SEMCITEC

EE PEI PROFESSOR CELSO PIVA

Alexandre Pereira Nascimento

CRIPTOGRAFIA: A MATEMÁTICA, EM SALA DA AULA, DE FORMA LÚDICA E DESAFIADORA

Guarulhos
Setembro/2023

RESUMO

Este trabalho tem por objetivo colocar o aluno como protagonista do processo de aprendizagem de forma lúdica. Assim, visa a compreensão da ideia geral sobre a criptografia, por parte dos educandos, permitindo que os indivíduos se envolvam diretamente com o conteúdo estudado. Por meio de conflitos cognitivos, os alunos constroem suas próprias maneiras de pensar, organizar ideias e estratégias para a resolução de problemas. Inicialmente, é apresentado um método específico de codificação de mensagens que não é enfatizado como o modelo único e central, concedendo a cada grupo formado autonomia e liberdade criativa para desenvolver sua própria cifra para ocultar uma mensagem. Ao longo do processo, fica evidente que a construção e concretização de conceitos não está ligada a condições sociais, mas à articulação de novas experiências e conhecimentos adquiridos anteriormente. As atividades produzidas pelos alunos mostram aprendizado significativo, indicando a internalização da ideia geral de criptografia. Embora os resultados sugiram que os objetivos tenham sido alcançados, ajustes são necessários devido a erros observados durante o processo de codificação de mensagens, afetando o procedimento de decodificação após a troca de mensagens. Os próprios grupos reconheceram pequenos erros à medida que se aproximavam do processo final, concluindo a atividade com sucesso, superando dificuldades iniciais e excedendo expectativas.

PALAVRAS-CHAVE: Aprendizagem. Criptografia. Interatividade.

INTRODUÇÃO

Em 2013, ao iniciar minha carreira como professor, deparei-me com a dificuldade, por parte dos alunos, em relacionar o conteúdo estudado com suas realidades e situações comuns do cotidiano, especialmente em matemática. Tanto no Ensino Fundamental quanto no Médio, os estudantes relatavam que a habilidade de cálculo é um pré-requisito inato. Atualmente, busco criar vínculos entre o aprendizado e situações reais, seguindo a abordagem de Freire (1996), que enfatiza a criação das condições para a produção e construção do conhecimento e não apenas a transferência de informações.

Este relato de experiência visa planejar, aplicar e relatar uma aula inédita, com foco em análise combinatória. Explorando assuntos relacionados a anagramas e mensagens criptografadas, pretende-se aproximar estudantes de realidades distintas. Duas turmas foram selecionadas: uma da terceira série do ensino médio de um colégio particular, aqui denominado Escola 1, localizado na região central de Guarulhos, e outra da segunda série do ensino médio na escola pública, aqui denominado Escola 2, na região periférica do mesmo município.

A Escola 1 foi fundada em 1974 e oferece Educação Infantil, Ensino Fundamental I e II e Ensino Médio, funcionando em dois períodos. Embora priorize valores cristãos, não exige que os alunos sejam fiéis de religiões evangélicas. A Escola 2 foi inaugurada em 1990, atende Ensino Fundamental II e Ensino Médio em três turnos e enfrenta limitações de recursos e espaços. Ambas as instituições refletem diferentes realidades sociais.

O tema da criptografia é relevante devido à presença de senhas e códigos de bloqueio em diversos dispositivos ou plataformas digitais que são utilizadas atualmente como celulares, e-mails ou redes sociais, por exemplo. Esta aula abordou, por meio de uma problematização desafiadora, a importância da criptografia de mensagens e informações digitais. Com isso, foi pretendido que o educando percebesse a relevância de elaborar senhas seguras devido à crescente democratização da internet e a necessidade de proteção de dados virtuais. A aprendizagem significativa, enfatizada por Alegro (2018), foi buscada para aproximar os alunos do conteúdo e ancorar novos saberes.

O objetivo era que os educandos reconhecessem a matemática em diversos contextos e percebessem sua importância na sociedade, pois o ensino não se resume

a fórmulas e equações mecânicas e a compreensão deve ser cultivada através da generalização e significado dos elementos matemáticos. O trabalho visou, portanto, quebrar preconceitos em relação à matemática, promovendo aprendizagem lúdica que transcende barreiras socioeconômicas e culturais.

O planejamento da aula incluiu etapas como introdução do assunto, apresentação da situação-problema, construção de um mecanismo de decodificação, discussão sobre disparidades educacionais, criação e codificação de mensagens, decodificação das mensagens recebidas e análise dos resultados. Pretendia-se que os alunos compreendessem a criptografia e sua aplicação prática, ao mesmo tempo em que ocorresse a interação entre diferentes realidades sociais.

DESCRIÇÃO DETALHADA DA EXPERIÊNCIA

O objetivo geral deste trabalho foi compreender a importância da criptografia em várias áreas do conhecimento e relacioná-la com situações cotidianas. Os objetivos específicos incluiram promover interação entre alunos de diferentes contextos econômicos por meio de mensagens criptografadas, desenvolver habilidades de resolução de problemas, interpretar informações em diferentes linguagens, compreender e aplicar a "Cifra de César"[1] para codificar e decodificar mensagens e criar uma codificação e mensagem criptografada.

As estratégias pedagógicas propostas envolvem a resolução de uma situação-problema contextualizada, abordando temas cotidianos como o uso de aplicativos, redes sociais e proteção de senhas. Os alunos receberam uma mensagem codificada que deveria ser traduzida posteriormente por eles. Antes disso, houve uma discussão introdutória sobre a criptografia.

A construção de um mecanismo baseado no código abordado foi realizada com materiais concretos para tradução e codificação de mensagens ao longo da aula. Isso permitiu que os alunos decodificassem a mensagem inicialmente apresentada. Em seguida, os jovens participaram de uma atividade que promoveu a troca de ideias entre diferentes realidades sociais. Eles elaboraram mensagens codificadas usando

[1] Em criptografia, a Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante.

anagramas ou outros meios de codificar para colegas de outra escola a fim de que estas fossem decodificadas e lidas.

Foi planejado a seguinte sequência didática:

Tabela 1. Sequência didática.

Aulas	Atividade	Tempo estimado por atividade
1ª	✓ Introdução do assunto; ✓ Apresentação da situação-problema e tentativas de solução. ✓	**15 min.** **30 min**
2ª	✓ Construção de um mecanismo para decodificação; ✓ Tradução da situação-problema; ✓ Debate: aula na escola pública x aula na escola particular;	**10 min.** **10 min** **25 min.**
3ª	✓ Elaboração de uma mensagem para os colegas da outra escola; ✓ Codificação da mensagem; ✓ Relatos sobre a experiência vivenciada.	**20 min.** **20 min.** **05 min.**
4ª	✓ Decodificação e leitura da mensagem; ✓ Outros métodos de criptografia (definir); ✓ Relatos da experiência vivenciada.	**20 min.** **15 min.** **10 min.**

Fonte: O autor (2023).

Os materiais necessários foram:

- Copos descartáveis para construção do mecanismo decodificador;
- Papel sulfite para rascunhos, decodificações, mensagens e alfabeto impresso que foi usado no decodificador;
- Fita adesiva;
- Cartolinas (cartazes com mensagens codificadas);
- Canetões coloridos;
- Recursos digitais (sala de multimídia) para introdução dos assuntos com recursos visuais;
- Giz, canetão, lousa e quadro branco para explanações.

Seguiu-se a aplicação:

A atividade foi desenvolvida por alunos das redes pública e particular de ensino de maneira concomitante. Assim, a descrição a seguir irá se referir a cada uma delas de maneira individualizada trazendo os apontamentos realizados durante o acompanhamento da tarefa. As estratégias de cada grupo foram registradas no decorrer a aplicação e não houve intervenção direta neste primeiro momento, ou seja, os grupos foram questionados quanto a suas primeiras impressões sem que mediações fossem realizadas.

Da aplicação na Escola 1:

Na Escola 1, a atividade foi dividida em cinco grupos, cada um composto por três a seis alunos, que são aqui identificados como grupo 1, grupo 2, grupo 3, grupo 4 e grupo 5.

O grupo 1, composto por três alunos que normalmente participam de forma moderada, focou na observação das terminações das palavras para identificar padrões entre vogais e consoantes. Eles rapidamente identificaram as letras "O" e "S", nas cifras "R" e "V", respectivamente, decifrando parte da mensagem para "Todos os Seus".

O grupo 2, composto por quatro alunos participativos, notou a repetição das cifras "R" e "V" e concentrou-se em trechos onde essas cifras apareciam juntas, deduzindo corretamente algumas palavras como "em" e "os". Após um tempo, eles decifraram completamente a mensagem para "Todos os seus sonhos podem se tornar realidade".

O grupo 3, formado por alunos moderadamente participativos, tentou estabelecer uma correspondência de cifras para cada letra do alfabeto, mas não conseguiu chegar a uma solução após algum tempo de tentativa.

O grupo 4, o maior com seis alunos participativos, fez uma suposição inicial de que a cifra "R" correspondia a "a" e a cifra "V" correspondia a "s", mas percebe o erro e substituiu a suposição pela cifra correta após alguns minutos. Os alunos desse grupo decifraram a mensagem corretamente após 25 minutos de atividade.

O grupo 5, composto por cinco alunos muito participativos, inicialmente teve dificuldades em definir uma abordagem, mas após uma intervenção e sugestão do professor, optaram por usar uma variação da Cifra de César. Eles decifraram a mensagem corretamente após 20 minutos, mostrando uma compreensão clara do processo.

Na etapa de elaboração e codificação de uma mensagem, os alunos do grupo 1 usaram uma variação da Cifra de César, girando os copos decodificadores para escolher aleatoriamente as letras correspondentes. A mensagem escolhida foi codificada como "WJX YNLJ J MNDB YJAJ PDRJA BNDN YJBBXB BN EXLN WJX NBCJ MRBYXBCX JVENA BNDB PNB", contendo alguns erros de transcrição.

O grupo 2 também usou uma variação da Cifra de César, com uma chave de troca de 23 posições, e codificou a mensagem escolhida como "JXP PB SLZB KXL PB XOOFPZXO, KRKZX QBOX EFPQLOFX MXOX ZLKQXO", sem erros.

O grupo 3 usou uma variação da Cifra de César e adicionou uma transposição numérica, mas enfrentou dificuldades na implementação. Os alunos codificaram a mensagem como "12 19-12-3-15-6-10-2-11-17-12 2 12 24-9-17-12 3-24-9-24-11-17-2 1-2 1-2-18-16 13-23-15-23 18-10 10-18-11-1-12 16-18-15-1-12", mas cometeram erros ao atribuir números correspondentes ao alfabeto tradicional.

O grupo 4 tentou criar algo inovador, usando símbolos além das letras do alfabeto e letras gregas, mas suas permutações aleatórias tornaram a decodificação impossível. A mensagem foi codificada de forma incorreta e não seguindo a proposta inicial.

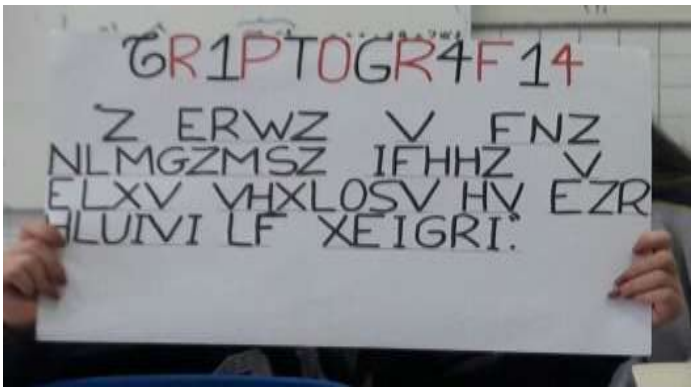
O grupo 5 utilizou um método diferente, a Cifra Hebraica, que envolve dobrar o alfabeto ao meio para criar uma substituição. Eles decifraram e codificaram a mensagem como "a vida é uma montanha russa e você escolhe se sofre ou curtir", cometendo um erro de transcrição na parte final.

Apesar de algumas dificuldades e erros, a maioria dos grupos compreendeu os conceitos de cifragem e decifragem, conseguindo decodificar a mensagem inicial e elaborar suas próprias mensagens codificadas. O envolvimento ativo dos alunos e a diversidade de abordagens refletem a eficácia do método de ensino proposto.

Figura 1. Aluno da Escola 1 durante o processo de decodificar a mensagem.

Fonte: O autor (2023).

Figura 2. Aluno da Escola 1 durante o processo de criação de mensagens criptografadas.



Fonte: O autor (2023).

Da aplicação na Escola 2:

Na continuação da aplicação da aula inédita na Escola 2, os alunos foram divididos em grupos nomeados como A, B, C, D e E. A comanda de trabalho seguiu o mesmo padrão da escola 1, apresentando as mesmas etapas desde a explanação inicial até a elaboração e codificação de uma mensagem.

Os grupos da escola 2 apresentaram reações iniciais de surpresa à tarefa, mas logo começaram a se familiarizar com o formato da aula inédita. Cada grupo, composto por diferentes perfis de alunos, demonstrou abordagens e estratégias variadas para decodificar a mensagem cifrada.

O Grupo A, composto por três meninas e um menino, teve um início mais lento devido à falta de iniciativa. Eles observaram a repetição de letras e tentaram identificar padrões nas vogais e consoantes da mensagem cifrada.

O Grupo B, formado por duas meninas e um menino, foi liderado pelo garoto, que propôs substituições aleatórias com base nas letras repetidas na cifra. Eles demonstraram organização na execução da tarefa.

O Grupo C, composto por um menino e três meninas, mostrou participação ativa e comunicação eficiente. Eles tentaram diferentes abordagens, incluindo observar palavras curtas e testar suposições sobre as combinações de duas e três letras.

O Grupo D, formado por quatro meninas e um menino, teve um início mais lento e tentou suposições aleatórias, associando a letra "W" à consoante "F". Eles não perceberam imediatamente a lógica do processo.

O Grupo E, com três meninas e um menino, focou palavras curtas, mas não considerou a repetição de letras. Após intervenções, eles começaram a realizar testes em toda a frase.

A etapa de decodificação também trouxe desafios para os grupos da escola 2. O Grupo C se destacou pela organização de ideias e participação efetiva, chegando à solução do enigma sem utilizar o decodificador. Os demais grupos precisaram de intervenção para apresentar o mecanismo facilitador.

Quando chegaram à fase de elaborar e codificar uma mensagem, os grupos da escola 2 demonstraram abordagens criativas e diversas. O Grupo A escolheu uma variação do Código de César para cifrar a frase e teve sucesso na maior parte, apesar de alguns erros na transcrição.

O Grupo B inovou com um método baseado no "Bastão de Licurgo", utilizando uma régua e papel enrolado para criar uma cifra única. A pesquisa prévia de um dos alunos influenciou a escolha desse método.

O Grupo C também inovou ao criar um sistema de codificação que substituiu vogais por números e aplicou uma variação do Código de César para consoantes. A participação ativa de todos os membros evidenciou a compreensão do conceito.

O Grupo D escolheu uma variação do Código de César para cifrar sua mensagem, mas cometeu alguns erros na transcrição de letras, demonstrando a importância da organização.

O Grupo E optou por criar anagramas das palavras para cifrar sua mensagem. Apesar de não ser um método seguro, eles entenderam a lógica por trás do processo.

A aplicação da aula inédita na escola 2 revelou diferentes abordagens e níveis de compreensão entre os grupos. Alguns grupos destacaram-se pela organização e pela compreensão profunda dos conceitos, enquanto outros apresentaram dificuldades iniciais que foram superadas com intervenções. As experiências nas Escolas 1 e 2 demonstram a diversidade de respostas e apropriações dos alunos diante de desafios de codificação e decodificação de mensagens.

Figura 3 – Aluno da Escola 2 durante o processo de decodificação da mensagem.

Fonte: O autor (2023).

Figura 4. Alunos da Escola 1 durante o processo de criação de mensagens criptografadas.

Fonte: O autor (2023).

EXPERIÊNCIA E TEORIA

Sabe-se que as escolas públicas e particulares desempenham papel importante no desenvolvimento educacional e social de um país. As escolas públicas que são financiadas pelo governo têm um compromisso fundamental com a democratização do ensino, proporcionando acesso à educação de qualidade para todos, independentemente da condição financeira. Elas refletem a diversidade e promovem a inclusão, promovendo um ambiente de aprendizagem enriquecedor (MORAN, 2021).

Nesta mesma linha de considerações, as escolas particulares oferecem uma gama variada de abordagens pedagógicas e recursos educacionais. Elas muitas vezes possuem turmas menores, o que possibilita uma atenção mais individualizada aos alunos, favorecendo um aprendizado mais personalizado. Além disso, essas escolas frequentemente investem em infraestrutura moderna e tecnologia educacional, enriquecendo a experiência de aprendizagem (MORAN, 2021).

Libâneo (1993) pontua que ambos os tipos de instituições têm profissionais altamente capacitados, dedicados a fornecer uma educação sólida e preparar os alunos para os desafios da vida. Sabe-se que o trabalho conjunto entre escolas públicas e privadas, visando a troca de experiências e a implementação das melhores práticas, é essencial para aprimorar continuamente o sistema educacional como um todo.

Assim iniciaram-se as reflexões sobre Escola 1 (pública) versus Escola 2 (particular) como parte da sequência didática. Três tópicos foram selecionados para discussão: professores, aulas e alunos. O objetivo era que os alunos expressassem suas perspectivas sobre as diferenças entre esses dois tipos de escolas, levando em consideração a visão dos próprios educandos e as intervenções do professor para enriquecer a discussão. O debate ocorreu a partir da ideia de que, apesar das realidades diferentes, o papel do aluno no seu próprio processo de aprendizado pode fazer a diferença.

A etapa final consistiu na troca e decodificação das mensagens criptografadas produzidas por cada escola. As mensagens foram trocadas entre as escolas e os grupos receberam uma mensagem para decodificar. Nenhum grupo teve acesso prévio às mensagens produzidas pela outra escola, e a escolha das mensagens foi aleatória. O decodificador foi a ferramenta principal utilizada por todos os grupos e rascunhos de alfabetos também foram utilizados durante o processo.

Os grupos demonstraram familiaridade com a situação e rapidamente começaram a fazer suposições para decodificar as mensagens. Alguns grupos decifraram suas mensagens em questão de minutos, enquanto outros levaram mais tempo. Algumas produções continham erros na transcrição, mas mesmo assim foram decodificadas. Algumas mensagens apresentaram erros propositais para avaliar a capacidade dos alunos de identificar e corrigir esses erros.

Os grupos decifraram as mensagens utilizando o decodificador e também realizaram testes com diferentes chaves. Algumas produções receberam elogios dos colegas devido ao grau de dificuldade, sistematização e criatividade. Alguns grupos levaram mais tempo para perceber os erros em suas mensagens, e intervenções foram feitas para ajudar a identificar esses erros. Em alguns casos, a lógica da codificação foi compreendida, mas as mensagens não faziam sentido até que os erros fossem corrigidos.

A tabela 2 apresenta as mensagens decifradas dentro dos primeiros dez minutos, indicando as criptografias utilizadas, a escola de origem das mensagens, os grupos que as produziram e os grupos que as decifraram.

Tabela 2. Mensagens decifradas dentro dos dez primeiros minutos.

Criptografia utilizada	Escola de origem	Grupo que produziu	Grupo que decifrou
Anagramas	2	E	3
Chave A = L (11 posições)	2	A	1
Substituição por números	1	3	2

Fonte: O autor (2023).

A tabela 3 mostra o tempo médio necessário para perceber os erros nas mensagens em diferentes criptografias.

Tabela 3. Tempo médio para percepção de erros.

Criptografia utilizada	Escola de origem	Grupo que produziu	Grupo que decifrou	Tempo médio para percepção de erros
Chave A=J (9 posições)	1	1	5	30 min.
Cifra Hebraica	1	5	A	35min.
Chave A = L (11 posições)	2	A	1	20 min.
Chave A = E (4 posições)	2	D	5	35 min.

Fonte: O autor (2023).

A tabela 4 destaca os trabalhos que receberam elogios por sua dificuldade, sistematização e criatividade.

Tabela – Trabalhos que receberam elogios.

Criptografia utilizada	Escola de origem	Grupo que produziu	Grupo que decifrou e fez os elogios
Releitura do Bastão de Licurgo	2	B	2
Letras e números	2	C	4
Cifras Hebraicas	1	5	A

Fonte: O autor (2023).

A etapa final envolveu a aplicação prática dos conceitos aprendidos, incluindo a decodificação de mensagens criptografadas, o uso de ferramentas como o decodificador e a análise da lógica por trás da codificação. Algumas produções foram mais desafiadoras do que outras, e os alunos puderam experimentar a sensação de descobrir soluções e identificar erros em suas próprias mensagens e nas dos colegas. Essa etapa final também encerrou o processo, consolidando o aprendizado obtido ao longo da sequência didática.

Dos resultados:

Após a realização da aula inédita, fico evidente a notável satisfação decorrente da aplicação das situações planejadas, nas quais os alunos alcançaram com sucesso

os objetivos preestabelecidos. A experiência foi validada pela ativa participação dos alunos, transformando-os em protagonistas no processo de ensino-aprendizagem proposto.

A participação dos alunos em ambas as escolas selecionadas para a aplicação foi geral e demonstrou entusiasmo durante o desenvolvimento das atividades, resultando em resultados significativos e até mesmo superando as expectativas iniciais. Assim, é possível concluir que os alunos, tanto na Escola 1 (particular) quanto na Escola 2 (pública), produziram materiais que serviram como indicadores de aprendizagem, promovendo a consolidação dos conceitos, competências e habilidades planejados para a aula.

O plano de aula foi apresentado utilizando recursos digitais, com uma apresentação de slides que auxiliou na introdução inicial sobre a criptografia. A primeira tarefa consistiu na decodificação de uma mensagem criptografada usando a Cifra de César. A partir de conhecimentos prévios e da identificação de padrões, os alunos foram desafiados a traduzir a mensagem. Posteriormente, os alunos elaboraram mensagens criptografadas usando anagramas para colegas de outra escola, com a premissa de criar um método de cifragem próprio ou adaptado.

As etapas foram conduzidas seguindo um roteiro prévio. A primeira situação utilizou uma imagem que relacionava senhas com situações cotidianas, considerando que a maioria dos jovens brasileiros utiliza redes sociais e celulares. Para introduzir o tema principal da aula, foi trabalhada uma imagem do aplicativo WhatsApp, que enfatizava a criptografia de ponta a ponta como forma de contextualizar a relevância do assunto para os alunos.

A criptografia foi explicada de forma sucinta, utilizando exemplos e analogias através de imagens para ilustrar o processo de cifragem. Os alunos foram então divididos em grupos para decifrar uma mensagem codificada, sem informações detalhadas sobre o método de codificação. Eles foram orientados a identificar padrões para resolver o problema.

A atividade foi realizada simultaneamente por alunos da escola pública quanto particular. As estratégias de cada grupo foram registradas durante a aplicação, sem intervenções diretas nesse primeiro momento. A seguir, serão descritas as estratégias de cada grupo, referindo-se a eles como Escola 1 (particular) e Escola 2 (pública).

Por meio da abordagem proposta, os alunos foram envolvidos ativamente no processo de aprendizagem, adquirindo habilidades de resolução de problemas,

interpretação e aplicação prática da criptografia. A interação entre alunos de diferentes contextos econômicos também promoveu uma experiência enriquecedora e uma compreensão mais profunda do tema, conectando-o à vida cotidiana dos jovens.

CONSIDERAÇÕES FINAIS

Ao término deste relato, pode-se concluir que os alunos aprendem com significado, tendo em vista que suas produções apontam para a apropriação de novos conceitos e não apenas para a compreensão de processos mecanizados.

A aplicação desta aula não se restringe à interação entre diferentes ambientes de ensino, pois pode ser aplicada, inclusive, dentro de um mesmo conjunto de alunos. As possíveis variações do processo aqui esquematizado não são restritas e ficam sob inteira autonomia do professor que desejar realizar em suas aulas situações semelhantes.

O trabalho diferenciado em sala de aula é desafiador, mas extremamente gratificante. A contextualização das aulas de matemática e a aproximação dos conteúdos ensinados com a realidade do aluno tornam as aulas mais interessantes e produtivas. O educando protagoniza o processo e se apropria do conceito estudado; ao invés de memorizar fórmulas e algoritmos, ele é capaz de fazer interações entre conhecimentos já interiorizados e as novas proposições, aprendendo de maneira significativa.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEGRO, Regina Célia. **Aprendizagem significativa.** São Paulo: Unesp, 2018.

FREIRE**,** Paulo**. Pedagogia da autonomia.** São Paulo**:** Paz e Terra, 1996.

LIBÂNEO, José Carlos. **Didática.** São Paulo: Cortez,

MORAN, José Manuel. **A educação que desejamos.** São Paulo: Papirus, 2021.