CRIPTOGRAFIA E SEGURANÇA

CLEBERTON JUNIO VIANA[1]
GUILHERME MARQUES DATTEIN[2]
JOÃO VICTOR BUENO DE GODOY DA SILVA[3]
PATRICIA KLINKERFUS DE CAMPOS[4]

RESUMO

O COVID-19 trouxe consigo inúmeros impactos sociais, gerando mudanças de comportamento em toda a sociedade, afetando o setor econômico, porém oferecendo, em contrapartida, a oportunidades de negócios com a utilização de tecnologias de informação e comunicação. Como a quantidade de informações trafegando nas redes aumentou consideravelmente, houve uma busca e empenho de várias empresas do setor de segurança da informação oferecendo inúmeras soluções para assegurar que os dados estivessem criptografados. Para tanto, este trabalho tem como foco analisar o fator segurança da informação, destacando os diferentes tipos de criptografias utilizados no mercado, uma vez que trata-se de garantir a confidencialidade, integridade e autenticidade dos dados dos usuários. É de suma importância que o profissional de tecnologia da informação conheça como se dá o funcionamento dos algoritmos criptográficos, destacando suas importâncias, reconhecendo-a como ferramenta essencial para o aumentando da segurança e confidencialidade de dados. Trata-se de uma pesquisa bibliográfica, com uma abordagem qualitativa, com fundamentação na leitura de livros, artigos digitais e sites de diferentes autores, apresentando, de forma clara, os dados através de quadros, gráficos e figuras que permitem legitimar as informações, de forma clara e concisa.

PALAVRAS-CHAVE: Segurança; Criptografia; Confidencialidade; Integridade; Autenticação.

[1] Graduando do 6° semestre do curso de Tecnologia em Gestão da Tecnologia da Informação da Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira”.
[2] Graduando do 6° semestre do curso de Tecnologia em Gestão da Tecnologia da Informação da Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira”.
[3] Graduando do 6° semestre do curso de Tecnologia em Gestão da Tecnologia da Informação da Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira”.
[4] Professora Mestre em Educação, dos todos os cursos de Graduação Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira” e dos cursos de Graduação de Administração e Ciências Contábeis da Faex - Faculdade de Ciências Aplicadas de Extrema. E-mail: patricia.klinkerfus@fatec.sp.gov.br

ENCRYPTION AND SECURITY

ABSTRACT

COVID-19 brought with it numerous social impacts, generating behavioral changes throughout society, affecting the economic sector, but offering, on the other hand, business opportunities with the use of information and communication technologies. As the amount of information traveling on the networks has increased considerably, there has been a search and effort by several companies in the information security sector offering numerous solutions to ensure that data is encrypted. Therefore, this work focuses on analyzing the information security factor, highlighting the different types of encryption used in the market, since it is about ensuring the confidentiality, integrity and authenticity of user data. It is extremely important that the information technology professional knows how cryptographic algorithms work, highlighting their importance, recognizing it as an essential tool for increasing data security and confidentiality. This is a bibliographic research, with a qualitative approach, based on the reading of books, digital articles and websites by different authors, clearly presenting the data through tables, graphs and figures that allow to legitimize the information, in a clear way. clear and concise manner.

KEYWORDS: *Security; Cryptography; Confidentiality; Integrity; Authentication.*

1. INTRODUÇÃO

Atualmente tem-se observado o crescimento considerável de tecnologias de informação e comunicação, sejam elas voltadas a hardwares ou softwares, em uma escalada inovadora e competitiva. Nota-se a grande tendencia da sociedade em estar, cada vez mais, conectadas ao mundo digital para a realização de inúmeras atividades, desde as profissionais até os pessoais, tais como: aplicativos de relacionamentos, entretenimento, compras online, acesso as instituições financeiras, entre tantas outras. Estamos, constantemente, compartilhando e inserindo informações, inclusive, dados pessoais, em dezenas de sites e instituições de diferentes nichos, que transitam na rede.

Com isso, quando fala-se de tráfego de dados na rede, que cresce constantemente, não se pode deixar de lado, o fato de que tem-se que garantir a segurança desses dados ou a segurança da informação, que se torna um desafio, já que atualmente, com tantas tecnologias disponíveis, ainda não existe nenhum sistema 100% seguros e uma técnica, método ou norma que seja 100% eficaz em proteger as organizações de ataques ou *Ciberataques,* na tentativa de roubar informações, como por exemplo, os dados que estão armazenados em diversos servidores espalhados pelo mundo.

Pode-se dizer que a segurança da informação nasceu a “600 anos a.C.”, com a criptografia hebraica. Nos remetendo para os dias atuais, vale lembrar de um marco importante na história, um ícone da segurança da informação, conhecido como a máquina “Enigma”, criada pelo engenheiro alemão Artur Scherbius em 1918. Essa máquina tinha o intuito de criptografar e descriptografar mensagens ou códigos de guerra, tendo como ideia central, impedir os inimigos de guerra, de ler informações que soldados alemães possuíssem, ou ainda, caso o sinal de comunicação fosse interceptado. Enfim, anos depois durante a segunda guerra, a Enigma foi decifrada pelo matemático inglês Alan Turing. Conclui-se, portanto, os alemães criaram a primeira máquina a utilizar cifra de chave única e os ingleses os primeiros a criarem um computador programável para fazer criptoanálise, chamado Colossos. A partir da década de 70 a “era da informação”, onde o ativo mais importante é o conhecimento,

mesmo que sem receber muito reconhecimento e atenção, deu primeiro passo na busca pelo fortalecimento e ênfase na segurança da informação, criando microprocessadores, algoritmos e sistemas integrados, em computadores pessoais, tais quais utilizamos hoje.

Pensando nos países mais populosos do mundo, como o Brasil, que possui o número de dispositivos conectados à internet maior que a própria população, já é de se esperar que estes tenham um maior índice de ataques virtuais. De acordo com o relatório de Ameaças Cibernéticas da SonicWall (2021), o Brasil está em 5° lugar, no ranking dos países que mais sofrem ataques de *ransomware*[5] em 2021, com 9,1 milhão de registros, ficando para trás dos Estados Unidos (227,2 milhões), Reino Unido (14,6 milhões), Alemanha (11 milhões) e África do Sul (10,5 milhões) respectivamente. Apesar de sofrer variações, o índice de ataques no Brasil cresceu bastante, em 2017, pulou do 7° lugar no ranking, de maiores números de incidentes, para 3° em 2019 com 875.327 incidentes, mas caiu para 665.079 em 2020 segundo CERT.br (2021). Apesar de estar em uma posição alta no ranking, o Brasil não sofre com ataques tão perigosos em relação aos outros países, mas não deixa de ser um ponto de atenção.

O padrão de criptografia avançado AES[6] 256 bits “especifica um algoritmo criptográfico aprovado pelo FIPS (Federal Information Processing Standards ou Padrões Federais de Processamento de Informações) usados para proteger dados eletrônicos, é uma cifra de bloco simétrico”, de acordo com (CRIPTOID, 2021). Esse padrão foi adotado pelos EUA em 2002, se tornando o mais utilizado no mundo anos depois. Enquanto a China, estuda utilizar criptografia quântica, no combate aos hackers, sendo este, um novo método a ser usado no combate a ataques, e promover melhor segurança.

A criptografia é uma técnica muito **importante** já que desempenha um papel com dois propósitos principais, sendo o primeiro de impedir a visualização dos dados sem algum tipo de autorização, e o segundo, permitir a transmissão de dados de forma

[5] É um tipo de malware que restringe o acesso a arquivos importantes ou um sistema infectado e exige um resgate para retomar o acesso.
[6] Advanced encryption standard ou padrão de criptografia avançado.

segura por locais ditos inseguros, para que os dados da origem cheguem ao seu destino sem qualquer alteração, ou seja a criptografia tem como objetivo principal garantir a confidencialidade, integridade e privacidade dos dados e está presente em dois dos pilares da segurança da informação.

Sendo assim, a escolha desse tema, pensando na importância de criptografias nesse meio de segurança da informação, se deu para expandir o conhecimento e entender de forma mais aprofundada sua importância.

Para tanto, o **objetivo** deste trabalho é abordar, estudar e apresentar conceitos básicos e as principais características de segurança da informação, atreladas a criptografias, além de mostrar os conceitos básicos e os principais algoritmos de cifragem., a fim de reforçar a importância da criptografia na segurança da informação.

Considerando o objetivo principal, a **metodologia** para o desenvolvimento deste trabalho buscou-se fundamentar a princípio nas obras relacionadas ao tema de autores peritos, para o estudo, com uma abordagem qualitativa de natureza básica, baseando-se em pesquisas bibliográficas como, leitura de livros e artigos, e utilização de quadros e tabelas para melhorar o entendimento, com objetivo de explorar o tema escolhido, visando apresentar os conceitos importantes, dando embasamento ao trabalho, e leitura de artigos digitais e sites para apresentação e aplicação do conteúdo como, os principais tipos de criptografias existentes e as mais utilizadas, com auxílio da ferramenta de busca *Google Acadêmico,* como principal fonte de informações.

Este trabalho está organizado da seguinte forma, inicialmente apresentamos o referencial teórico, sendo apontado os conceitos básicos de segurança da informação e criptografias afim dar entendimento a sua importância, bem como seu papel crucial na segurança dos dados, além de sua utilidade, em seguida apresentaremos a análise dos dados, demonstrando o uso das criptografias, como são aplicadas, as mais usadas no mercado e aquelas que garantem maior confiabilidade no mercado, e por fim, nossas considerações finais.

2. REFERENCIAL TEÓRICO

Neste capítulo serão apresentados conceitos importantes de segurança da informação e criptografias para fundamentação do conteúdo.

Segurança da Informação

Deve-se ter em mente, inicialmente, que informação é um recurso muito valioso, pois a partir dela que se pode descobrir novas formas de entender o mundo, bem como as causas e consequências de fatores naturais e artificiais, que interferem direta e indiretamente na vida de toda a humanidade. Com a informação usada de forma inteligente, evoluímos e avançamos como profissionais e pessoas, e para as empresas, a informação pode ser um dos bens mais valiosos, tanto para descobertas, análises, tomada de decisões estratégicas, dentre outras, e por este motivo, que a segurança desses dados tem que estar entre os primórdios atos a serem tomados por cada uma delas. Portanto, segurança da informação se refere a defesa de dados, assegurar que informações sigilosas sejam acessadas somente pelos responsáveis de direito, mantendo seu valor, seja para um indivíduo ou organização.

Fontes (2006, pg. 14) afirma que “sua definição simples e objetiva é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando eu o negócio da organização seja realizado e a sua missão seja alcançada.”

Enfim, segurança da informação é um conjunto de técnicas, estratégias, normas adotadas a fim de proteger qualquer dado ou informação, evitando que indivíduos mal-intencionados roubem ou divulguem estes indevidamente.

Depois de entender o que é segurança da informação vamos entender a diferença entre dados e informações. Um dado nada mais é que um elemento de informação quantificável não tendo necessariamente um significado importante como: números, letras, imagens etc. Informação é o agrupamento e organização dos dados para transmitir um significado e compreensão de determinado assunto.

Para Machado (2014, pg.10) Dado “é uma representação, um registro de uma informação” que pode ser quantificado.

Ainda segundo Machado (2014, pg.10) “informação acrescenta algo ao conhecimento de uma realidade analisada”, como exemplo a dosagem de um determinado remédio que um paciente precisa receber é uma informação.

2.1 Pilares da Segurança da Informação

Tendo em mente já o conceito de segurança da informação, devemos ter conhecimento de seus pilares ou, princípios fundamentais em todo e em qualquer programa de segurança da informação também conhecida como a *tríade CIA*, sendo: confidencialidade, integridade e disponibilidade. Fontes (2006) apontou como sendo os objetivos principais, e incluiu: legalidade, auditabilidade e não repúdio de autoria.

Confidencialidade diz respeito ao sigilo ou em garantir o acesso a informações somente a pessoas com autorização.

> Confidencialidade é a capacidade de garantir que o nível necessário de sigilo seja aplicado em cada junção de dados em processamento. [...] A confidencialidade pode ser fornecida por meio de técnicas de criptografia de dados e da forma como eles são armazenados e transmitidos, assim como de acesso rigoroso, classificação de dados e treinamento de pessoal sobre os procedimentos adequados na utilização de informações na empresa.” (MACHADO, 2014, pg.7)

A criptografia será abordada mais para frente, mas ela transforma dados em códigos o que dificulta a leitura por pessoas não autorizadas, garantindo a confidencialidade e o sigilo, e somente pessoas autorizadas possuem uma chave para acessar esses dados codificados.

Integridade deve garantir que o conteúdo de uma mensagem ou que as informações não sejam alteradas sem autorização. “A integridade é a garantia de rigor e confidencialidade das informações e sistemas e de que não ocorrerão modificações não autorizadas de dados” (MACHADO, 2014, pg.8). Criptografar os dados significa que dificultara a leitura dessa determinada informação seja lida sem autorização, automaticamente dificulta também sua alteração indevida mantendo assim a integridade.

Agora, como último pilar, porém, não menos importante, temos a disponibilidade, que se pode afirmar que está relacionada a uma boa infraestrutura confiável para garantir que o desempenho de operações ou das atividades principais de uma empresa estejam sempre funcionando e ativo, sem problemas, ou seja, “é a capacidade que os sistemas e as redes devem ter para executar e disponibilizar os dados de forma previsível e adequada às necessidades da empresa” (MACHADO, 2014, pg.8). Afetar a disponibilidade está relacionada a equipamentos ou softwares com problemas ou com falhas. Vale ressaltar, a criptografia não desempenha um papel diretamente ligado a disponibilidade, porém, como sendo um dos princípios da segurança é importante ter isso em mente.

Quanto a legalidade em segurança da informação pode-se afirmar que está relacionada com as políticas de segurança, pois a informação tem que estar de acordo com as leis, de forma regulamentada, em contratos estabelecidos. Já auditabilidade e não repúdio de autoria estão ligadas a confidencialidade, pois diz respeito ao registro de acessos e garantia de autenticidade respectivamente. Fontes (2006, pg. 15) diz que na auditabilidade, “o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito.”, e no princípio do não repúdio “o usuário que gerou ou alterou a informação, não pode negar o fato, pois existem mecanismos que garantem sua autoria”, ou seja, garante a identidade de quem está enviando a mensagem, o usuário que criou ou alterou algum documento de texto ou mensagem, por exemplo, não pode negar ter feito aquilo pois existem meios para comprovar seu acesso e o que foi feito.

2.2 Criptografia

Todos nós temos informações que queremos manter em segredo, seja por motivos de privacidade nas redes sociais, ou para autoproteção, pois sempre tem ladrões ou pessoas mal-intencionadas que poderiam usar algumas informações para nos roubar ou fazer algum mal, porém, ainda estaríamos tratando com uma quantia pequena de informação se compararmos a quantidade de informações utilizadas pelas Empresas. Mostrar as questões relacionadas à segurança das empresas, que

possuem segredos, como dados financeiros, estratégias, resultados de pesquisas, dentre outros, envolve uma gama muito maior de informações, que precisam ser protegidas, seja de hackers, concorrentes ou até mesmo pessoas da própria empresa insatisfeitas com seu trabalho.

Atualmente existem diversas técnicas e métodos de proteção de informações que devem operar em conjunto para cumprir e manter a *CIA,* como mencionado anteriormente, existe também a segurança fornecida diretamente pelos sistemas operacionais de computadores, porém, essas ferramentas não se mostram suficientes, sendo necessário adotar uma medida de proteção mais eficaz, que é a criptografia, para Fontes (2006, p.8) “uma das ferramentas mais importantes para proteção dos dados é a criptografia, qualquer um dos vários métodos que utilizamos para transformar arquivos legíveis em algo ilegível.”

2.3 O que define a criptografia

A criptografia é imperceptível, está presente no dia a dia de qualquer usuário, seja em sites, aplicativos até mesmo em sistemas mais complexos. É principalmente usada para manter o sigilo das informações que trafegam na rede, sendo também essa sua importância, exatamente preservar o direito à privacidade e proteção de dados. De acordo com Ramiro e Canto (2020, pg.7) o uso de criptografias está cada vez mais importante com o aumento de serviços sociais na rede, como “aplicativos de mensagem: garante o sigilo e integridade das mensagens”, em serviços de saúde e bancários: “protegendo dados sensíveis de pacientes” e “informações em ferramentas de internet banking”, lojas online e até mesmo “centrais de energia: garantindo a estabilidade e segurança de redes elétricas”. Devido ao aprimoramento das criptografias, tarefas que hoje já estão familiares, como transações financeiras pelo celular, relações profissionais e pessoais na palma da mão, se tornam possíveis e cada vez mais seguras.

Atualmente existem diversas criptografias em utilização no mercado, sendo todas elas divididas em duas modalidades que serão melhor apresentadas mais a frente, sendo criptografia simétrica ou de chave privada e, criptografia assimétrica ou

de chave pública. A primeira, mais simples, com a utilização de uma chave única, porém, considerada vulnerável, pois, em alguns casos, sua utilização se torna inviável, devido ao risco de interceptação da chave simétrica, passando para o desenvolvimento (evolução) da segunda, a chave assimétrica, que usa duas chaves diferentes: uma chave pública e uma privada, a fim de aumentar e garantir maior nível de segurança nas transações via web.

Na criptografia de chave simétrica segundo Burnett e Paine (2002, pg 11) “um algoritmo utiliza uma chave para converter as informações naquilo que se parece com bits aleatórios.” (criptografa a informação), “assim, o mesmo algoritmo utiliza a mesma chave para recuperar os dados originais”.

Segundo o artigo publicado no site *infowester* em 2005*,* sobre criptografia*,* escrito por Emerson Alecrim a chave assimétrica “trabalha com duas chaves: uma denominada privada e outra denominada pública. Neste método, um emissor deve criar uma chave de codificação e enviá-la ao receptor. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta.”

2.4 Empresas e Criptografias

Falando de criptografias no meio empresarial, é interessante ressaltar a criptografia de ponta a ponta utilizada pelo WhatsApp, Apple, Google entre outras, que além de ter ganho bastante notoriedade, também foi motivo de polémica, como apresentado abaixo, que o governo pretendia derrubar essa criptografia.

De acordo com o WhatsApp, devido a vários exemplos de ataques maliciosos de hackers para obter ilegalmente dados privados e abusarem da tecnologia para ferir pessoas, foi implementada a criptografia de ponta a ponta, em 2016. O objetivo foi fornecer chaves criptográficas que ficam em poder do usuário, que somente o remetente e o destinatário saibam o que estariam falando, sem que ninguém mais pudesse ter acesso a essa informação, nem mesmo o próprio WhatsApp.

A dois anos atrás essa criptografia foi motivo de polêmica, segundo um artigo publicado por Ronaldo Gogoni (2019) no site *meiobit,* o “departamento dos EUA discutiam tornar essa criptografia ilegal”, e no Brasil o “STF poderia quebrar o sigilo

do WhatsApp", justamente por não possibilitar que as informações pudessem ser acessadas por pessoas ou empresas externas, que resultaria em dificultar investigações criminais.

No mesmo ano o Conselho Nacional endureceu as regras para a criptografia no país, com uma proposta de que "as empresas devem ser obrigadas por lei a fornecerem os dados solicitados à quebra do sigilo" segundo Ronaldo Gogoni (2019) no site *meiobit*, caso contrário isso resultaria no banimento dessa criptografia, ou dos próprios aplicativos e produtos que a utilizassem. Contudo, o WhatsApp atualmente, continua com essa criptografia, porém agindo em conformidade com as leis vigentes, além da melhora significativa na segurança do aplicativo.

Por fim a criptografia de ponta a ponta é do tipo assimétrico, esse método protege texto, áudios, vídeos, fotos, documentos e ligações, porém existe um ponto de atenção quando falamos do backup em nuvem, essa criptografia protege as informações em casos de interceptações durante a troca de mensagens, mas quando são armazenadas na nuvem, perdem a criptografia e ficam vulneráveis, isso se tratando de dispositivos Android, que no caso do WhatsApp usa a ferramenta gratuita Google Drive para os backups onde a criptografia de ponta a ponta não se aplica, mas isso funciona de forma diferente para usuários Apple, pois ela possui seu próprio sistema de armazenamento em nuvem o iCloud, no caso disponíveis para iPhones, que por sua vez, quando um usuário faz o backup pelo Whatzapp para o iCloud, os arquivos são enviados criptografados, isso funciona como uma camada extra segurança. Embora seja possível usar o Whatzapp sem o backup em nuvem, é conveniente a possibilidade de recuperar suas mensagens caso perca o celular, a menos que tenha um iPhone que garante mais tranquilidade.

Vale ressaltar que essa criptografia foi adotada por vários aplicativos de mensagens como o Telegram, Signal, Google Mensagens, entre outros, mas vale ressaltar que apesar de mais atrasada em relação aos outros aplicativos, o "Zoom Cloud Meetings", aplicativo de reuniões online, decidiu aderir essa criptografia, para ter uma camada extra de privacidade.

2.5 Impacto na sociedade

Nesse meio digital onde cada vez mais sites, aplicativos, dispositivos e infraestruturas maiores, como sistemas de controle aéreo, estão crescendo, se tornando cada vez mais essenciais, a base para que esses sistemas continuem e evoluam economicamente, é a confiabilidade e estabilidade, que para melhorar necessitam de níveis mais robustos de segurança.

Pensando nesse ambiente digital, novas dinâmicas e hábitos econômicos surgem, oferecendo aumentos nos níveis de geração de renda e inovação tecnológica, porém é crucial pensar em impedir vulnerabilidades de segurança para que continue crescendo de forma mais segura e confiável.

Tendo como exemplo a pesquisa Febraban de tecnologia bancária, publicada no site *Deloitte* (2021) “transações bancárias pelo celular ultrapassam 50% das operações feitas pelos brasileiros” e “gastos dos bancos com tecnologia cresceu 8% (aproximadamente R$25,7 bilhões) em 2020; e 10% disso é voltado para cibersegurança”, o que gera um crescimento da necessidade de segurança da informação, consequentemente aumenta a geração de empregos, em uma busca de profissionais qualificados que trabalhem nessa área.

Segundo o site *sopesp notícias,* com informações retiradas do jornal de economia “*Valor Econômico*” publicado em maio de 2020, o Itaú Unibanco, está com cerca de 450 vagas abertas em tecnologia, já com contratações de quase 500 pessoas feitas anteriormente, a diretora de recursos humanos do banco Itaú, Valéria Marretto (2020) diz, “dentro do nosso plano de expansão de tecnologia, a gente prevê aumentar em 150 o número de vagas para profissionais na área de segurança.”, sendo que o Itaú Unibanco é o maior banco privado do Brasil, e uma das maiores instituições financeiras do mundo.

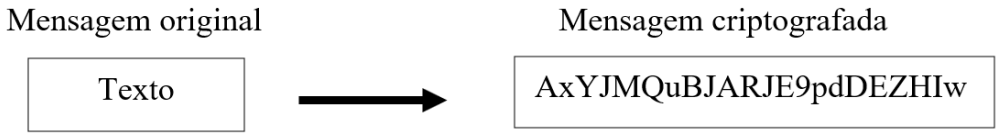
3. LEVANTAMENTO DE DADOS

Neste capítulo será apresentado os principais tipos de criptografia, como as criptografias do tipo simétrica e assimétrica, e assinaturas digitais.

3.1 Criptografia Simétrica ou de Chave Privada

Proteger uma informação, e garantir sua privacidade, ou confidencialidade, precisa-se de um algoritmo de encriptação que trabalha em conjunto com uma chave de segurança (tipicamente representada por uma senha), que irá transformar uma mensagem original em uma mensagem criptografada ou cifrada, que não seja compreensível por um terceiro, como representado abaixo.

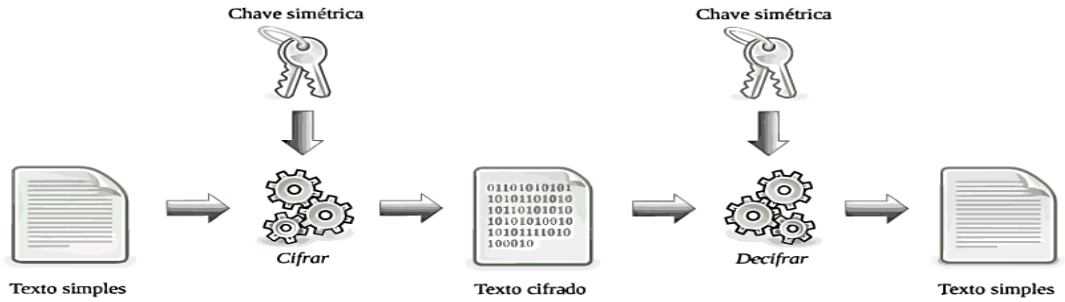
Figura 1: Cifrando uma mensagem



Fonte: Próprios autores (2021)

A criptografia simétrica utiliza algoritmos de chave única, ou seja, a mesma chave que foi usada para criptografar uma mensagem, necessariamente será a mesma a ser usada para descriptografar a mensagem, e essa chave é conhecida pelo emissor e pelo receptor.

Figura 2: Criptografia de chave simétrica



Fonte: medium.com/3xbit-academy/criptografia-parte-ii-387beaf4184b (2019)

Quando o emissor criptografa (ou cifrar) uma mensagem, é utilizado um algoritmo de encriptação que transforma o conteúdo em um texto cifrado, e para o receptor descriptografar (ou decifrar) a mensagem, ele utiliza o mesmo algoritmo para

converter o texto cifrado na mensagem original, porém se um interceptor (intruso), souber o algoritmo de encriptação ele pode decifrar a mensagem facilmente, como o receptor. Entra então a chave de segurança (chave simétrica ou privada), a ideia é que quando o emissor utilizar o algoritmo de encriptação, coloque também uma chave de segurança, por sua vez o receptor utiliza o mesmo algoritmo e a mesma chave para decifrar o texto, o interceptor se não possuir esta chave não conseguiria decifrar a mensagem.

A vantagem desse tipo de criptografia está na facilidade de implementação e velocidade de processamento, porém o problema desse tipo, é que a chave deve ser compartilhada entre origem e destino e armazenada em um local seguro, mas durante o compartilhamento essa chave pode ser interceptada, o que é fundamental utilizar canais seguros para esse compartilhamento, fora que nessa modalidade não é possível garantir os princípios de autenticidade e não repúdio.

A seguir estão apresentados os principais algoritmos de encriptação de chave simétrica:

Quadro 1: Principais algoritmos de criptografia simétrica

Algoritmo	Tamanho (bits)	Descrição
DES	56	Data Encryption Standard, um dos primeiros modelos de criptografia a ser implementado da programação com tamanho aproximado de 56 bits, criado em 1977 pela IBM, inseguro hoje em dia, pois pode ser decifrado por força bruta (baseada em tentativa e erro), apesar de inseguro hoje, foi o algoritmo mais disseminado no mundo até o AES.
3DES	168	Triple DES é uma variação mais avançada para substituir o DES, esse algoritmo trabalha com três chaves diferentes de 56 bits, seguro, porém lento, mas já foi considerado padrão recomendado.

DESX	120	DES-X é mais uma variação do DES, uma solução simples eu aumento a resistência do algoritmo original, com objetivo de resistir a ataques de força bruta, a diferença é a adição de 64 bits antes da encriptação, porém atualmente está se tornando ultrapassado contra ciberataques mais sofisticados, como as criptoanálises (programas que evoluem a cada tentativa).
AES	128	Advanced Encryption Standard, um dos algoritmos mais populares e seguros desde 2006, com alto nível de eficiência e confidencialidade, padrão adotado pelo governo dos Estados Unidos. Tem um bloco de tamanho fixo 128 bits, e uma chave com tamanho de 128, 192 ou 256 bits, conhecido como um algoritmo quase “imune” a todos os tipos de ataques exceto ataques de força bruta.
IDEA	128	International Data Encryption Algorithm, criado em 1991 por James Massey e Xuejia Lai, segue com estrutura semelhante ao DES, mas opera blocos de informação de 64 bits e chaves de 128 bits, ela utiliza princípios de confusão, que impede e realinhamento das informações, usado principalmente no mercado financeiro e PGP, programa para criptografia de e-mail pessoal.
RC	8 a 1024	Ron’s Code ou Rivest Cipher, criado por Ron Rivest da RSA Data Security, utilizado no protocolo S/MIME, popular par criptografia de e-mails, de tamanho variável. Rivest também possui as versões RC4, RC5, RC6.
Blowfish	32 a 488	Criado por Bruce Schneir em 1993, popular em e-commerce, com confiabilidade em lidar com métodos de pagamento, reconhecido pela velocidade e confiabilidade, além de ser open source (não patenteado,

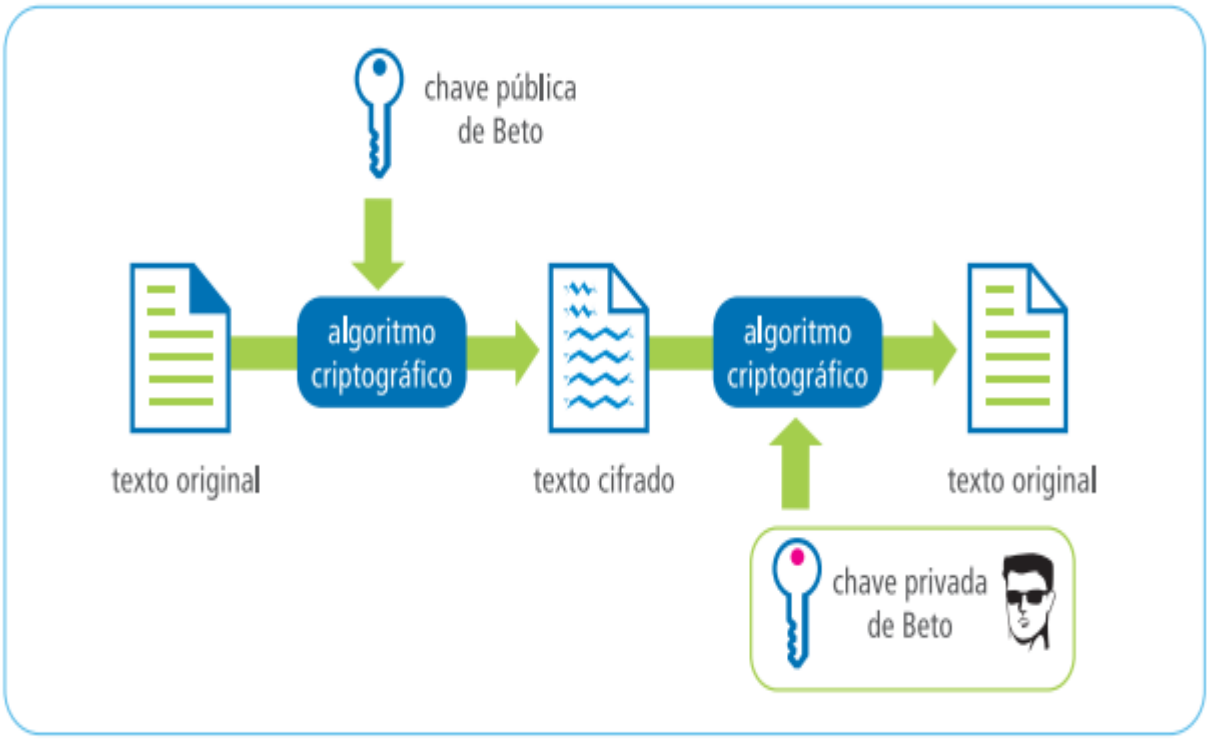
		sua licença é livre). Segmenta as informações em blocos de 64 bits aperfeiçoado no Twofish.
Twofish	128	Variação do Blowfish por blocos de 128 bits e chaves de 256 bits, também é de uso livre para qualquer um sem restrição.

Fonte: ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf (2012)

3.2 Criptografia assimétrica ou de chave pública

Esse modelo de criptografia assimétrica criado em 1970 por um matemático chamado Clifford Cocks, e veio para solucionar alguns problemas do modelo simétrico, esse utiliza um par de chaves, uma chave pública e uma privada, diferentes, porém complementares. A chave privada deve ser mantida em segredo, e a chave pública pode ser distribuída livremente, assim o interceptor tem acesso à chave pública, mas não consegue decifrar a informação, mas diferente da simétrica, aqui a chave pública é usada para criptografar a mensagem e a chave privada usada para decifrar.

Figura 3: Criptografia de chave assimétrica



Fonte: jkolb.com.br/criptografia-assimetrica/ (2015)

Diferente da chave simétrica, onde a chave usada para cifrar não é a mesma para decifrar, não é preciso compartilhar a chave privada, e os dados criptografados só podem ser decifrados por ela, soluciona-se então um problema, pois agora fornece garantia de confidencialidade, autenticidade e não repúdio enquanto a chave privada estiver segura. Assim qualquer um pode enviar uma mensagem criptografada sem o risco de quebrar a confidencialidade, por uma interceptação, é mais segura e complexa, com isso também é mais lenta que a simétrica.

Do mesmo jeito a criptografia assimétrica possui algoritmos de encriptação, mais no caso, com uso de chaves assimétrica:

Quadro 2: Principais algoritmos de chave assimétrica

Algoritmo	Descrição
RSA	Um dos mais usados até o momento e uma das mais poderosas formas de criptografia, criado em 1977 por Ron **Rivest**, Adi

	Shamir e Leonard **Adleman**, professores do MIT, essa forma utiliza dois números primos grandes que são multiplicados para gerar um terceiro número mas muito difícil de recuperar os dois primos que o geraram, os números primos são a chave privada e o terceiro é a chave pública, ou seja é muito difícil descobrir a chave privada a partir da chave pública, pois seria necessário um poder de processamento muito alto. Para descobrir tais números envolve fatorar esse terceiro número, que por sua vez é muito grande, não sendo possível fazer isso em tempo razoável. A segurança desse algoritmo se baseia na dificuldade de fatorar esse número gerado pela multiplicação de dois números primos.
ElGamal	Criado pelo egípcio Taher Elgamal em 1984, opera com a manipulação de grandes quantidades de números, também de forma cumulativa, sua segurança se baseia na dificuldade de calcular o chamado “logaritmo discreto” (na matemática são grupos análogos a logaritmos naturais, um logaritmo é a solução de uma equação (“a^x = b”.).
Diffie-Hellman	É baseado no problema de logaritmo discreto, publicado em 1976, criado por Whitfiels Diffie e Martin Hellman, porém não é um sistema de encriptação, e sim um sistema para troca ou compartilhamento de chaves de forma segura, em meios públicos.

Fonte: ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf (2012)

Observa-se, portanto, que as criptografias, sejam simétricas ou assimétricas são desenhadas por algoritmos e estes, se propõe em garantir que a efetiva segurança seja aplicada nas transações. Evidencia-se, porém, que as criptografias de chaves assimétricas possuem uma tecnologia mais avançada, garantindo um grau de segurança maior.

3.3 Assinatura Digital

Pode-se dizer que assinatura digital é uma adaptação da assinatura de próprio punho para o ambiente virtual. Por estar necessariamente em um documento eletrônico, ela é uma identidade eletrônica, ou seja, é a identificação de um documento, que garante autenticidade, integridade e não-repúdio da informação.

A assinatura digital de baseia no processo inverso da criptografia assimétrica, como falado anteriormente, pois como já verificado, enquanto a criptografia assimétrica usa duas chaves, uma pública para cifrar as informações e outra privada para decifrar, a assinatura digital faz o inverso, utilizando a chave privada para cifrar e, a chave pública para decifrar, onde o receptor deve usar a chave pública para decifrar a assinatura e verificar a validade da informação.

Como vimos anteriormente, na modalidade de chave assimétrica, qualquer um pode ter acesso a chave pública, ou seja, qualquer um pode acessar e verificar a assinatura digital, logo é importante lembrar que ela garante apenas autenticidade, integridade e não-repúdio da informação, e não a confidencialidade. No caso vai possibilitar identificar a autoria do documento ou se foi alterado.

Agora, para fazer a validação dessa assinatura, para saber se a informação é realmente do remetente que esperava receber ou se foi adulterado, a assinatura digital é apoiada pela função *hashing*, pois se alguém modificar o conteúdo, no momento que o receptor for validar, o sistema de verificação não irá reconhecer a assinatura como válida, identificando assim, que aquela assinatura não é a de quem esperava receber ou foi adulterada.

Logo, a função *hash* apoia a assinatura digital, pois assegura que a mensagem recebida é a mesma enviada pelo remetente e não foi adulterada A função *hashing é* conhecida também por resumo, pois gera um valor pequeno, de tamanho fixo (geralmente de 128 a 256 bits), derivado da informação ou documento (de tamanho variável) que se pretende assinar, independentemente do tamanho desse documento. Como mostrado abaixo com exemplo de um valor hash.

Figura 4: Gerando um hash

Fonte: criptonoticias.com.br/o-que-e-uma-cadeia-de-blocos-block-chain/ (2020)

Observa-se, conforme imagem acima que quando um documento é calculado através de uma função *hashing*, é gerado um valor de tamanho, também chamado de resumo, e qualquer modificação mínima no documento, geraria a alteração do valor *hash*, sendo, a partir daí, possível identificar as alterações em um documento.

3.4 Criptografias utilizadas nas empresas

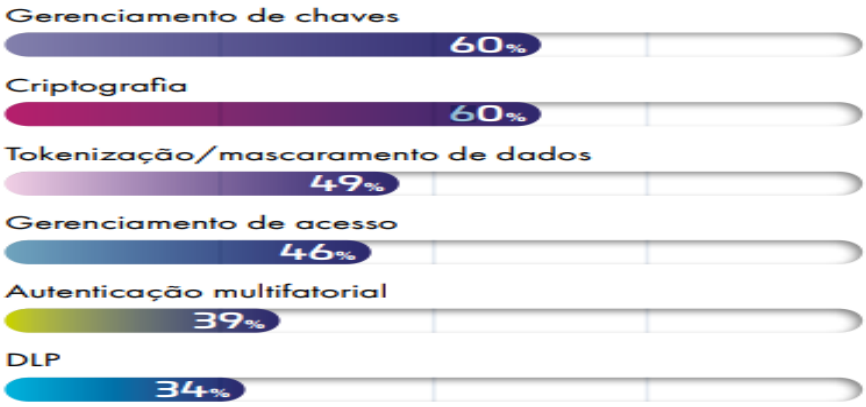
É difícil listar o algoritmo criptográfico individualmente mais usados, pois a criptografia está incorporada em muitas ferramentas, porém esse tópico objetiva apresentar o tipo de criptografia mais usado nas empresas. Será demostrado, de forma genérica, pois os processos para garantir a segurança da informação em uma empresa não são apenas um. Vamos verificar alguns tipos de criptografias utilizadas em algumas empresas, tais como, Amazon, Google e Microsoft.

Mas antes, é importante salientar que os dados ou informações podem ter dois estados, sendo em trânsito ou em repouso, e a proteção da informação é diferente em cada estado. Os dados em repouso podem ser criptografados normalmente de acordo com a escolha ou necessidade da empresa, porém os dados em trânsito geralmente são protegidos por protocolos, que já possuem uma criptografia incorporada.

- **Dados em repouso:** são os dados que não estão em movimento, estão armazenados, em servidores locais ou em nuvem, em computadores, drivers externos entre outros.
- **Dados em trânsito:** são os dados que estão em movimento, que estão transitando na rede, pode ser pública como a internet ou privada, como uma rede local de uma empresa.

No gráfico a seguir, pode-se observar as tecnologias descritas como a mais utilizadas pelas empresas na busca pela proteção dos dados.

Gráfico 1: Tecnologias de segurança que empresas utilizam



Fonte: Thales (2021)

Criptografia lidera em utilização pelas empresas junto com gerenciamento de chaves, que consiste em armazenar e organizar as chaves criptográficas.

A empresa *Amazon*, atualmente, oferece muitos tipos de serviços, além do seu *e-commerce*, quando se verifica sua plataforma de computação em nuvem *Amazon Web Services* (AWS), observa-se a proteção dos dados em repouso. Além disso, empresa oferece alguns modelos de proteção, um deles é, criptografia no lado do cliente, onde o método de criptografia fica sob a responsabilidade do usuário, ou seja, o tipo de criptografia a ser usada fica por escolha do usuário, outro modelo é, criptografia no lado servidor, em que o método de criptografia fica sob responsabilidade da empresa, ou seja, o tipo de criptografia usada é de escolha da empresa.

Pensando na criptografia no lado servidor, de acordo com o artigo da *Amazon* (2013, pg.12) “o padrão principal utilizado é do tipo simétrico, algoritmo AES-256 bits”, já citado anteriormente.

A empresa *Google* também oferece inúmeros serviços, como o Google Cloud, sendo uma plataforma de computação em nuvem, e em muitos processos para proteção dos dados. Aqui o padrão de criptografia AES está muito presente também.

A *Microsoft* na sua plataforma Azure (destinada à execução de aplicativos e serviços em nuvem), também utiliza o padrão AES, porém possui uma hierarquia de chave muito interessante. Essa “hierarquia” usa a criptografia AES-256bits para criptografar os dados, a chave usada para cifrar esses dados são chamadas de DEK

(chave de criptografia de dados), e utilizam uma criptografia assimétrica que criptografa as DEKs, chamado de KEK (chave de criptografia de chave).

Vale ressaltar que esse padrão de criptografia assimétrica AES, também foi adotado pelo governo dos Estados Unidos, e foi aprovada pela Agência Nacional de Segurança (NSA), para proteger dados ultrassecretos.

Portanto o tipo de criptografia mais usado pode ser confuso de posicionar exatamente, pois, existem, por exemplo, diversos tipos de protocolos voltados para segurança de dados em transito, que possuem criptografias incorporadas, e geralmente são assimétricas. Contudo, o algoritmo AES é o mais utilizado e não tem custo, e está presente na maioria dos processos de criptografia nas empresas, principalmente em dados em repouso, tratando-se do tipo simétrico, sendo o mais comum, devido sua simplicidade e rapidez.

Como apresentado no gráfico acima, existem outra formas de proteger dados, entre elas a *Tokenização*. *Token* é uma representação digital de um ativo real de uma empresa, que é qualquer recurso que tenha valor econômico. Já *Tokenização* é o termo para esse processo, em que um ativo real passa a ser representado de forma digital, por um *token* criptografado, e isso acontece dentro da *blockchain*, falado mais adiante.

Já, Gerenciamento de acesso está relacionado ao gerenciamento de quem tem acesso aos recursos, quais áreas e o que tem permissão de fazer, dentro de uma empresa ou um sistema por exemplo. A autenticação multifatorial é a maneira mais simples de proteger dados, é garantir a identidade do indivíduo por múltiplas tecnologias ou fatores, por exemplo, quando colocamos um PIN com senha em um celular, isso seria um único fator, agora colocar um PIM com reconhecimento facial e/ou biometria, seria multi-factor, a utilização de múltiplas tecnologias para autenticar um usuário.

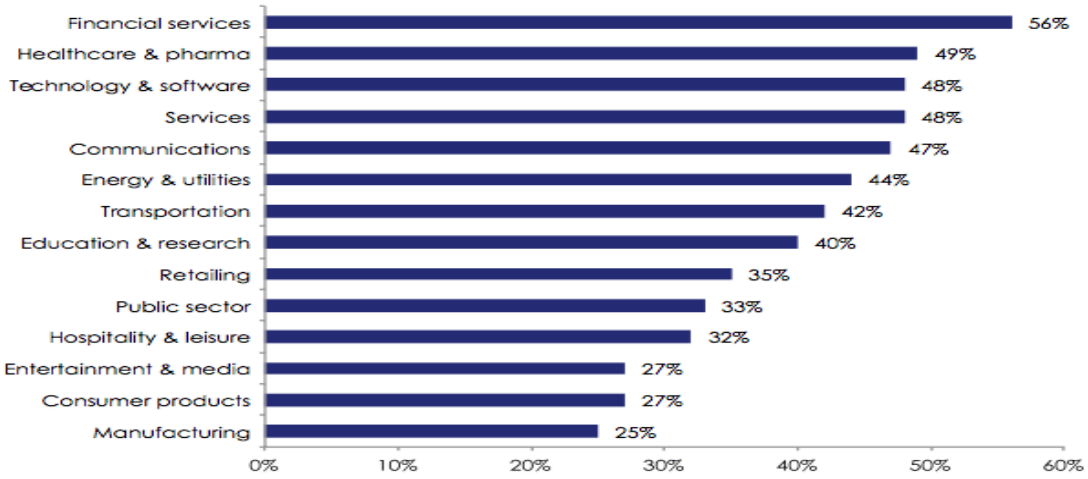
E, por último, o DLP ou Data Loss Prevention, que se trata de uma solução, através de um software que trabalha na prevenção de perda de dados, detectando possíveis violações de dados, além de bloquear dados sensíveis.

3.5 Criptografias usadas em instituições financeiras

As instituições financeiras têm ganhado notoriedade quando se trata de segurança da informação. Por serem alvo de ataques, e trabalharem com dinheiro, o interesse em manter os dados seguros de extrema importância. É interessante comentar, o aumento exponencial da adoção da criptografia nas empresas, desde 2015. O site *CIO* (2016), revela que a adoção da criptografia nas empresas, em particular, no setor financeiro, é o que mais investe. \

Pode-se observar o gráfico abaixo a adoção de medidas de segurança pelas empresas.

Gráfico 2: Adoção da criptografia nas empresas



Fonte: cio.com.br/tendencias/uso-de-criptografia-cresce-nas-empresas/ (2016)

Em geral a utilização da criptografia nas instituições financeiras pode ser aplicada da mesma maneira, como falado no tópico anterior, porém dados em trânsito podem ser mais frequentes do que em repouso, e muitos bancos atualmente estão adotando uma tecnologia chamada *blockchain*, para transações financeiras seguras, tecnologia que surgiu junto com a *bitcoin.*

O *blockchain* é chamado de um “grande livro contábil”, mas ele é um banco de dados com armazenamento de forma pública. Trata-se de um banco de dados distribuído, onde as transações são criptografadas, e o armazenamento é feito em

sequência de blocos interligados, validados pela função *hash*, sendo blocos que se formam em períodos. Quando um bloco se forma ele é “carimbado” com um número único (*hash*), e o próximo bloco se conecta a ele e assim por diante, como a figura abaixo:

Figura 05: Blocos de armazenamento do blockchain

Fonte: blog.mercadobitcoin.com.br/blockchain-o-que-e-como-funciona-e-qual-a-tecnologia-usada (2021)

Conforme ilustra a figura acima, trata-se de um número único do bloco, em sequência, que leva em consideração o número do bloco passado. Então, cada bloco subsequente depende do anterior, e se for mudado algum dos blocos anteriores, todos os blocos da frente mudam também. Esta estratégia torna o sistema muito difícil de ser burlado, proporcionando maior segurança. Além disso, o *blockchain* tem criptografia incorporada, tratando-se de um tipo assimétrico.

Essa tecnologia tem sido adotada por empresas no mundo todo, mas temos casos de instituições brasileiras que adotaram essa tecnologia para otimizar transações internacionais e outros processos, como o Itaú Unibanco, Santander, Banco Central do Brasil.

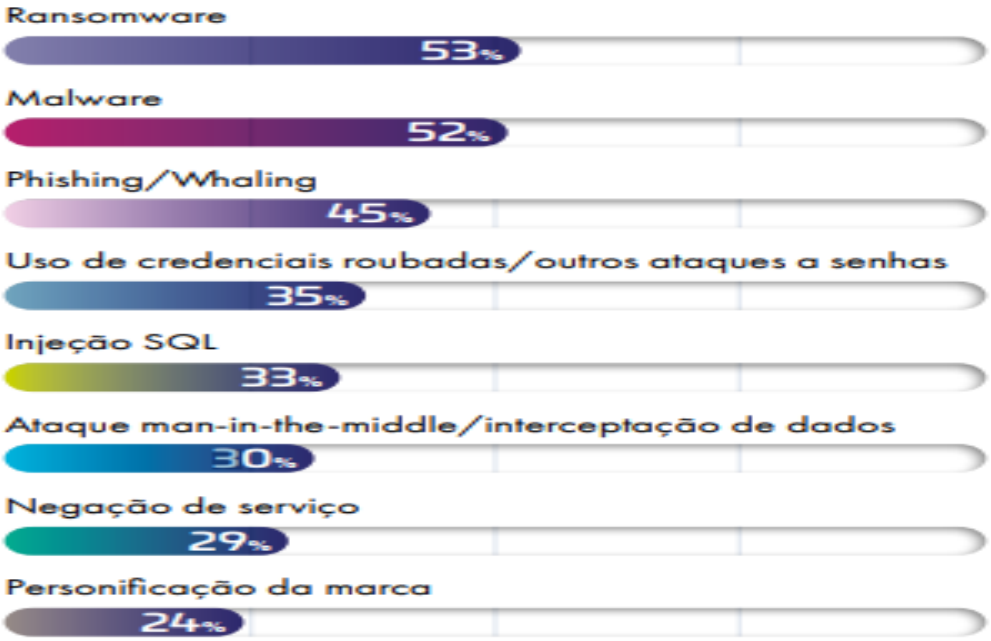
Portanto, pode-se afirmar que o *blockchain* é uma tecnologia versátil e segura, que tem crescido bastante no setor financeiro, e pode registrar tanto transações financeiras, quanto dados médicos, além de fluxos de caixa, entre outros. Também reduz os riscos de fraudes, porém sua segurança depende da criptografia, estando incorporada a ele a do tipo assimétrica.

3.6 Níveis de segurança e ataques

Com o aumento de tecnologias da informação, dados e informações importantes estão cada vez mais se tornando virtuais, até mesmo se tratando de dinheiro, ou seja, o aumento no número de ataques cibernéticos aumenta, com pessoas maliciosas tentando roubar informações.

Thales (2021, pg. 6), trouce informações importantes, relacionadas aos tipos de ataques decorrentes na rede, que colocam em “xeque” os sistemas de segurança. O gráfico abaixo ilustra bem isso.

Gráfico 3: Tipos de ataques que mais aumentaram



Fonte: Thales (2021)

Observa-se acima, que existem vários tipos de ataques a dados na web, vamos entender, um pouco, cada um deles.

Quadro 3 – Tipos de Ataques cibernéticos

Tipo de ataque	Descrição
Ransomware	É um tipo de ataque que usa da própria criptografia, este ataque quando infecta um sistema, restringe o acesso ao sistema ou aos dados criptografando-os, e os malfeitores cobram um determinado valor para reestabelecer o acesso.
Malware	Classifica todo tipo de softwares malicioso, intencionalmente feito para executar funções que cause danos a um computador, com por exemplo softwares com vírus, que infectam um computador.
Phishing	É a tentativa de obter ilicitamente dados pessoais de outra pessoa, caracteriza-se em uma técnica que engana usuários, induzindo-os a enviar dados pessoais e confidenciais, como por exemplo o recebimento de um suposto e-mail do seu banco pedindo atualizações de dados, contendo um link para um site falso, em que o usuário compartilharia seus dados com o hacker, sem saber.
Uso de credenciais roubadas	Tentativa de conseguir acesso a bancos, contas de e-mail ou redes sociais, onde um hacker coleta dados roubados de empresas, ou que conseguiu informações vasadas ou compradas, a fim de conseguir acesso indevido.
Injeção SQL	Ataque onde o hacker aproveita de uma falha da uma aplicação, e injeta códigos para violar as medidas de segurança, podendo controlar o banco de dados de um software e ter acesso aos dados da de usuários ou da empresa.
Ataque MITM	(man-in-the-middle) ataque onde os dados durante a comunicação de duas partes, são interceptados, e

	o interceptor pode registrar esses dados ou se colocar entre as duas partes, por exemplo o envio de faturas de um banco para um usuário, poderia ser interceptado e o hacker se passar pelo banco, mandando faturas falsas ao usuário.
Negação de serviço	(DoD) É a tentativa de indisponibilizar os recursos de um sistema.
Personificação da marca	É a tentativa de se passar por uma marca, como exemplo mensagens falsas se passando como se fosso de um determinado banco.

Fonte: Próprios autores (2021).

A criptografia como dito, tem objetivo de proteger dados e informações, independentemente do tipo de ataque, podendo ele ser qualquer um dos citados acima.

Contudo, o relatório de *Security Report* da ESET (2021, pg. 4), aponta que, “ataques de força bruta cresceram 704% somente na América Latina” em 2021, ataques de força bruta é justamente, o tipo de ataque em que tenta quebrar as criptografias, tentando descobrir as chaves usadas, por isso é importante adotar padrões de criptografias seguros, e o padrão AES é considerado o mais forte.

Porém, é fato que a criptografia não trabalha sozinha na segurança da informação, sendo necessárias outras ações tais como, controle de acessos, sistemas de senhas, realização de backups periodicamente, manutenção nos equipamentos entre outros, mas com certeza, a criptografia desempenha uma função indispensável. Além disso, para garantir sua segurança, alguns sistemas ou tecnologias dependem da criptografia, como por exemplo, a *blockchain*, sendo ela determinante no oferecimento de segurança e garantia de proteção dos dados.

4. CONSIDERAÇÔES FINAIS

Conclui-se, em síntese, que a utilização de criptografias varia bastante de acordo com a necessidade de cada situação, sendo a utilização do modelo assimétrico a mais utilizada, pois está mais presente nas plataformas, além de apresentar uma resposta mais rápida. Porém, é comum o emprego de tipos diferentes, trabalhando em conjunto, a medida em que serviços e base de dados são informatizados. Cresce, daí, portanto, a necessidade de proteger dados pessoais, mantendo a privacidade dos usuários, usando a criptografia como ferramenta para atingir tal necessidade.

É fato que segurança da informação é um assunto muito extenso, sendo importante enfatizar que a criptografia não opera sozinha, pois não é, e nem existe alguma solução única para resolver todos os problemas de segurança. Além de que, estamos longe de ter uma rede absolutamente segura, pois, assim como surgem novas tecnologias para proteger sistemas e dados, também surgem novas formas de burlá-los. Não podemos esquecer que as mesmas ferramentas utilizadas na proteção, também são usadas nos ataques, ou seja, tudo parte de códigos ou algoritmos.

Portanto, conclui-se que cada vez mais temos um número maior de informações trafegando na *web*, através de tecnologias inovadoras apresentadas ao mercado, em pequenos espaços de tempo, que necessitam de ferramentas de segurança, também inovadoras, para proteção dos dados, sendo a criptografia uma destas tecnologias.

REFERÊNCIAS

ADIL, Josué. **Entenda a importância da criptografia para segurança dos seus dados na internet.** Acadi-TI, 2019. Disponível em: <https://acaditi.com.br/entenda-a-importancia-da-criptografia-para-a-seguranca-dos-seus-dados-na-internet/> Acesso em: 24 out. 2021.

ALECRIM, Emerson. **Criptografia.** InfoWester, 2009. Disponível em: < https://www.infowester.com/criptografia.php> Acesso em: 22 set. 2021.

APPLE. **Visão geral da segurança do iCloud.** Apple, 2021. Disponível em: <https://support.apple.com/pt-br/HT202303> Acesso em: 26 out. 2021.

BEER, Ken; HOLLAND, Ryan. **Proteção de dados em repouso com criptografia.** Amazon, 2013. Disponível em: <https://d1.awsstatic.com/whitepapers/pt_BR/AWS_Securing_Data_at_Rest_with_Encryption.pdf> Acesso em: 24 out. 2021.

BURNETT, Steve; PAINE, Stephen. **Criptografia e Segurança:** O Gui Oficial RSA. Rio de Janeiro: Campus, 2000.

CERTIFICADORA, Valid. **Assinatura digital:** tudo o que você precisa saber. Valid, 2017. Disponível em: < https://blog.validcertificadora.com.br/assinatura-digital-tudo-o-que-voce-precisa-saber/> Acesso em: 18 out. 2021.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** O usuário faz a diferença. 1. Ed. São Paulo: Saraiva, 2006.

LAVADO, Thiago. **Uso da internet no Brasil cresce, e 70% da população está conectada.** G1, 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml> Acesso em: 26 out. 2021.

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação:** Princípios e controle de ameaças. 1. Ed. São Paulo: Saraiva, 2014.

MACHADO, Leia. **Mercado nacional de Segurança Cibernética deve atingir U$$ 1,8 bilhão esse ano.** Security Information News, 2019. Disponível em: < https://securityinformationnews.com/2020/02/06/mercado-nacional-de-seguranca-cibernetica-deve-atingir-us-18-bilhao-esse-ano/amp/> Acesso em: 22 out. 2021.

MARRETO, Valéria. **Cresce a busca por profissionais da área de cibersegurança.** Valor Economico, 2020. Disponível em: < https://valor.globo.com/carreira/noticia/2020/05/11/cresce-a-busca-por-profissionais-da-area-de-ciberseguranca.ghtml> Acesso em 17 out. 2021.

NUNES, Délio Silva. **PKI – Infraestrutura de chave pública.** UFRJ, 2007. Disponível em: <https://www.gta.ufrj.br/grad/07_2/delio/index.html> Acesso em: 1 nov. 2021.

PRISA, Pedro. **O que é Hash?.** TechTudo, 2012. Disponivel em: < https://www.techtudo.com.br/noticias/2012/07/o-que-e-hash.ghtml> Acesso em: 16 out. 2021.

THALES. **Relatório sobre ameaças a dados de 2021:** Segurança na nuvem e trabalho remoto. América Latina, 2021. Disponível em: <https://d335luupugsy2.cloudfront.net/cms/files/130669/16346515752021-relatorio-sobre-ameacas-a-dados-thales-pt.pdf> Acesso em: 24 out. 2021.

TOTVS, Equipe. **A importância da criptografia para sua segurança de dados.** Totvs, 2020. Disponível em: <https://www.totvs.com/blog/negocios/criptografia/> Acesso em: 23 out. 2021.

WHATSAPP. **Sobre a criptografia de ponta a ponta.** Whatsapp, 2021. Disponível em: < https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br> Acesso em: 15 set. 2021.

WHATSAPP. **Segurança do WhatsApp.** Whatsapp, 2021. Disponível em: < https://www.whatsapp.com/security> Acesso em: 15 set. 2021.