SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

SÁVIO DOS REIS FERREIRA

A UTILIZAÇÃO DA CRIPTOGRAFIA NO ENSINO DE MATRIZES

TOMÉ AÇU – PA
2022

SÁVIO DOS REIS FERREIRA

A UTILIZAÇÃO DA CRIPTOGRAFIA NO ENSINO DE MATRIZES

Trabalho de Conclusão de Curso, em formato de artigo, apresentado a Faculdade de Ciências Exatas e Tecnologia, do Campus Universitário de Abaetetuba, da Universidade Federal do Pará, como requisito obrigatório para obtenção do grau de Licenciado em Matemática.

Orientadora: Prof.ª Dr.ª Suellen Cristina Queiroz Arruda

TOMÉ AÇU – PA

2022

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

D722u. dos Reis Ferreira, Sávio.
A utilização da Criptografia no ensino de Matrizes / Sávio dos Reis Ferreira. — 2022.
24 f. : il. color.

Orientador(a): Profª. Dra. Suellen Cristina Queiroz Arruda
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Pará, Campus Universitário de Abaetetuba, Curso de Matemática, Abaetetuba, 2022.

1. Criptografia . 2. Matrizes . 3. Ensino. 4. Aprendizagem . I. Título.

CDD 510

SÁVIO DOS REIS FERREIRA

A UTILIZAÇÃO DA CRIPTOGRAFIA NO ENSINO DE MATRIZES

Trabalho de Conclusão de Curso, em formato de artigo, apresentado a Faculdade de Ciências Exatas e Tecnologia, do Campus Universitário de Abaetetuba, da Universidade Federal do Pará, como requisito obrigatório para obtenção do grau de Licenciado em Matemática.

Data da Aprovação: 09/09/2022

Conceito: EXCELENTE

Suellen Cristina Q. Arruda

Prof.ª Dr.ª Suellen Cristina Queiroz Arruda

Orientadora – FACET/CUBT/UFPA

Laila Conceição Fontinele

Profa. Dra. Laila Conceição Fontinele

Membro Interno – FACET/CUBT/UFPA

Nélio Santos Nahum

Prof. Me. Nélio Santos Nahum

Membro Externo – SEDUC/PA

A Deus primeiramente, aos meus pais, Edivaldo e Rosa, pelo amor, apoio e incentivo, sempre presentes em minha vida; à minha irmã Sâmia, pela ajuda financeira e apoio durante essa trajetória; à Silmara, minha namorada, pelo apoio total e por me incentivar sempre.

AGRADECIMENTOS

A Deus, pela dádiva da vida e por sempre me dar forças e permitir que eu chegasse até aqui.

Aos meus pais, Edivaldo Cunha Ferreira e Maria Rosa dos Reis, por sempre acreditarem em mim, pelo apoio e estímulo que sempre tiveram para comigo e pelo enorme amor e carinho que nunca deixaram faltar ao longo da vida.

À minha orientadora, Prof.ª Dr.ª Suellen Cristina Queiroz Arruda, pela orientação, força, paciência e compreensão, os quais foram essenciais para que esse trabalho fosse realizado.

Aos meus irmãos, Danilo, Salena e Sâmia, pelo apoio e incentivo sempre e, em especial, a Sâmia por ser uma das principais responsáveis por eu estar concluindo esse curso hoje.

À minha namorada, Silmara, pelo grande apoio e incentivo.

Aos meus familiares em geral, em especial, aos meus avós, Leocádio e Raimunda, pelo incentivo para estudar e buscar um futuro promissor.

Aos meus amigos de curso, pela parceria sem igual no decorrer das aulas e dos anos de faculdade, pelas risadas, pelos obstáculos vencidos e pela grande construção de uma amizade verdadeira e forte que se firmou entre nós a qual eu tenho uma imensa consideração por cada um.

A todos os professores do curso, que foram grandes mestres na arte de ensinar, pelo conhecimento repassado para todos da turma e por fazerem parte da realização deste sonho.

Enfim, agradecer a todos que contribuíram de alguma forma para que eu pudesse estar hoje realizando uma grande etapa da minha vida, meu fraterno carinho e obrigado a todos.

“A alegria está na luta, na tentativa, no sofrimento envolvido e não na vitória propriamente dita”.

(MAHATMA GANDHI).

A UTILIZAÇÃO DA CRIPTOGRAFIA NO ENSINO DE MATRIZES

Sávio dos Reis Ferreira[1]

Suellen Cristina Queiroz Arruda[2]

RESUMO

O presente trabalho propõe uma alternativa metodológica ao ensino de matrizes baseada na utilização da criptografia, possibilitando uma abordagem diferenciada das comumente aplicadas em sala de aula. A partir dos processos de codificação e decodificação de mensagens, buscou-se proporcionar uma aprendizagem mais significativa de matrizes aos alunos do terceiro ano do Ensino Médio da rede pública de ensino no município de Belém/PA. Com uma abordagem qualitativa, a pesquisa utilizou um questionário avaliativo da oficina matemática desenvolvida na escola. Os resultados mostram que a aplicação da criptografia auxilia no entendimento dos conceitos básicos de matrizes de uma forma dinâmica e interessante.

Palavras-chave: Criptografia; Matrizes; Ensino; Aprendizagem.

ABSTRACT

The present work proposes a methodological alternative to the teaching of matrices based on the use of cryptography, enabling a differentiated approach from those commonly applied in the classroom. From the processes of codification and decoding of messages, we sought to provide a more significant learning of matrices to third-year high school students from the public school system in the municipality of Belém/PA. With a qualitative approach, the research used an evaluative questionnaire of the mathematical workshop developed in the school. The results show that the application of encryption helps in understanding the basic concepts of matrices in a dynamic and interesting way.

Palavras-chave: Cryptography; Matrices; Teaching; Learning.

[1] Discente do Curso de Licenciatura em Matemática/CUBT/UFPA: savioreis19@gmail.com

[2] Docente orientadora. Doutora em Matemática: scqarruda@ufpa.br

INTRODUÇÃO

A criptografia surgiu como uma maneira de codificar as mensagens, tornando-as secretas. Um dos primeiros códigos descobertos é o famoso código de César, usado pelo ex-ditador romano Júlio César para conquistar territórios pela Europa e transformar Roma em um império.

> Enviar mensagens secretas é uma tarefa muito antiga. O homem sentiu, desde muito cedo, a necessidade de guardar informações em segredo; ela nasceu com a diplomacia e com as transações militares. Generais, reis e rainhas, durante milênios, buscavam formas eficientes de comunicação para comandar seus exércitos e governar seus países. A importância de não revelar segredos e estratégias às forças inimigas, motivou o desenvolvimento de códigos, cifras e técnicas para mascarar uma mensagem, possibilitando apenas ao destinatário ler o conteúdo (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 1).

Com o advento da tecnologia, a criptografia se conceitua como um recurso tecnológico utilizado para enviar mensagens em forma cifrada ou codificada, permitindo que apenas seu emissor e seu receptor tenham acesso ao conteúdo das mensagens criptografadas. Um dos seus princípios é usar seus mecanismos e suporte de segurança digital como ferramenta principal para proteção de dados e informações sigilosas de interesses individuais ou coletivos.

> A tecnologia e o interesse na proteção de dados evoluíram ao longo dos séculos, todavia, o grande impulsionador foi certamente o advento do computador, que introduziu uma nova realidade em termos de volume e guarda de dados. Diante deste novo cenário, a tecnologia para a proteção de dados, especialmente no campo da criptografia simétrica (chave única), foi responsável pelo surgimento de soluções que garantem a inviolabilidade dos dados, mesmo contra o uso do computador (ZANCANELLA, 2021).

No âmbito educacional, verifica-se a contribuição da criptografia no processo de ensino e aprendizagem da Matemática, pois consegue aguçar o interesse e a curiosidade dos alunos, visto que, a abordagem serve como uma motivação para fomentar a pesquisa sobre a temática e proporciona abordar conteúdos matemáticos de forma contextualizada com a realidade dos estudantes, conforme descreve Rosseto (2018, p. 5) no seguinte trecho:

> Usando a criptografia como ferramenta no ensino da Matemática, atribuímos significado ao conceito estudado, de forma que o aluno se sinta motivado a aprendê-lo. Assim, ressaltamos a importância de inserir o uso de assuntos ligados a realidade do aluno, que estimulem o empenho dos mesmos nas aulas, contribuindo de forma significativa para sua aprendizagem (ROSSETO, 2018, p. 58)

De acordo com Viviani e Costa (2010, p. 50-51) uma das dificuldades no processo de ensino-aprendizagem, e que de alguma forma pode comprometê-lo, é a falta de atividades práticas e a aproximação dos conteúdos abordados com a realidade dos alunos. Neste contexto,

o presente trabalho consiste na execução de uma oficina matemática a alunos do terceiro ano da Escola Estadual de Ensino Médio Augusto Meira com o intuito de possibilitar uma melhor compreensão de matrizes por meio da criptografia.

O trabalho está organizado da seguinte forma: na primeira seção, apresentamos alguns fatos históricos sobre a criptografia, seu conceito e importância nos dias atuais. Na segunda seção, evidenciamos as potencialidades do uso da criptografia no ensino da matemática, em especial, no processo de ensino e aprendizagem de matrizes, na perspectiva de tornar as aulas mais atrativas ao trabalhar os conceitos matemáticos atrelados à uma situação-problema real da sociedade. A terceira seção é destinada a descrição da oficina matemática realizada com os alunos do Ensino Médio. Por fim, a última seção, faz-se a apresentação e discussão dos resultados obtidos através do questionário avaliativo aplicado após a oficina.

1 UM BREVE HISTÓRICO DA CRIPTOGRAFIA

A palavra criptografia deriva do grego *kryptos*, na qual significa secreto, oculto. A criptografia tem como objetivo codificar uma mensagem para que apenas o seu destinatário tenha acesso e consiga decodificá-la.

> A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos 'códigos secretos', que todos já praticamos quando criança. O mais simples destes códigos consiste em substituir uma letra pela seguinte; isto é transladar o alfabeto uma casa para diante (COUTINHO, 2005, p. 1).

A cifra de César é um dos mais antigos e conhecidos, datado aproximadamente em 60 a.C., foi criado por Júlio César durante seu governo militar, com intuito de se comunicar com seus soldados e integrantes das corporações militares. O método utilizado no referido código é a substituição monossilábica, em que consiste em uma reorganização das letras do alfabeto, onde as mesmas são deslocadas. Portanto, isso faz com que seja muito simples e fácil de ser decifrado.

> A cifra de César é uma técnica de criptografia bastante simples e provavelmente a mais conhecida de todas. Trata-se de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto, porém deslocada um certo número de posições à esquerda ou à direita. A cifra de César recebe esse nome pois, segundo o escritor Suetônio, foi utilizada por Júlio César para se comunicar com seus generais, protegendo mensagens militares (REIS, 2016).

A cifra de Vigenère, desenvolvida pelo criptologista italiano Giovan Batista Bellaso em 1553, atribuída erroneamente a Blaise de Vigenère, utiliza várias combinações da cifra de

César, baseando-se na substituição polialfabética, ou seja, na substituição múltipla de alfabetos. Com este método de criptografia, é possível melhorar a cifra de César tornando-a mais segura e complexa. Ao longo de três séculos, a cifra de Vigenère se manteve inquebrável, chegando a receber a alcunha de "Le chiffre indéchiffrable" (A cifra indecifrável, em francês). Em meados de 1854, Charles Babbage elaborou a quebra da cifra de Vigenère, porém, o desenvolvimento da decodificação dessa valiosa cifra não foi suficientemente eficaz, tornando-se completa somente no ano de 1863 pelo criptógrafo e arqueólogo Friedrich Wilhen Kassiski.

> Para criptografar uma mensagem utilizando a Cifra de Vigenère, o primeiro passo é montar a grelha de Vigenère, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. O remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante. Esse sistema deve ser previamente combinado entre remetente e destinatário (BRANDÃO, 2017, p. 51).

Um outro método de criptografia bastante conhecido é a Cifra de Hill, desenvolvido pelo matemático norte americano Lester S. Hill em 1929, o qual consiste em um tipo de cifra de substituição tendo como suporte a álgebra linear. Segundo Brandão (2017, p. 53)

> A cifra de Hill consiste em um sistema de criptografia por substituição polialfabética, baseado em transformações matriciais. Para a aplicação de tal cifra, é necessário criar uma relação biunívoca entre as letras do alfabeto e um subconjunto dos números inteiros (BRANDÃO, 2017, p. 53).

Um marco importante na história da criptografia foi o estudo do francês Jean François Champollion para decifrar os códigos antigos da famosa Pedra de Roseta, levada para a França como espólio de guerra, mas que, atualmente, está exposta no Museu Britânico, em Londres. A Pedra de Roseta está escrita em três línguas e a sua tradução foi importante tanto para compreensão da história do Egito Antigo quanto para entender como o uso da criptografia está presente há muito tempo na sociedade.

> Nenhuma pedra é tão famosa quanto a de Roseta. O fragmento de um bloco que pesa quase 1 tonelada, mede 118 centímetros, tem 77 centímetros de largura e 30 de espessura, foi fundamental para a compreensão da história do Egito Antigo. O objeto, encontrado na cidade de Roseta, próxima a Alexandria, pelo exército de Napoleão em 1799, tem uma mensagem escrita em três línguas: hieróglifos, demótico e grego. A pedra virou o trabalho da vida do linguístico francês Jean-François Champollion, que também era professor de história, o que facilitou a missão. Ele trabalhou na tradução de 1822 e 1824, comparando as três línguas para transcrever o decreto. Com isso, conseguiu uma espécie de "chave mestre" para traduzir muitos outros documentos encontrados (REVISTA GALILEU, 2021).

Como podemos observar, a criptografia vem sendo utilizada há bastante tempo como

uma ferramenta de comunicação e informação, tendo uma grande importância em momentos cruciais na história da humanidade como, por exemplo, a Segunda Guerra Mundial. A criptografia na época fez-se necessária para envio e recebimento de mensagens secretas entre os comandos militares e seus aliados, presente em códigos e linguagens sigilosas, além do uso de máquinas para codificar e decodificar os códigos de guerra

> Com a Segunda Guerra Mundial consolidou-se a importância da informação e da criptografia. O volume de troca de mensagens e a necessidade da criptografia fez com que surgissem as primeiras máquinas de codificação. O exército alemão dispunha de uma máquina, conhecida como Enigma, cujo número de combinações gerada era da ordem de 15×10^{18}, o que a tornava praticamente impossível de ser quebrada. As cifras da Enigma foram quebradas por outra máquina, a Enigma Bomb, desenvolvida por Alan Turing. Com a quebra da Enigma os aliados ganham vantagem estratégica e vencem a Segunda Guerra (BRUNO. JORNAL DA USP, 2017).

Após as repercussões da Segunda Guerra Mundial, a criptografia passa a ter um papel fundamental no desenvolvimento dos computadores digitais e consequentemente da Internet, dando início a era da Criptografia computacional. Com o avanço tecnológico, a criptografia dá origem a uma importante ciência, a Criptologia, e ganha novas utilizações em vários contextos importantes na sociedade voltados a aspectos de segurança, tais como, sigilo em bancos de dados, aplicativos de comunicação e informações de crédito pessoal, conforme relata Bezerra, Malagutti e Rodrigues (2010, p. 2):

> Hoje em dia, entretanto, com o advento da comunicação eletrônica, a criptografia deixou de ser unicamente segredo de estado, pois muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet. Até recentemente, a criptografia era considerada uma arte; hoje em dia, entretanto, passou a ser considerada uma ciência. As aplicações da Criptografia atualmente incluem: sigilo em banco de dados; censos; investigações governamentais; dossiês de pessoas sob investigação; dados hospitalares; informações de crédito pessoal; decisões estratégicas empresariais; sigilo em comunicação de dados; comandos militares; mensagens diplomáticas; operações bancárias; comércio eletrônico; transações por troca de documentos eletrônicos (EDI); estudo de idiomas desconhecidos; recuperação de documentos arqueológicos, hieróglifos; e até tentativas de comunicações extraterrestres (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 2).

Portanto, a criptografia é de extrema importância para a humanidade e sua evolução ao longo dos tempos, desde a época da Grécia antiga até os dias atuais, provocando grandes transformações nas formas de transmitir as mensagens, garantindo privacidade e proteção nas comunicações.

2 MATRIZES E CRIPTOGRAFIA

O professor no uso de uma didática que busca conectar os conteúdos matemáticos com

situações presentes no cotidiano, possibilita a construção do conhecimento a partir da constatação da importância da Matemática para o indivíduo, estimulando assim uma aprendizagem mais significativa e a democratização do conhecimento. Esta prática docente está alinhada com as finalidades do Ensino Médio de acordo com os seguintes trechos da Lei de Diretrizes e Bases da Educação Nacional:

> O aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico; a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina; a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores (BRASIL, 1996).

Neste sentido, a criptografia surge como uma alternativa metodológica no ensino da matemática uma vez que a sua aplicabilidade em vários contextos ligados a tecnologia, além de despertar o interesse e curiosidade dos alunos em desvendar o mundo da criptografia, possibilita uma nova forma de ensinar conteúdos matemáticos a partir da contextualização de situações-problemas presentes no cotidiano da sociedade, conforme é apontado por Arinos (2014, p. 43):

> Sabemos que a matemática enfrenta diversos desafios na busca de ligar o interesse discente e a formação do cidadão, partindo do pressuposto que a educação se concretiza nesta relação. Portanto, aproximar a linguagem matemática da realidade é o foco de estratégias educacionais, para que os alunos se tornem cidadãos conscientes, apropriando-se de conhecimentos matemáticos fundamentais para uma formação crítica de nossa sociedade. Neste contexto, a criptografia pode ser um elemento motivador para o processo de ensino e aprendizagem da matemática, pois seu desenvolvimento histórico e sua aplicabilidade disponibilizam ao professor muitos exemplos contextualizados, ao mesmo tempo em que promovem uma interessante ligação com as ciências sociais e sociedade (ARINOS, 2014, p. 43).

O ensino da matemática através da criptografia torna-se uma abordagem de grande importância e utilidade tanto aos alunos quanto ao professor por se tratar de uma metodologia que possibilita o desenvolvimento cientifico e a busca por novos desafios para resolução de problemas matemáticos.

Segundo Tamarozzi (2001, p. 41),

> O tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo os conteúdos de matrizes e funções que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação de conteúdos matemáticos (TAMAROZZI, 2001, p. 41).

Partindo deste pressuposto, a aplicação da criptografia no ensino de matrizes soma e enriquece o processo de aprendizagem dentro da sala de aula ao apresentar o quão vasto e

importante é o seu estudo. Além disso, a utilização da criptografia proporciona dinâmica na construção do conhecimento sobre matrizes uma vez que, seu ensino sai da prática monótona ainda adotada por muitos professores no ensino tradicional, tornando o seu estudo cansativo e desinteressante, fato este mencionado por Moura (2018, p. 47):

> A criptografia pode ser usada como ferramenta para enriquecer o ensino da matemática, pois sua aplicabilidade abrange os diferentes níveis de ensino e auxilia no desenvolvimento de competências de leitura e escrita por meio da história, além de colaborar com a interdisciplinaridade e principalmente tornar o aprendizado mais significativo (MOURA, p. 47, 2018).

É importante frisar que as técnicas criptográficas são fundamentadas em alguns ramos da Matemática, tais como, a Álgebra Linear e a Teoria dos Números. De acordo com Druck, Hellmeister e Peixoto (2004, p. 71),

> Uma das maneiras de manifestação da Criptografia no ensino da matemática é vista no estudo de Álgebra Matricial. Para isto utilizando meios como a multiplicação de Matrizes e Matrizes Invertíveis como chaves, o que faz dificultar a violação da mensagem (DRUCK; HELLMEISTER; PEIXOTO, 2004, p. 71).

Diante disso, ao adotar um método onde o processo de codificação e decodificação de mensagens utiliza matrizes, a criptografia se torna uma ferramenta de ensino significativa no processo de ensino e aprendizagem do conteúdo matemático atrelado, possibilitando ao aluno aprender com maior facilidade por meio de técnicas que demonstrem o que está presente em seu cotidiano e ao docente uma nova abordagem de ensinar o assunto em sala de aula.

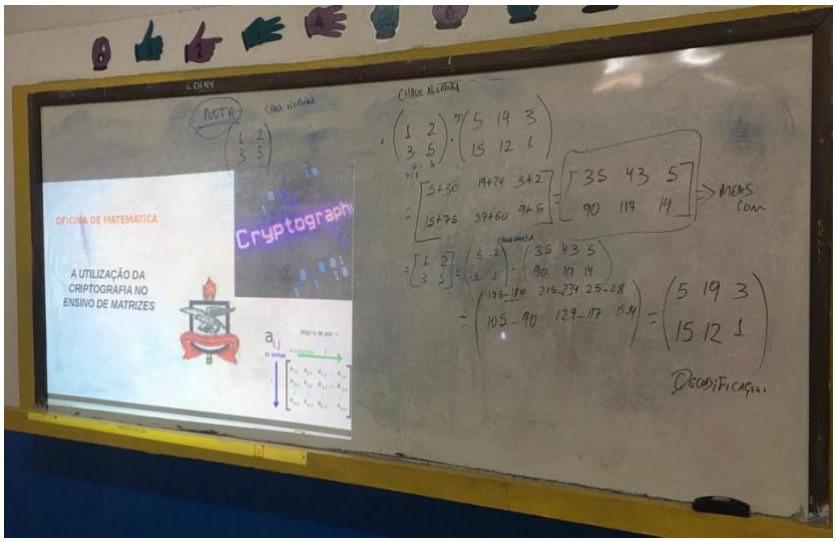
3 OFICINA MATEMÁTICA

Para alcançarmos o objetivo deste trabalho foi elaborada a oficina “A utilização da criptografia no ensino de matrizes” a ser aplicada a alunos do 3º ano do Ensino Médio da Escola Estadual de Ensino Médio Augusto Meira, no município de Belém/PA. Antecipadamente, a proposta foi apresentada a um professor de Matemática da escola, que gentilmente cedeu algumas aulas em 4 (quatro) turmas para a realização da intervenção metodológica. Cabe informar que os tópicos de matrizes abordados na intervenção já tinham sidos trabalhados pelo professor ou vistos no segundo aluno em outra escola.

No primeiro momento da oficina, em cada turma, foi perguntado aos alunos se eles sabiam o que era criptografia. A maioria dos alunos respondeu que não sabia do que se tratava, e os poucos que responderam algo, falaram que tinha a ver com aplicativos de mensagens ou internet. Com estas respostas, o conceito de criptografia foi introduzido, evidenciando a sua

relevância para a sociedade ao exemplificar a sua aplicabilidade na segurança de dados e informações confidenciais.

Figura 1 – Foto com o título da oficina exposto no quadro



Fonte: autoria própria (2022).

Figura 2 – Imagem de um dos slides utilizados na apresentação da oficina

Fonte: autoria própria (2022).

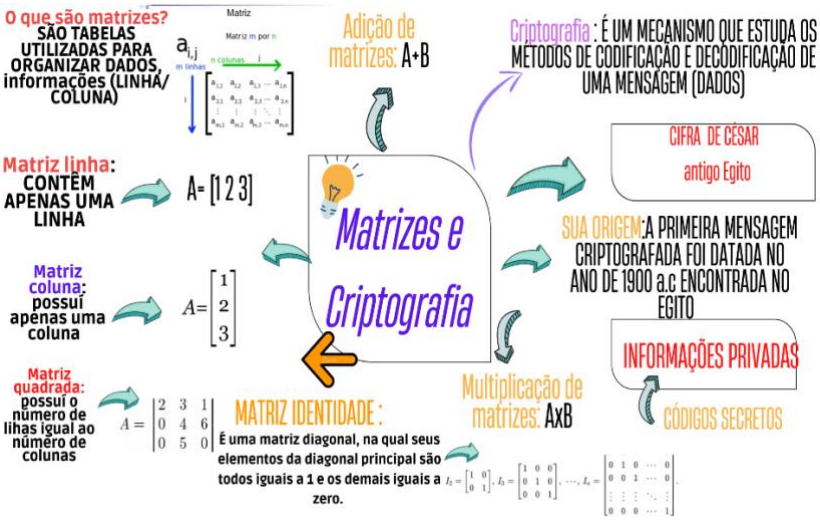
Dando continuidade, foi abordado o papel de grande importância da criptografia no século XX durante as guerras em que o mundo presenciou. Para despertar o interesse e a curiosidade dos estudantes em saber mais sobre o uso da criptografia nestes momentos históricos da humanidade, alguns filmes foram sugeridos, a saber: Códigos de Guerra, com

Nicolas Cage; The Gray Man, com Ryan Gosling e Chris Evans; e O Jogo da Imitação, com Benedict Cumberbatch.

Para abordar que esta necessidade de enviar mensagens com segurança é muito antigo, informou que na Grécia Antiga o ex-ditador Júlio César utilizava um sistema de substituição monoalfabética para se comunicar com os seus aliados de guerra, ficando conhecido como “cifra de César” e sendo considerado um dos mais antigos métodos criptográficos que se tem registro. No entanto, enfatizamos que o processo de codificação das mensagens utilizava somente as 26 letras do alfabeto e, com o passar do tempo, foi percebido que a cifra era muito simples e fácil de ser quebrada.

Em seguida, explicamos que para aplicar a criptografia no ensino de matrizes por meio da criptografia era necessário relembrar alguns tópicos sobre o assunto matemático. Dito isso, foram explanados o conceito e os elementos de uma matriz, dando alguns exemplos para a classificação em matriz linha, matriz coluna, matriz identidade e matriz quadrada. Além disso, abordamos as operações em matrizes, principalmente, a multiplicação entre matrizes e matriz inversa. Depois da exposição do conteúdo matemático, foi disponibilizado um mapa mental com intuito de ressaltar o conhecimento até então explorado na oficina, veja a Figura 3.

Figura 3 – Mapa mental com os tópicos abordados na oficina



Fonte: autoria própria (2022).

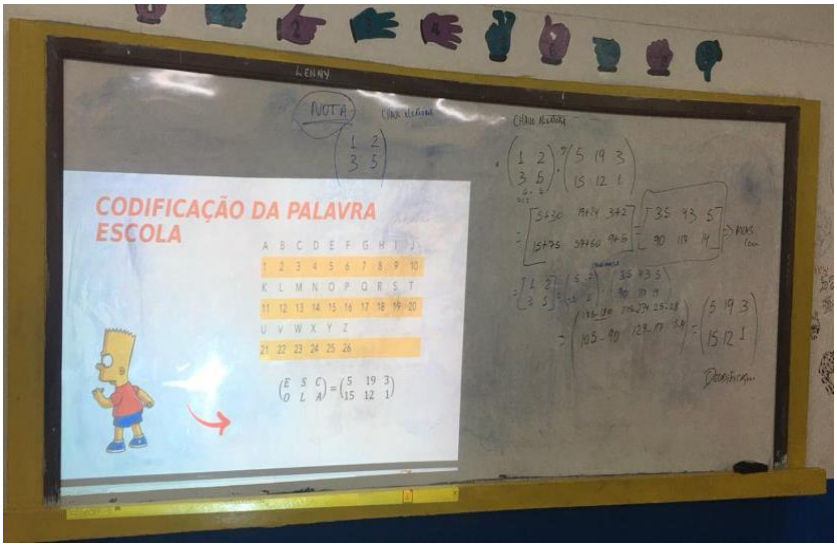
No segundo momento da oficina, introduzimos a atividade elaborada para relacionar matrizes e criptografia. Incialmente, falamos sobre a cifra de Hill, explicando que o processo de codificação e decodificação utiliza uma tabela com as letras do alfabeto enumeradas de 1 (um) a 26 (vinte e seis), conforme mostra a Figura 4, e uma chave aleatória para codificação

cujo propósito é proteger ainda mais a mensagem a ser transmitida. A chave aleatória deve ser de conhecimento apenas do remetente e do destinatário da mensagem. Feito isso, realizamos os seguintes passos com os alunos:

1º Passo: Dada a palavra ESCOLA para ser codificada, a partir da posição de cada letra no alfabeto, encontramos a matriz mensagem

$$M = \begin{pmatrix} 5 & 19 & 3 \\ 15 & 12 & 1 \end{pmatrix}.$$

Figura 4: Foto do alfabeto e da matriz mensagem codificada no quadro



Fonte: autoria própria (2022).

2º Passo: Para proteger ainda mais a mensagem, a chave dada para codificação foi a matriz $C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$. Ao realizarmos a multiplicação entres as matrizes C e M, nesta ordem, encontramos a matriz com a mensagem codificada

$$P = \begin{pmatrix} 30 & 69 & 10 \\ 55 & 119 & 17 \end{pmatrix}.$$

Neste momento, enfatizamos os tópicos necessários sobre matrizes para a obtenção da matriz P. Além disso, para a realização da atividade foi permitido aos alunos, o uso da calculadora no aparelho celular.

3º Passo: Para fazer a decodificação da mensagem, efetuamos uma nova multiplicação entre matrizes, desta vez utilizando a matriz inversa da chave aleatória e a matriz com a mensagem codificada. Assim, ao calcular $C^{-1} \cdot P$, obtemos a matriz

$$\begin{pmatrix} 5 & 19 & 3 \\ 15 & 12 & 1 \end{pmatrix}$$

e, assim, concluímos que a matriz resultante é a matriz M, a qual sabemos que corresponde a

palavra ESCOLA.

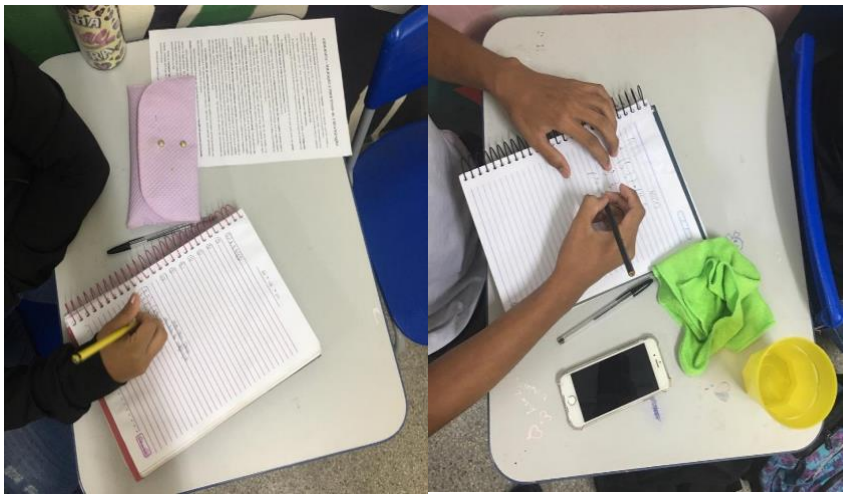
Nesta etapa da atividade, resgatamos os procedimentos teóricos anteriormente mencionados para determinar a matriz inversa C^{-1}. Além disso, explicamos que o procedimento realizado para a decodificação só foi possível porque a matriz C é inversível e, por este fato ao multiplicar a matriz P por C^{-1}, pela esquerda, obtemos a matriz M.

Em termos matemáticos, fizemos o seguinte:

$$C^{-1} \cdot P = C^{-1}(C \cdot M) = (C^{-1} \cdot C) \cdot M = I_2 \cdot M = M,$$

onde I_2 é a matriz identidade de ordem 2.

Figura 5: Alunos codificando e decodificando a mensagem.



Fonte: Autoria própria (2022).

Figura 6: Alunos resolvendo o desafio.

Fonte: autoria própria (2022).

No último momento da oficina, foi proposto um desafio aos alunos com a colaboração do professor da turma. Solicitamos ao docente que escolhesse uma palavra qualquer em segredo, esta seria criptografada por ele usando a mesma chave aleatória C dada anteriormente e, em seguida, decodificada pelos estudantes.

Após de sanada algumas dúvidas em relação a multiplicação de matrizes, os alunos conseguiram concluir o desafio com êxito obtendo a matriz da mensagem secreta, que ao consultar o alfabeto revelou-se que a palavra escolhida pelo professor foi a palavra NOTA.

4 RESULTADOS E DISCUSSÕES

Nesta seção será apresentado os dados do questionário avaliativo disponibilizado via formulário google aos alunos participantes da oficina matemática. O questionário foi respondido por 37 (trinta e sete) discentes das 4 (quatro) turmas do 3º ano do Ensino Médio onde a oficina foi executada e contava com as seguintes perguntas:

Pergunta 1: Você compreendeu o que é a criptografia?

Pergunta 2: A abordagem através da criptografia facilitou a compreensão sobre matrizes?

Pergunta 3: O que você achou da didática do ministrante da oficina?

Pergunta 4: O que você achou da oficina? Comente.

Pergunta 5: Qual parte da oficina que você achou mais interessante?

Do universo que responderam ao questionário avaliativo, 97,3% dos alunos informaram que compreenderam o conceito de criptografia. Cabe lembrar que no início da oficina, antes de introduzirmos o conceito de criptografia, os alunos foram questionados se sabiam do que se tratava, somente a metade dos alunos informaram que tinham escutado falar sobre o assunto, mas que não sabia explicar o que significava.

Considerando a segunda pergunta, 94,6% dos alunos responderam que a abordagem por meio da criptografia facilitou a compreensão dos tópicos de matrizes abordados na oficina. Com esse resultado, podemos inferir que o uso da criptologia, além de despertar a curiosidade dos estudantes, é uma potencialidade no processo de absorção do conhecimento sobre matrizes.

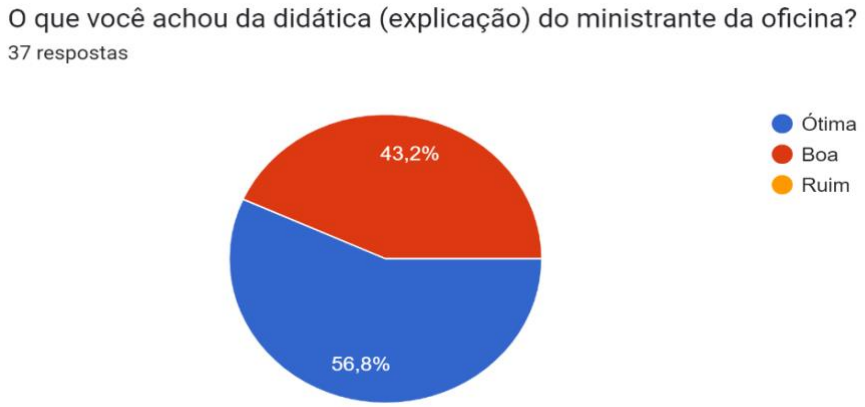
Observando o gráfico com as respostas da Pergunta 3, veja a Figura 7, foi possível constatar que a didática do ministrante da oficina foi bem avaliada pelos alunos, uma vez que 56,8% atribuíram o conceito ótimo e 43,2%, o conceito bom. Estes dados também são corroborados por alguns comentários obtidos na Pergunta 4:

> Muito interessante, os temas abordados de forma geral, foi uma boa experiência, e o professor repassou o conteúdo de forma muito boa e que deu para entender bastante.

> Achei bom, bem dinâmico, interação do professor foi boa para compreensão do assunto.
> Ótima! Eu achei muito didática e divertida.
> Super interessante, normalmente não participo de resoluções de trabalhos em sala, dessa vez senti animada para realizar a atividade.
> Interessante! O professor é prático e a explicação foi ótima, aprendi com facilidade.

Analisando os comentários obtidos na Pergunta 4, conclui-se que a grande maioria dos alunos teve uma boa percepção do assunto matrizes mediante a aplicação da criptografia. Assim, depreende-se a importância de que o professor utilize novas estratégias de ensino para capturar a atenção do aluno com intuito de que a aula seja mais produtiva e que os alunos possam aprender com mais facilidade e interesse, conforme podemos observar no seguinte relato acima: “superinteressante, normalmente não participo de resolução de trabalhos em sala, dessa vez senti animada para realizar a atividade”.

Figura 7: Gráfico sobre a didática do palestrante da oficina



Fonte: Formulário preenchido pelos alunos da Escola Augusto Meira (2022)

Com relação a Pergunta 5, pode-se constatar que, a parte mais interessante da oficina para os alunos foi o método usado para a explicação do assunto, pois o ministrante utilizou ferramentas capazes de aguçar a curiosidade e fazer com que os estudantes prestassem mais atenção, como, por exemplo, a utilização de filmes como referências para explicar o uso da criptografia e sua importância; os métodos criptográficos, entre eles, a cifra de Hill, utilizada no processo de codificação e decodificação das mensagens dadas no exemplo e no desafio. Esses mecanismos foram capazes de proporcionar aos discentes um melhor aproveitamento e compreensão sobre o conteúdo abordado, como pode-se verificar nas seguintes respostas à Pergunta 5:

> Foi quando ele explicou tudo sobre matrizes de forma que todos interagiram com

> perguntas, e o professor deixou bem claro o assunto sobre matrizes, foi uma aula muito boa.
> Quando ele usou filmes como exemplo para explicar sobre a criptografia e propôs um desafio para turma (eu ganhei) ;).
> As referências de filmes. O alfabeto posto em números.
> A parte sobre criptografia e questões de como criar uma senha codificada.
> Tudo, a abordagem dos conteúdos foi bem explicadas e deu de entender bem.
> O momento em que nos foi apresentado a leitura da criptografia (a tradução).
> A dinâmica de decodificação de códigos.

Portanto, os resultados da pesquisa foram importantes para a compreensão da necessidade do docente em buscar alternativas metodológicas que estimulem a participação discente no processo de ensino e aprendizagem de matrizes, utilizando exemplos que possam ser aplicados no cotidiano do aluno. A realização de aulas que desafiem a interação e a participação dos discentes é de suma importância para que eles possam aprender o que foi repassado em sala de aula e que sejam motivados a sempre buscar conhecimento.

A criptografia está intimamente presente na vida das pessoas, muitas vezes de forma imperceptível, sendo assim, é adequado usá-la como ferramenta motivadora para a aprendizagem da matemática, despertando aos alunos o prazer em aprender, conhecer e realizar as atividades relacionadas ao ensino, as dificuldades apresentadas pelos alunos na aprendizagem da matemática decorrem de vários fatores, entre eles pode-se destacar a falta de contextualização do conteúdo abordado, a procura por soluções para amenizar essa situação demanda do professor de matemática comprometimento, criatividade, persistência, espírito inovador entre outras virtudes (GRISELI, 2018, p. 10).

Desta forma, os dados da pesquisa contribuíram para se ter uma visão crítica da importância em adotar métodos diferenciados como a utilização da criptografia para complementar a abordagem tradicional do ensino de matrizes, possibilitando uma aula mais dinâmica e fazendo com que o discente tenha o prazer de estar em sala e com interesse naquilo que o professor está ensinando.

CONSIDERAÇÕES FINAIS

Ao chegarmos ao final do trabalho, consideramos que, o estudo da criptografia possibilita aos alunos uma interação com os conteúdos de matrizes de forma contextualizada, e que interligam os temas matemáticos a um tema atual, de forma que verificamos a presença da criptografia em diferentes situações e aplicações reais do aluno.

A partir dos estudos e pesquisas feitos sobre criptografia e matrizes, verificamos a grande importância em analisar e estudar cada detalhe presente na história e desenvolvimento de ambos os temas, tendo como proposta acerca da criptografia, trabalhar métodos

criptográficos que se aliam a conceitos matemáticos, como na atividade realizada na oficina de matemática, cujos processos de codificação e decodificação se deram a partir de uma cifra bastante conhecida, chamada cifra de Hill, que por sua vez se alia a conteúdos matriciais.

Outros métodos criptográficos também foram estudados como a cifra de César, a cifra de Vigenère e as máquinas criadas no período da Segunda Guerras Mundial. Esses fatores vistos no decorrer do trabalho foram essenciais para entender a história da criptografia desde os tempos antigos até sua modernização tecnológica, proporcionando desta maneira uma viajem ao tempo em relação ao histórico da criptografia.

Entendemos que a criptografia deveria estar mais presente nos currículos educacionais do ensino médio, uma vez que, seu uso se apresenta com muita aplicabilidade em diversas áreas importantes e interessantes não apenas da matemática como em várias outras ciências, como por exemplo na área computacional que interliga segurança de dados, arquivos confidenciais, dados bancários e muitos outros, ou seja, a influência da criptografia nos dias passados e atuais é de extrema importância para humanidade, uma vez que, ela está ligada a privacidade e a confiança do ser humano e de seus bens. Desta forma, tornando-se um dos vieses motivadores que despertaram o interesse para aprender conteúdos matemáticos.

Por meio da oficina matemática realizada em sala de aula, pude perceber e conhecer a importância do planejamento docente. A atividade foi muito interessante e empolgante, percebi o interesse dos alunos junto à vontade e motivação em aprender através de uma aula diferente e dinâmica, na qual foi possível ter uma visão como futuro professor de quais métodos podem contribuir para o ensino aprendizagem dos alunos. Portanto, espera-se que este trabalho possa colaborar nas discussões e reflexões docente em relação ao processo de ensino aprendizagem de matrizes, proporcionando aos discentes a construção do conhecimento a partir da curiosidade em desvendar o mundo.

REFERÊNCIAS

ARINOS, E. J. S. C**riptografia: aplicações no ensino fundamental e médio.** 2014. 100 f. Trabalho de Conclusão de Curso (Mestrado em Matemática PROFMAT) – Universidade Federal do Mato Grosso do Sul, Campo Grande, 2014. Disponível em: https://repositorio.ufms.br/bitstream/123456789/2154/1/EDGARD%20JOS%C3%89%20DOS%20SANTOS%20ARINOS.pdf. Acesso em: 05 de set. de 2022.

BEZERRA, D. D. J., MALAGUTTI, P. L., RODRIGUES, V. C. D. S. Aprendendo criptologia de forma divertida. *In*: BIENAL DE MATEMÁTICA, 5., 2010, João Pessoa, Paraíba. **Anais da V Bienal de Matemática da Sociedade Brasileira de Matemática – livro eletrônico /organização Universidade Federal da Paraíba**. Rio de Janeiro: SBM –

Sociedade Brasileira de Matemática, 2010. Disponível em: disponível em: http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final. Acesso em: 22 de jun. de 2022.

BRANDÃO, M. M. D. **Uma adaptação da Cifra de Hill para estudo de matrizes.** 2017. 92 f. Trabalho de Conclusão de Curso (Mestrado em Matemática PROFMAT) - Universidade Federal de Ouro Preto, Ouro Preto, 2017. Disponível em: https://www.repositorio.ufop.br/bitstream/123456789/9170/1/DISSERTA%C3%87%C3%83O_Adapta%C3%A7%C3%A3oCifraHill.pdf. Acesso em: 05 de set. de 2022.

BRASIL. Ministério da Educação. **Parâmetros Curriculares Nacionais (Ensino Médio).** Brasília, 1996. Disponível em: http://portal.mec.gov.br/setec/arquivos/pdf/BasesLegais.pdf. Acesso em: 15 de mar. de 2022.

BRUNO. O. M. **Criptografia: De arma de guerra a pilar da sociedade moderna-Artigo. JORNAL DA USP**. 2017 Disponível em: https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/. Acesso em: 05 de set. de 2022.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** Rio de Janeiro: IMPA, 2005. Disponível em: https://idoc.pub/queue/numeros-inteiros-e-criptografia-rsa-s-c-coutinho-impa-jlk902q8x545. Acesso em: 20 de jun. de 2022.

DRUCK, S., HELLMEISTER, C. P. PEIXOTO, C. M. **Coleção Explorando o ensino – Matemática (Ensino Médio),** vol 3. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2004. Disponível em: http://www.dominiopublico.gov.br/pesquisa/DetalheObraDownload.do?select_action=&co_obra=17171&co_midia=2. Acesso em: 20 de agosto de 2022.

GRISELI, R. C. **Criptografia: uma proposta para a educação básica**. 2018. 106 f. Trabalho de Conclusão de Curso (Mestrado em Matemática PROFMAT) - Universidade Federal da Fronteira Sul, Chapecó, 2018. Disponível em: https://rd.uffs.edu.br/bitstream/prefix/2637/1/GRISELI.pdf. Acesso em: 05 de set. de 2022.

MALAGUTTI, P. L. **Atividades de Contagem a partir da Criptografia.** Rio de Janeiro, IMPA, 2015. Disponivel em: http://www.obmep.org.br/docs/apostila10.pdf. Acesso em: 05 de set. de 2022.

MOURA, M. D. O. **A criptografia motivando o estudo das funções no 9º ano do ensino fundamental**. 2019. 93 f. Trabalho de Conclusão de Curso (Mestrado em Matemática PROFMAT) - Universidade Federal do Tocantins, Arraias, 2019. Disponível em: https://repositorio.uft.edu.br/bitstream/11612/1373/1/Mois%C3%A9s%20de%20Oliveira%20Moura%20-%20Disserta%C3%A7%C3%A3o.pdf. Acesso em: 05 de set. de 2022

REIS. F. D. Criptografia- Cifra de César**. Artigo, Revista Bóson Treinamentos em Ciência e Tecnologia** 2016. Disponível em: https://www.bing.com/ck/a?!&&p=f49f9b4d7c891c7eJmltdHM9MTY2Mjc2ODAwMCZpZ3VpZD0zNTA0MGQ1My1jZGViLTZkYjQtM2E5Yi0xYzJmY2MzYTZjMzQmaW5zaWQ9NTE3NA&ptn=3&hsh=3&fclid=35040d53-cdeb-6db4-3a9b-

1c2fcc3a6c34&u=a1aHR0cDovL3d3dy5ib3NvbnRyZWluYW1lbnRvcy5jb20uYnIvc2VndXJhbmNhL2NyaXB0b2dyYWZpYS1jaWZyYS1kZS1jZXNhci8&ntb=1. Acesso em: 22 de jun. de 2022.

REDAÇÃO GALILEU - **Revista Galileu - Conheça a Pedra de Roseta, que mudou a história da arqueologia 2021**– Disponível em: https://revistagalileu.globo.com/Ciencia/Arqueologia/noticia/2018/07/conheca-pedra-de-roseta-que-mudou-historia-da-arqueologia.html. Acesso em: 22 de jun. de 2022.

ROSSETO, C. K. **Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática -** 2018. 84 f. Trabalho de Conclusão de Curso (Mestrado em Matemática PROFMAT) - Universidade Estadual Paulista, Presidente Prudente, 2018. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/152825/rosseto_ck_me_sjrp.pdf?sequence=3&isAllowed=y. Acesso em: 03 de set. de 2022.

TAMAROZZI, A. C. **Codificando e decifrando mensagens.** ***In*** **Revista do Professor de Matemática** 45, São Paulo: Sociedade Brasileira de Matemática, 2001. Disponível em: http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/veiculos_de_comunicacao/RPM/RPM45/RPM45_08.PDF. Acesso em: 20 de jul. de 2022.

VIVIANI, D.; COSTA, A. et al. **Práticas de Ensino de Ciências Biológicas**. Centro Universitário Leonardo da Vinci – Indaial, Grupo UNIASSELVI, 2010. Disponivel em: https://www.bing.com/ck/a?!&&p=af734daa1b38783eJmltdHM9MTY2Mjc2ODAwMCZpZ3VpZD0zNTA0MGQ1My1jZGViLTZkYjQtM2E5Yi0xYzJmY2MzYTZjMzQmaW5zaWQ9NTE4Mw&ptn=3&hsh=3&fclid=35040d53-cdeb-6db4-3a9b-1c2fcc3a6c34&u=a1aHR0cHM6Ly9iaWJsaW90ZWNhdmlydHVhbC51bmlhc3NlbHZpLmNvbS5ici9saXZyb3MvYmFpeGFyLzM1NzI4&ntb=1. Acesso em: 28 de agosto de 2022.

ZANCANELA. L. C. **Artigo, Revista CRYPTOID- Proteção de dados por Luiz Carlos Zancanella, 2021**. Disponível em: https://www.bing.com/ck/a?!&&p=40471930ee8cd2caJmltdHM9MTY2Mjc2ODAwMCZpZ3VpZD0zNTA0MGQ1My1jZGViLTZkYjQtM2E5Yi0xYzJmY2MzYTZjMzQmaW5zaWQ9NTE2NQ&ptn=3&hsh=3&fclid=35040d53-cdeb-6db4-3a9b-1c2fcc3a6c34&u=a1aHR0cHM6Ly9jcnlwdG9pZC5jb20uYnIvc2FmZXdlYi9wcm90ZWNhby1kZS1kYWRvcy1wb3ItbHVpei1jYXJsb3MtemFuY2FuZWxsYS8&ntb=1. Acesso em: 03 de set. de 2022.