criptoanalistas que funcionavam em uma escala industrial onde cada um se atinha a um tipo diferente de cifra se tornando especialistas, formando uma linha de montagem “o tempo era essencial, e a

linha de montagem dos criptoanalistas fornecia as informações de modo rápido e eficiente”.

Em 1918, o alemão Arthur Scherbius (engenheiro) desenvolveu uma máquina criptográfica, que mais tarde viria se tornar o sistema de cifragem mais eficiente da história, máquina Enigma (Fig. 4). Sua forma básica consistia em um teclado para a entrada de cada letra do texto original, uma unidade misturadora, que cifrava cada letra e um mostrador, que iluminava a letra cifrada, estrutura muito semelhante a uma máquina de escrever.

Figura 4 - Máquina alemã Enigma

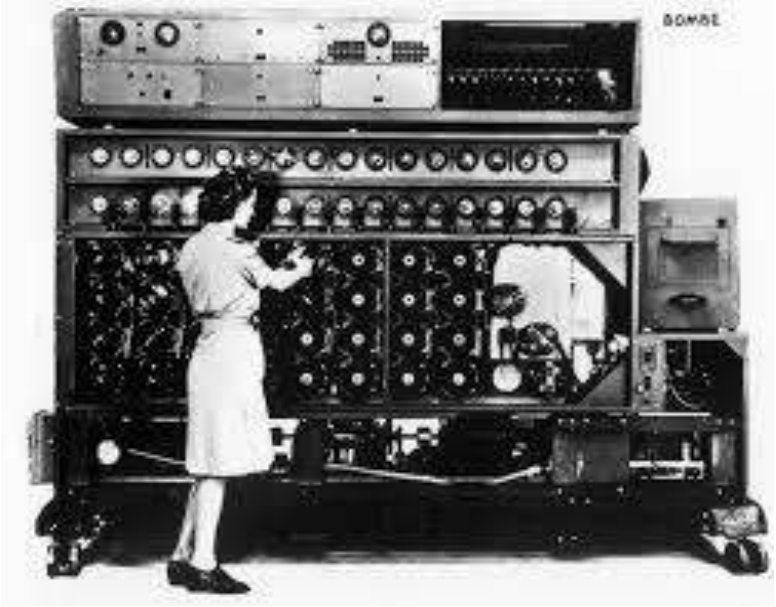
Fonte: https://www.gratispng.com/png-nr9rbc/

Essa história é contada no filme “O Jogo da Imitação” (2014) com direção de Morten Tyldum. A Enigma era utilizada pelos alemães em todas as comunicações durante a Segunda Guerra Mundial, o sucesso em decifrar essa máquina daria um fim na tão terrível guerra.

O governo britânico formou uma equipe com especialistas de diferentes áreas, trouxe matemáticos, linguistas, jogadores de xadrez, especialistas em palavras cruzadas entre outros para descobrir como quebrar o código Enigma num centro secreto em Bletchley Park na Inglaterra. No filme a equipe conclui de que existem mais de 159 milhões de configurações possíveis para

encontrar a configuração usada pelos alemães na máquina. Logo Alan Turing, matemático inglês, membro desta equipe desenvolveu uma máquina para competir com a Enigma por acreditar que uma equipe de homens ainda que brilhantes não poderiam medir forças com uma máquina e esse enorme número de possibilidades, era necessário um combate máquina contra máquina. Eles construíram a Bombe, uma máquina capaz de analisar a frequência das letras e suas configurações tão rápido quanto a Enigma, A Bombe mais conhecida no ramo da Ciência da Computação como a Máquina de Turing (Fig. 5) foi a precursora do que hoje chamamos de computador, por isso Alan Turing é considerado o pai da computação.

Figura 5 - Máquina de Turing



Fonte:https://sociedadematematica.wordpress.com/2015/08/30/matematicos-na-segunda-guerra-mundial/

Durante esse mesmo período da Segunda Guerra Mundial o autor se volta para os Estados Unidos da América que também enfrentavam uma máquina de criptografia, a Púrpura, desenvolvida pelos japoneses que também foi vencida. No entanto os militares estadunidenses perceberam que apesar das máquinas serem extremamente seguras, o processo de cifragem e decifragem era muito lento para ambientes mais intensos como campos de batalha por exemplo. Eles precisavam de um meio de comunicação secreto, seguro e mais rápido.

A solução veio do engenheiro estadunidense Philip Johnston, que filho

de missionário, viveu parte de sua vida junto dos índios da tribo Navajo se tornando conhecedor da língua e cultura daquela tribo. Basicamente a ideia era utilizar o idioma navajo como código de substituição para o idioma inglês, visto que o navajo era uma língua de conhecimento restrito apenas da tribo navajo que fica no estado do Arizona no Estados Unidos, então por mais que as informações sejam passadas em frequências de rádio abertas de nada adiantaria para os inimigos ouvirem as mensagens já que não possuem conhecimento da língua.

> O dialeto tribal navajo é completamente incompreensível para todas as outras tribos e todas as outras pessoas, exceto os 28 americanos que fizeram um estudo do dialeto. Essa linguagem equivale a um código secreto para o inimigo e plenamente adequada para comunicações rápidas e seguras. (SINGH, 2003, p. 216).

A ideia foi implementada como é possível assistir no filme Código de Guerra (2002) de John Woo, mas passou por desafios. Era necessário era que uma quantidade substancial de membros da tribo navajo fossem alfabetizados em inglês para transmitir, receber e traduzir as informações pelo rádio (Fig. 6), o que era um problema para os Estados Unidos na época e acabou ocasionando na demora da implementação do método para que cada membro da tribo se tornasse fluente em inglês além do treinamento militar que também foi necessário. Outro desafio foi que alguns termos técnicos utilizados por militares não existiam na língua navajo, então eles desenvolveram uma espécie de glossário com palavras equivalentes usando coisas da natureza que fazem parte do cotidiano navajo como podemos ver na imagem a seguir:

Figura 6: Cabo e soldado usando o código navajo floresta.

Fonte: (SINGH, 2003, p. 223)

Passados esses desafios o que ficou conhecido como “código navajo” foi implementado e obteve sucesso em sua aplicação pois manteve segura a informação, tornou as comunicações em campo de batalha muito mais rápidas através do rádio e permanece indecifrável durante toda a guerra.

A grande fragilidade no uso da criptografia estava no fato da chave ter de ser transmitida ao destinatário da mensagem. Fazer com que a chave para decifrar o código chegasse ao destinatário sem que fosse descoberta e apanhada era um grande desafio.

Dois grupos distintos de matemáticos se dedicaram a solucionar esse problema e chegaram à mesma conclusão: tudo estaria resolvido se a chave pudesse ser pública e transita-se livremente.

A ideia era que a mensagem pudesse ser cifrada por uma função matemática de “mão única”, isto é, de fácil aplicação, mas de difícil decifragem. Haveria duas chaves: uma pública, para que todos pudessem codificar e enviar a mensagem para uma determinada pessoa, e uma privada, conhecida apenas pela pessoa a quem a mensagem estivesse destinada, para sua decifragem.

O nome deste sistema é RSA, sigla que representa a junção do sobrenome de seus inventores: Ronald Rivest, Adi Shamir e Leonard Adleman, pesquisadores do Massachusetts Institute of Technology (MIT). A dificuldade de se quebrar o sistema RSA consistia na dificuldade em se fatorar grandes números – atualmente, com cerca de 150 algarismos. Trata-se de um sistema cuja utilização exige o uso de computadores.

Inicialmente era necessário a escolha de dois números primos quaisquer b e g. Quanto maior o número escolhido, mais seguro seria o algoritmo. O produto n = pq faz parte da chave pública de codificação. Os primos b e g, da chave privada. Logo, a segurança do sistema está na dificuldade em fatorar n, como explica Cunha (2012).

Computadores digitais processam apenas números. Por isso, cada mensagem a ser codificada é transformada num número, antes de cifrada.

4 CRIPTOGRAFIA COMO MÉTODO DE SEGURANÇA DA INFORMAÇÃO

Apesar do termo Segurança da Informação não ser estranho atualmente, seu conceito, história, métodos e desdobramentos não estão muito difundidos no cotidiano dos usuários da informação.

> Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, uma informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente. (LAURENO; MORAES, 2005, p. 40).

A missão de assegurar que a informação seja compreendida apenas pelo emissor e destinatário da mensagem evitando que seu conteúdo se torne público, é uma preocupação histórica e, ao mesmo tempo, cotidiana.

A tecnologia se tornou um notório facilitador da vida humana, com o passar do tempo nós nos tornamos muito dependente dela e das evoluções que ela trouxe, em especial a internet. Com o advento da internet, o plus da globalização e o aumento exponencial de seus usuários era natural que a produção de informações aumentasse no meio cibernético.

Neste trabalho não desprezamos esse contexto atual, mas acreditamos que para compreendermos melhor os fenômenos que nos perpassam hoje, precisamos compreender suas origens e desdobramentos. Estamos nos propondo a eliminar a dependência extrema em relação a sistemas, equipamentos, dispositivos e atividade vinculadas à segurança dos sistemas de informação e voltando nosso olhar para o passado a procura de referências que justifiquem o modo como vemos a segurança da informação e convivemos com seus métodos.

Segundo Corrêa (2015) a internet hoje é um meio em que a informação se encontra à mão de todos, de caráter democrático, uma vez que qualquer usuário é capaz de produzir ou adquirir conteúdo para o alcance de seus objetivos.

Seguindo esse raciocínio, pode-se pensar na internet como uma rede de compartilhamento, sem relação de subordinação, onde a informação seria distribuída e acessada de forma horizontal.

> A facilidade de uso e a grande quantidade de serviços e informações ofertadas, foram determinantes para a popularização da Internet, e, como subproduto desta massificação, vimos surgir uma variedade de problemas,

> dentre os quais, destacamos os relacionados à segurança dos dados que por ela trafegam. (SILVA, 2001, p. 19).

As formas de aplicação de segurança da informação estão geralmente ligadas às ameaças ou vulnerabilidade identificadas que se deseja prevenir ou remediar, independente do suporte em que a informação está contida, esteja em papel ou em ambiente digital.

De acordo com o dicionário Aurélio (2008) método pode ser definido como procedimento organizado que conduz a um certo resultado.

O termo método também é conhecido como o conjunto de procedimentos, regras e operações previamente fixados que permitem chegar à determinada meta, fim ou conhecimento. Ações que uma pessoa realiza de forma estruturada na realização de uma tarefa.

A Segurança da Informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade da informação. E para isso vem desenvolvendo métodos ao longo da história que garantam esses objetivos.

Entretanto apesar dos autores deixarem claro que a segurança da informação seja necessária e aplicável independente da forma em que a informação está contida, a literatura pertinente a segurança da informação permeia sempre ambientes digitais e ferramentas tecnológicas como podemos observar no trecho do Artigo 2 do Decreto 3.505/2000 pela maneira como define Segurança da informação:

> Segurança da Informação é proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Se os conceitos e até mesmo leis e regulamentos estão voltadas para a gestão da segurança da informação em sistemas de informação digitais é de se esperar que os métodos sugeridos para esse fim sejam sempre deste mesmo meio. O que é bem compreensível, afinal onde estão a maioria das informações a respeito das pessoas e de organizações senão em sistemas de informação em computadores? Logo, os métodos apontados são os que

atuam em ambientes digitais como por exemplo antivírus, firewalls e até mesmo a própria criptografia.

Alguns dos principais mecanismos de segurança usados para se proteger dos riscos associados ao uso da Internet são: o *firewall,* que atua como uma barreira de proteção que controla o tráfego de dados entre seu computador e a Internet, controlando o acesso ao sistema por meio de regras e a filtragem de dados; os antivírus que são programas de computador concebidos para prevenir, detectar e eliminar vírus de computador e a criptografia já definida anteriormente.

De acordo com a Cartilha de Segurança para Internet [9]os métodos de criptográficos atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizada pelos métodos de criptografia para criptografar e descriptografar mensagens. Esses métodos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas. Definidas por Bugs da seguinte forma:

> A criptografia de chave única utiliza a mesma chave tanto para criptografar quanto para descriptografar mensagens. Apesar de este método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas. Utilizada normalmente em redes de computadores por ser mais simples a administração.
> Criptografia de chaves pública e privada (assimétrica) utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Chave pública: Pública no que se refere ao grau de acesso, ou seja, todos conhecem ou tem acesso a esta chave. Até mesmo o invasor a conhece? Sim! Pois, ela é utilizada apenas para criptografar mensagens. Chave privada: Privada no que se refere ao grau de acesso, ou seja, apenas o seu dono a conhece e não a divulga. Ela é utilizada para descriptografar as mensagens geradas pela sua chave pública correspondente. As mensagens criptografadas com a chave pública só podem ser descriptografadas com a chave privada correspondente. (2010, p. 3).

[9] https://www.terra.com.br/informatica/especial/cartilha/privacidade_1.htm

De acordo com Assange (2015) no início dos anos 90 quando Philip Zimmermann criou o PGP[10], a criptografia era de comando exclusivo das agências de espionagem e os governantes a classificavam como uma arma muito perigosa para pessoas comuns usarem. Hoje, todos fazem uso da criptografia o tempo todo em atividades do dia a dia, mesmo sem perceber, em serviços como de internet banking e em aplicativos de mensagens como Whatsapp e Telegram.

Na tentativa de suprimir problemas de segurança, de acordo com Silva (2010) a solução bem mais aceita atualmente é a utilização de sistemas de criptografia por seu nível de seguridade.

A criptografia entretanto não é um método como os outros por algumas razões, uma delas é que a criptografia não limita seu uso ao suporte em que a informação está contida, como foi possível observar através da seção anterior 'história da criptografia' a criptografia evoluiu seu nível de complexidade, se adaptou aos mais variados meios de comunicação vigentes em cada período e possibilitou o desenvolvimento de tecnologias contemporâneas sendo um dos mais antigos métodos de segurança da informação, sendo até mesmo mais antigo que o termo de segurança da informação, talvez até seja por isso que apesar da relação óbvia dos dois a associação entre os dois termos não esteja tão presente nas literaturas.

Assange (2015) afirma que a tecnologia avançada de criptografia pode ajudar a tornar as comunicações dentro e fora da internet efetivamente anônimas e não rastreáveis, a crença do autor é tão firme, que o próprio site do qual ele é fundador (wikileaks) é inteiramente criptografado e garante o anonimato[11] das fontes que realizam o vazamento das informações.

Uma outra razão pela qual a criptografia não é um método qualquer de segurança da informação é que seu processo de realização envolve completa desconfiguração do conteúdo original da mensagem tornando-a ilegível em caso de qualquer interceptação da mensagem por qualquer um que não

[10] Pretty Good Privacy (pt: privacidade muito boa) - Software de criptografia.

[11] Até hoje não houve registro de nenhuma fonte (pessoa ou organização) que tenha vazado informações no wikileaks e tenha tido sua identidade revelada. Com exceção de Chelsea Manning, que foi descoberta por ter relatado seu vazamento a um hacker que trabalhava secretamente para o FBI e NSA.

entenda a cifra (chave) aplicada ou não tenham autorização para ver o conteúdo daquela mensagem.

Esses motivos demonstram a eficácia e eficiência da criptografia enquanto método de segurança da informação e porque de autores como Burnett e Paine (2002) afirmarem que a ferramenta mais importante de segurança é a criptografia.

A criptografia é o método de segurança que se destaca neste trabalho, pois ele se propôs a tratar de um estudo sob a perspectiva histórica da segurança da informação, e a criptografia é um dos primeiros métodos de segurança da informação de que se tem registro, assim como a esteganografia[12]. Esses dois métodos históricos proporcionaram a existência dos métodos atuais que se constituem basicamente evoluções desses métodos mais tradicionais.

As denúncias de espionagem no Brasil feitas por Snowden geraram uma série de medidas protetivas não só no governo brasileiro que tenta regular o uso da internet através das leis, mas também em parte da população que passou a se mobilizar para proteger seu direito à privacidade por entender a importância geopolítica da dominação do governo estadunidense sobre fontes e fluxos de informação na internet. Encontraram a criptografia como uma solução não só técnica, mas também uma expressão, ajudando a desenvolver e disseminar a cultura da segurança da informação através de eventos e ações.

A *Cryptoparty* é uma ação global que tem por objetivo compartilhar conhecimentos sobre como se proteger no espaço digital. Isso pode incluir comunicação criptografada, evitando rastreamento durante a navegação na web e conselhos gerais de segurança relacionados a computadores e smartphones.

Inspirada nessa ação, aqui no Brasil foi desenvolvida a Cryptorave [13]que é um evento anual que normalmente acontece em São Paulo, descentralizado para disseminar e democratizar o conhecimento e conceitos básicos da criptografia e software livre que reúne atividades sobre segurança,

[12] A esteganografia é uma técnica usada para ocultar a existência de uma mensagem dentro de outra, uma forma de segurança por obscurantismo.
[13] https://cryptorave.org/

criptografia, hacking, anonimato, privacidade e liberdade na rede. O evento teve sua primeira edição em 2014, como reação à divulgação de informações que confirmavam a ação dos EUA para manter a população mundial sob vigilância e monitoramento constante. Sua última edição foi em maio deste ano (2019) realizado na Biblioteca Mário de Andrade em São Paulo.

Corrêa (2015) ponta a criptografia como assunto de vital relevância para segurança e soberania dos Estados signatários. E cita como exemplo uma ferramenta para proteção em meio digital, o “PGP10 *pretty good privacy*, (pt: privacidade bastante razoável), descrito por Glenn Greenwald:

> Basicamente, o programa envolve cada mensagem em um escudo de proteção formado por um código composto por centenas, ou até milhares, de número aleatórios e letras com distinção entre caixa alta e baixa. As agências de inteligência mais avançadas do mundo grupo que sem dúvida inclui a NSA têm softwares de quebra de senhas com capacidade de um bilhão de tentativas por segundo, mas os códigos PGP são tão compridos e aleatórios que mesmo o mais sofisticado dos softwares precisa de muitos anos para quebrá-los. As pessoas que mais temem ter suas comunicações monitoradas, como agentes de inteligência, espiões, ativistas dos direitos humanos e hackers, confiam nesse padrão de criptografia para proteger suas mensagens. (2014, p.17).

Assim que Snowden entrou em contato com Glenn Greenwald, na época jornalista do *The Washington Post,* insistiu para que ele instalasse um programa de criptografia para que ele pudesse receber os documentos que ele lhe enviaria. Ele assim como Laura Poitras incentiva a todos os jornalistas a usarem a criptografia, por conta do receio de que uma provável vigilância estadunidense descobrisse seus planos. O que representa uma ameaça a privacidade e a democracia.

Vale ressaltar que Edward Snowden é um perito em segurança “cibernética”, como ele chama, tendo ele mesmo diversas vezes tendo a função de ensinar a agentes e da CIA e NSA como se proteger na rede. Esse mesmo homem declara o uso da criptografia como indispensável e seguro.

Snowden, em uma entrevista a Sonia Bridi (2014) diz que uma das coisas mais importantes que ele aprendeu com essa situação é que a criptografia é muito importante e muito difícil de se usar e afirma:

> “Ninguém terá comunicação segura no Brasil, Estados Unidos ou em qualquer lugar a menos que tenhamos acesso a essas ferramentas que são invisíveis. Não é preciso instalar nada, nem aprender nada, mas acontece por *default*, porque

> naturalmente não nos damos ao trabalho". (informação verbal[14]).

Ao The Guardian em 2014 Edward Snowden disse que "o primeiro contato sem usar canais de criptografia pode pôr tudo a perder".

> Inicialmente, compreender criptografia (especialmente para quem não detém conhecimento de técnicas computacionais) parece complicado. Todavia, utilizar seus benefícios não requer tais conhecimentos, pois, modernamente, a encriptação de dados está completamente integrada (facilmente utilizada) à grande maioria dos softwares existentes. (BORGES, 2016, n.p.)

Em unidades de informação a tecnologia está presente em equipamentos de informática, sistemas, aplicativos e softwares que ajudam no desenvolvimento e fluxo da informação. Uma unidade de informação como uma biblioteca não está isenta de possíveis invasões cibernéticas como as citadas anteriormente nesse trabalho. É de extrema importância assegurar as ações desenvolvidas em cada um dos processos de uma unidade, em especial os processos que envolvem conteúdos com restrição de acesso e dados pessoais dos usuários, com operações feitas em rede.

O uso da criptografia em sistemas utilizados em unidades de informação pode contribuir na gestão de riscos, permitindo maior controle de acessos as informações.

Para os profissionais da informação ter conhecimento a respeito das práticas de segurança da informação é fundamental. Através do desenvolvimento de uma política de segurança da informação em unidades de informação, pode-se estabelecer as medidas utilizadas para garantir acesso seguro e disponibilidade de informação aos seus usuários. Além de educar os usuários para que se tornem mais conscientes a respeito do uso das informações e segurança de seus dados.

---

[14] Entrevista fornecida por Edward Snowden à jornalista Sonia Bridi da Globonews em junho de 2014.
Disponível em: https://www.youtube.com/watch?v=k3Sxp3yIeGQ

CONSIDERAÇÕES FINAIS

Para muitos a Segurança da Informação se resume a sistemas de segurança, com firewalls, sistemas de detecção de intrusos e antivírus. Outros acham que incluir a adoção de políticas de segurança e o estabelecimento de responsabilidades funcionais ao aparato tecnológico é suficiente. Mas nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconsequente Sêmola (2016). Não é errado pensar dessa maneira, afinal no nosso contexto atual existem aparatos tecnológicos para as funções mais simples, por exemplo, existem mais de 9 aplicativos com a mesma finalidade, nos lembrar de beber água. Pensar pelo viés tecnológico já que estamos cada vez mais integrados a ambientes digitais é inevitável, tendo em vista nossa dependência da tecnologia.

Com tudo que abordamos até aqui podemos afirmar que o progresso é precedido de uma necessidade, os métodos de segurança da informação só foram desenvolvidos em função da necessidade de proteger informações valiosas. Atualmente a informação tem o mesmo preciosismo de outrora, entretanto, a diferença é que antes a concentração da informação e o poder de tomar a decisão que possivelmente influenciaram na vida das pessoas estava concentrado nos reis, rainhas e comandantes de exércitos, e agora não, com a internet todos somos produtores de informação, gerimos nosso conteúdo nas redes de comunicação. Com os exemplos que citamos na pesquisa não podemos dizer que a mais simples de nossas informações não tem valor, pois nossas informações de Facebook e Twitter foram o suficiente para manipular uma eleição.

O êxito da privacidade sociedade da informação depende em grande parte de protegermos as informações dentro desse fluxo mundial frenético. Durante milhares de anos a criptografia só foi importante no âmbito militar, e hoje pessoas comuns dependem dela para garantir a privacidade de suas informações. Graças aos avanços narrados neste trabalho, hoje a criptografia é facilmente aplicável por mecanismos tecnológicos, um aplicativo, uma senha, um software e estamos protegidos. Não é mais necessário que

sejamos matemáticos para tanto. A medida que nos aprofundamos mais nesse nem tão novo século, os defensores de direitos civis na internet como o Wikileaks e Edward Snowden começam a pressionar pelo uso generalizado da criptografia para proteger a privacidade dos indivíduos, ou ao menos torná-los cientes do que se passa, tornando-os capazes de escolher o que muitas vezes lhe é imposto. Escolher entre a privacidade e a segurança.

É importante ressaltar que devido aos variados tipos de ameaças a que estamos expostos no ambiente digital é recomendável o uso da criptografia aliada a outros métodos e medidas de segurança. O uso exclusivo de um único método pode ser perigoso no contexto atual.

As características da criptografia como: desconfiguração completa de conteúdo; garantia de decifragem apenas ao receptor da mensagem e utilização abrangente faz com que esse método se sobreponha aos outros, mas não exclui a utilização de outros métodos, pelo contrário, quando aliados garantem um nível maior de segurança.

REFERÊNCIAS

ALMEIDA, Paulo. Criptografia e segurança. São Paulo: Publindustria, 2012.

ASSANGE, Julian. **Quando o Google encontrou o Wikileaks**. Boitempo Editorial, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO IEC 17799**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: tecnologia da Informação: técnicas de Segurança Sistemas de gestão de segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Rio de Janeiro, 2013.

BARBOSA, Ricardo Rodrigues. Gestão da informação e do conhecimento: origens, polêmicas e perspectivas. **Informação & Informação**, v. 13, n. 1, p. 1-25, 2008.

BRAGA, Ascenção. A gestão da informação. **Millenium**, 2000.

BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso; NICOLÁS, Maria Alejandra. A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos. **Revista Eptic**, v. 17, n. 1, p. 237-255, 2015.

BRASIL. DECRETO Nº 9.668, DE 2 DE JANEIRO DE 2019. Brasília,DF, jan 2019. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9668.htm>. Acesso em: 20 jun. 2019.

BRASIL.DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018., Brasília,DF, dez 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 20 jun. 2019.

BRASIL.LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco civil da internet**, Brasília,DF, abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 jun. 2019.

BRASIL.LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de proteção de dados pessoais**, Brasília,DF, ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 jun. 2019.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p.

BRIDI, Sonia. Milênio: Sônia Bridi entrevista Edward Snowden.**Youtube**, 17 mar. 2017. Disponível em: <https://www.youtube.com/watch?v=k3Sxp3yIeGQ>. Acesso em: 20 jun. 2019.

BORGES, Fabiani. **Criptografia**: o uso maléfico de uma tecnologia criada para a proteção da privacidade dos usuários. Escola Paulista de Direito, São Paulo. 2016.

BUGS, Wagner. **Segurança da informação:** pilares e conceitos de proteção e segurança. [S.l.: s.n.], 2010. Disponível em: <https://docplayer.com.br/4599988-Seguranca-da-informacao-pilares-e-conceitos-de-protecao-e-seguranca-prof-wagner-bugs.html>. Acesso em: 29 nov. 2018.

BURNETT, Steven; PAINE, Stephen. **Criptografia e segurança:** o guia oficial RSA. Gulf Professional Publishing, 2002.

CÓDIGOS de guerra. Direção de John Woo. California:Metro Goldwyn Mayer, 2002. (134 min.)

CORRÊA, Filipe Mariano de Paula. A falta de segurança na internet: realidade, dinâmica e alerta. 2015.

COUTINHO, Severino Colier. **Números inteiros e criptografia RSA**. IMPA, 1997.

DA SILVA, Denise Ranghetti Pilar; STEIN, Lilian Milnitsky. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, v. 10, 2011.

DE SOUZA ABREU, Jacqueline. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 24-42, 2018.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de segurança da informação. **Ciência Moderna**, 2008.

FIARRESGA, Victor Manuel Calhabrês et al. **Criptografia e matemática**. 2010. Tese de Doutorado.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação**. Brasport, 2008.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Editora Saraiva, 2017.

FONSECA FILHO, C. **História da computação**: o caminho do pensamento e da Tecnologia. EDIPUCRS, 2007.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

GREENWALD, Glenn. **Sem Lugar Para Se Esconder**. Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GREENWALD, Glenn; MACASHILL, Ewen. Programa NSA prism aproveita os dados de usuários da apple, google e outros. **The Guardian**, 7 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 20 jun. 2019.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber Franke; DE ASSIS Olgin, Clarissa. Códigos e senhas no Ensino Básico. **Educação Matemática em Revista–RS**, v. 2, n. 10, 2012.

GUEDES, Maria Helena. Os mecanismos. Joinville: Clube de autores, 2015.

LAUREANO, Marcos Aurélio Pchek; MORAES, Paulo Eduardo Sobreira. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, v. 8, n. 3, p. 38-44, 2005.

MARCACINI, Augusto. **Direito e informática**: uma abordagem jurídica sobre a criptografia. São Paulo, 2010.

MARCIANO, João. Luiz. Pereira.; LIMA-MARQUES, Mamede. **Segurança da informação**: uma abordagem social. 2006. Tese (Doutorado) - Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília.

MARCHIORI, Patrícia Zeni. A ciência e a gestão da informação: compatibilidades no espaço profissional. **Ciência da informação**, v. 31, n. 2, 2002.

MARS, Amanda. Como a desinformação influenciou nas eleições presidenciais? **El País**, 25 fev. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/02/24/internacional/1519484655_450950.html>. Acesso em: 20 jun. 2019.

NAKASHIMA, Ellen. Coleção de registros de telefonia da NSA faz pouco para prevenir ataques terroristas, diz grupo. **The Washington Post**, 12 jan. 2014. Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html?noredirect=on&utm_term=.096d97f676cc>. Acesso em: 20 jun. 2019.

_____.; SOLTANI, Ashkan. Painel pede novas restrições à vigilância dos EUA. **The Washington Post**, 18 dez. 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-shouldnt-keep-phone-database-review-board-recommends/2013/12/18/f44fe7c0-67fd-11e3-a0b9-249bbb34602c_story.html?utm_term=.5efe963ec245>. Acesso em: 20 jun. 2019.

O JOGO da imitação. Direção de Morten Tyldum. Nova Iorque:The Weinstein Company, 2015. (114 min.)

OLIVEIRA, Carlos Eduardo Elias de. Aspectos principais da lei n. 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica. 2014.

PALACIOS, Eduardo Marino García. et. al. **Introdução aos estudos CTS (Ciência, Tecnologia e Sociedade)**. Organización de Estados Iberoamericanos (OEI), 2005.

PEREIRA, Eduardo Martins et al. Segurança da informação. 2003

PETERSON, Andrea. Os "especialistas externos" de Obama para a revisão da NSA são ex-funcionários da Intel e da Casa Branca. **The Washington Post**, 22 ago. 2013. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2013/08/22/obamas-outside-experts-for-nsa-review-are-former-intel-and-white-house-staffers/?utm_term=.63c96ffe874b>. Acesso em: 20 jun. 2019.

PIMENTA, Alexandre Manuel Santareno; QUARESMA, Rui Felipe Cerqueira. **A segurança da informação e o comportamento dos usuários**. JISTEM J.Inf.Syst. Technol. Manag. vol.13 no.3 São Paulo Sept./Dec. 2016.

REZENDE, Pedro Antonio Dourado. Criptografia e Segurança na Informática. **Apostila-Capítulos**, v. 1, n. 2, p. 3, 1998.

RIVEST, Ronald Linn. **Cryptography**: Algorithms and Complexity. [S.l.: s.n.], 1990.

RUSBRIDGER, Alan et.al. Edward Snowden: 'If I end up in chains in Guantánamo I can live with that' - video interview. **The Washington Post**, 14 ju. 2014. Disponível em: <https://www.theguardian.com/world/video/2014/jul/17/edward-snowden-video-interview>. Acesso em: 20 jun. 2019.

SANTOS, José Luiz dos. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de matemática básica**. 2013. Dissertação (Mestrado). Instituto de Matemática, Universidade Federal da Bahia, Salvador.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Elsevier, 2014.

SILVA, Alexandre Alcântara da. **O uso da internet pela secretaria da fazenda do estado da Bahia**: aspectos legais e de segurança. Tese (Doutorado). Universidade Federal da Bahia, Salvador. 2001.

SINGH, Simon. **O Livro dos Códigos**: a ciências do sigilo - do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2003.

TERADA, Routo. Criptografia e a importância das suas aplicações. **Revista do Professor de Matemática (RPM)**, n. 12, p. 1-6, 1988.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86, p. 269-285, 2016.

VALDEVINO, André. Criptografia Caótica. **Brasília: Universidade Católica de Brasília**, 2010

VERASZTO, Estéfano Vizconde et al. Tecnologia: buscando uma definição para o conceito. **Prisma.com**, n. 8, p. 19-46, 2009.

WEBER, Raul Fernando. Criptografia contemporânea. In: **VI Simpósio de Computadores Tolerantes a Falhas**. 1995. p. 7-32.

.