PROPOSTA DE UM JOGO EDUCACIONAL UTILIZANDO CRIPTOGRAFIA DE DADOS EM APLICAÇÕES RFID PARA ENSINO DE CONCEITOS E PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Emanuel de Franceschi Vieira[1]; Simone Regina Ceolin[2]; Rogerio Correa Turchetti[3]; Tiago Antônio Rizzetti[4]; Renato Preigschadt de Azevedo[5]

Resumo
Este artigo explora a aplicação da tecnologia de Identificação por Radiofrequência (RFID) através de uma abordagem lúdica e interativa para o ensino de criptografia de dados e tecnologias emergentes no contexto da Educação Profissional e Tecnológica (EPT). Propõe-se a utilização de um jogo educacional como ferramenta pedagógica para facilitar a compreensão e aplicação dos conceitos fundamentais de criptografia e segurança em RFID. O jogo simula a troca segura de mensagens, onde os jogadores devem realizar autenticação de dispositivos, estabelecer conexões seguras e aplicar diferentes algoritmos para garantir a integridade, confidencialidade e autenticidade dos dados transmitidos. Espera-se que o jogo possa reforçar o aprendizado técnico e promover habilidades de pensamento crítico e resolução de problemas.
Palavras-chave: Criptografia de dados; educação profissional e tecnológica; jogo educacional; segurança da informação**.**

Abstract
This paper explores the application of Radio Frequency Identification (RFID) technology through a playful and interactive approach for teaching data encryption and emerging technologies in the context of Vocational and Technical Education (VTE). An educational game is proposed as a pedagogical tool to facilitate the understanding and application of fundamental concepts of encryption and security in RFID. The game simulates the secure exchange of messages, where players must authenticate devices, establish secure connections, and apply different algorithms to ensure the integrity, confidentiality, and authenticity of transmitted data. It is expected that the game can reinforce technical learning and promote critical thinking and problem-solving skills.
Keywords: Data encryption; educational game; information security; vocational and technical education**.**

1 Introdução

A rápida evolução da tecnologia de informação tem impulsionado transformações significativas em diversos campos, incluindo a educação. Em particular, a Educação Profissional e Tecnológica (EPT) enfrenta o desafio de integrar tecnologias emergentes em

[1] Tecnólogo em Redes de Computadores pela Universidade Federal de Santa Maria-UFSM. E-mail: emanuel.franceschi@acad.ufsm.br.
[2] Doutora em Ciência da Computação pela Universidade de York/Reino Unido, professora Associada do Colégio Técnico Industrial da Universidade Federal de Santa Maria (CTISM-UFSM). E-mail: sceolin@redes.ufsm.br.
[3] Doutor em Informática pela Universidade Federal do Paraná-UFPR, professor associado da Universidade Federal de Santa Maria-UFSM. E-mail: turchetti@redes.ufsm.br.
[4] Doutor em engenharia elétrica pela Universidade Federal de Santa Maria-UFSM, professor da Universidade Federal de Santa Maria-UFSM. E-mail: rizzetti@ctism.ufsm.br.
[5] Doutor em Informática pela Universidade do Minho/Portugal, professor adjunto da Universidade Federal de Santa Maria-UFSM. E-mail: renato@redes.ufsm.br

currículos que preparem os alunos de maneira eficaz para as demandas do mercado de trabalho. Um exemplo desse tipo de tecnologia é a identificação automatizada que, nos últimos anos, ganhou grande popularidade em diversos setores (Santana, 2023).

Um exemplo de tecnologia de identificação automatizada é a Identificação por Rádio Frequência (RFID). Os incentivos para a adoção desta tecnologia surgem a partir da ampla possibilidade de automatizar tarefas manuais, como a gestão de estoque em empresas (Fonseca; Ferreira, 2022), controle de acesso (Silva e Schluter, 2023), e até mesmo procedimentos na área da saúde (Mehta *et al*., 2020). Esses usos variados demonstram a versatilidade e a eficácia do RFID em otimizar processos e aumentar a eficiência operacional em diferentes setores.

Este estudo propõe a criação de um jogo educacional como ferramenta para o ensino de conceitos de segurança da informação, com foco na tecnologia RFID e na criptografia de dados. O jogo, ao utilizar uma metodologia lúdica, visa não apenas engajar os alunos, mas também facilitar a compreensão e aplicação prática desses conceitos em um ambiente interativo. A expectativa é que essa abordagem promova um aprendizado mais profundo e prepare os alunos para enfrentar desafios reais, simulando a troca segura de mensagens e a autenticação de dispositivos em um cenário controlado.

A escolha de utilizar um jogo educacional como ferramenta de ensino se justifica pela motivação e pelo engajamento oferecido por essa abordagem. Estudos mostram que métodos de aprendizagem lúdicos podem aumentar significativamente o interesse e a construção de conhecimento por parte dos alunos. No contexto da EPT, onde a aplicabilidade prática das tecnologias estudadas é fundamental, um jogo que simula a utilização do RFID e a criptografia de dados permite que os alunos experimentem situações reais de forma segura e controlada.

Este artigo está organizado da seguinte maneira: na Seção 2, é apresentado o Referencial Teórico, onde são discutidos os conceitos fundamentais de RFID, criptografia de dados, e metodologias de ensino lúdicas. Na Seção 3, a Metodologia detalha o processo de planejamento e desenvolvimento do jogo, abordando as principais etapas para sua implementação. A Seção 4, Proposta de jogo, é apresentada a estrutura do jogo e os conceitos que serão aplicados. Na Seção 5, Discussão, são exploradas as expectativas e possíveis impactos educacionais do jogo proposto. Por fim, na Seção 6, são discutidas as considerações finais e sugestões para trabalhos futuros.

2 Referencial teórico

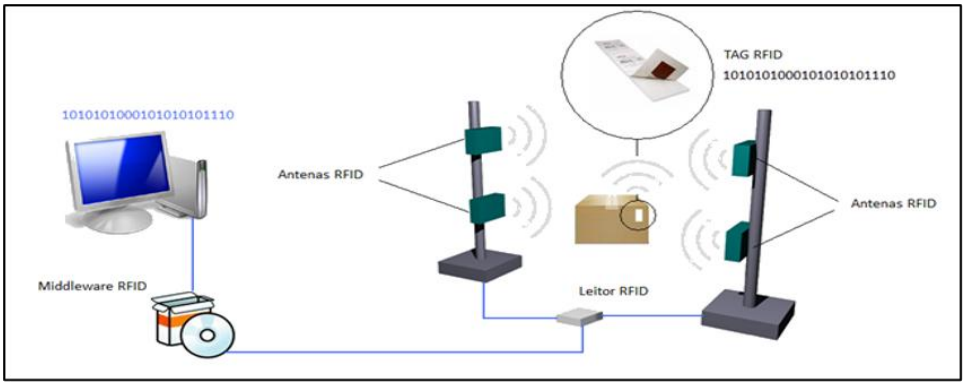
Nesta seção, será apresentada uma revisão bibliográfica detalhada, abordando os principais conceitos e estudos relacionados ao tema do trabalho. O objetivo é fornecer um

embasamento teórico que permita compreender o contexto e oferecer uma visão abrangente sobre a tecnologia RFID, explorando os componentes de um sistema RFID, suas principais características, funcionalidades e aplicações. Além disso, serão apresentados os conceitos e estudos relacionados às metodologias de ensino lúdicas e à aplicação de jogos em ambientes educacionais.

2.1 Identificação por Rádio Frequência

Segundo Pinheiro (2017), a Identificação por Radiofrequência (RFID) é uma tecnologia de identificação automatizada que utiliza ondas de rádio para transferir dados entre um dispositivo leitor e uma etiqueta eletrônica, também conhecida como tag RFID. Essa tecnologia permite a leitura de dados sem a necessidade de contato físico ou linha de visão direta entre o leitor e a tag, o que a torna extremamente eficiente em diversas aplicações. A tecnologia RFID é composta por três componentes principais: tags (etiquetas), leitores e o middleware. Cada um desses componentes desempenha um papel essencial no funcionamento de um sistema que busca obter as informações contidas em uma etiqueta (Narciso, 2008). A Figura 1 ilustra um exemplo de comunicação utilizando a tecnologia RFID.

Figura 1 - Configuração RFID



Fonte: Retirado de https://www.roisoft.com/solucoes/roi-midware.

As tags RFID são dispositivos que armazenam dados específicos e consistem em um microchip acoplado a uma antena. Elas podem ser classificadas em três tipos: passivas, ativas e semi-passivas. Tags passivas não possuem fonte de energia própria e dependem da energia do leitor para funcionar, tornando-as mais baratas e duráveis. Tags ativas possuem uma fonte de energia própria, o que permite um maior alcance de leitura e maior capacidade de armazenamento de dados. As tags semi-passivas oferecem um equilíbrio entre custo e desempenho, pois também possuem uma bateria, mas operam como etiquetas passivas, transmitindo dados somente quando acionadas por um leitor (Musci *et al*., 2023). O leitor de RFID, que é equipado com uma antena, é o dispositivo responsável por emitir ondas de rádio e receber os sinais retornados pelas tags.

O leitor recebe e converte as ondas de rádio em dados digitais, que são repassados para o middleware. Esses leitores podem ser fixos ou móveis, dependendo das necessidades específicas da aplicação. Geralmente, leitores fixos são montados em paredes ou outros objetos e permanecem em um determinado local, enquanto os leitores móveis podem ser transportados para onde forem necessários (Musci *et al*., 2023).

O middleware RFID é o software que processa e interpreta os dados capturados pelos leitores. Ele atua como um intermediário entre os leitores e os sistemas de gestão da informação. O middleware integra os dados capturados aos sistemas de gestão, permitindo uma análise e tomadas de decisões (Haibi *et al*., 2023).

De acordo com Maulana, Aisyah e Wikanta (2023), a Identificação por Rádio Frequência possui diversas características e funcionalidades que a tornam extremamente eficiente em várias aplicações. Uma das principais vantagens da tecnologia RFID é a capacidade de leitura à distância. As tags RFID podem ser lidas a vários metros de distância, dependendo da frequência e potência do leitor, sem a necessidade de contato físico direto, o que permite uma maior flexibilidade e eficiência na coleta de dados. Além disso, as tags RFID podem armazenar uma quantidade significativa de dados, incluindo informações específicas sobre o objeto ao qual estão anexadas, facilitando a gestão e o rastreamento de itens em tempo real.

As tags RFID também são projetadas para suportar condições ambientais adversas, como umidade, calor e impacto físico. Outra característica importante é a capacidade de leitura simultânea de várias tags, o que facilita a verificação rápida de grandes volumes de itens, tornando o processo de inventário e rastreamento mais eficiente.

Devido à sua eficiência e versatilidade, a tecnologia RFID possui aplicações em diversos setores. Na logística e cadeia de suprimentos, a RFID é utilizada para rastreamento de produtos e otimização de processos logísticos. No setor de saúde, a tecnologia é aplicada para controle de equipamentos médicos, rastreamento de pacientes e gestão de medicamentos. Em termos de segurança, a RFID pode ser empregada de diversas formas, como por exemplo, em sistemas de controle de acesso. No varejo, a tecnologia auxilia na gestão de estoque e prevenção de perdas. No setor de transporte, a RFID é utilizada para rastreamento de veículos, gestão de frotas e controle de acesso em portos e aeroportos.

2.2 Segurança da informação

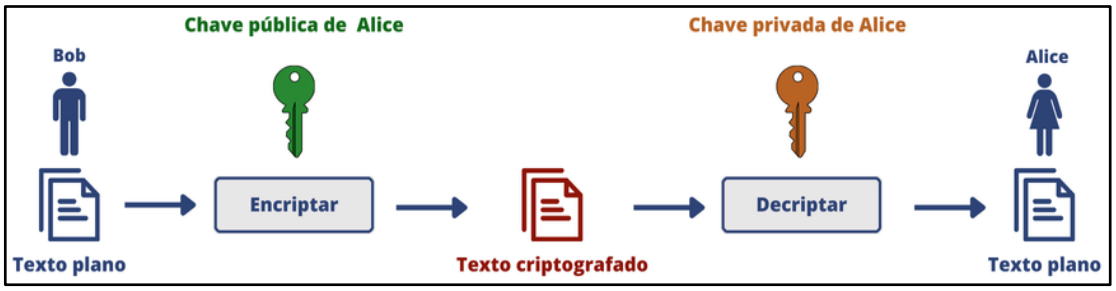
A segurança da informação é fundamental para proteger dados contra ameaças como acesso não autorizado, manipulação e perda. Implementar técnicas robustas de segurança é fundamental em diversos contextos, especialmente na transmissão de dados sensíveis, a fim de

assegurar a integridade, confidencialidade e autenticidade das informações (Stallings; Brown, 2015).

Uma das principais técnicas de segurança da informação é a criptografia, que envolve a conversão de dados em um formato codificado, tornando-os inacessíveis para usuários não autorizados (Paar; Pelzl, 2010). Existem dois tipos principais de criptografia: a criptografia simétrica e a criptografia assimétrica. A criptografia simétrica, ilustrada na Figura 2, utiliza a mesma chave para cifrar e decifrar a informação, o que requer que ambas as partes envolvidas na comunicação tenham acesso à chave secreta. Alguns dos algoritmos mais conhecidos de criptografia simétrica incluem o AES (Advanced Encryption Standard) e o DES (Data Encryption Standard).

Por outro lado, a criptografia assimétrica utiliza um par de chaves, uma pública e uma privada. A chave pública é usada para cifrar a informação, enquanto a chave privada correspondente é usada para decifrá-la. Este método é amplamente utilizado em protocolos de segurança como o SSL/TLS (Secure Sockets Layer/Transport Layer Security), que garantem comunicações seguras na internet. Um exemplo de algoritmos de criptografia assimétrica é o RSA (Rivest-Shamir-Adleman). A Figura 3 ilustra o funcionamento da criptografia assimétrica

Figura 2 - Funcionamento da criptografia simétrica



Fonte: Autoria própria.

Figura 3 - Funcionamento da criptografia assimétrica

Fonte: Autoria própria.

No contexto da Identificação por Rádio Frequência (RFID), a criptografia desempenha um papel essencial na proteção dos dados transmitidos entre as etiquetas RFID (tags) e os leitores, uma vez que a criptografia é um processo de tornar a informação ininteligível para uma

pessoa não autorizada, proporcionando assim confidencialidade aos utilizadores genuínos (Patil *et al*., 2016). A segurança da informação em sistemas RFID pode ser comprometida por diversos tipos de ataques, como clonagem de tags, eavesdropping, snooping, dentre outros. Portanto, a implementação de algoritmos de criptografia robustos é essencial para reduzir esses riscos (Khattab *et al*., 2017).

Além da criptografia, outros mecanismos de segurança são igualmente importantes, como a autenticação e a integridade dos dados. A autenticação é um processo fundamental que verifica a identidade dos dispositivos antes de permitir a troca de informações, isso garante que a comunicação ocorra entre dispositivos confiáveis. Métodos comuns de autenticação incluem senhas, biometria e tokens de segurança (Mostafa *et al*., 2023). A integridade dos dados assegura que a informação não foi alterada durante a transmissão ou armazenamento. Técnicas como funções hash e assinaturas digitais são utilizadas para verificar a integridade dos dados, garantindo que a informação recebida é exatamente a mesma que foi enviada (Kaur; Kaur, 2012).

2.3 Método de ensino

Ao longo da história, o modelo de formação de profissionais da educação tem seguido metodologias tradicionais de ensino-aprendizagem. De acordo com Freire (1996) este modelo é descrito como "bancário", pois envolve apenas a transmissão de conhecimento do professor para o aluno. Este método tem se mostrado insuficiente para atender às variadas necessidades dos indivíduos e para a formação adequada dos profissionais.

Nesse contexto, as Metodologias Ativas de Aprendizagem, como a Problematização e a Aprendizagem Baseada em Problemas (ABP), têm ganhado destaque. Na ABP, grupos de alunos discutem problemas apresentados pelo docente, com base nos temas descritos na grade curricular, proporcionando a integração das disciplinas (Cyrino; Toralles-Pereira, 2004). Esse método tem raízes na Teoria da Indagação de John Dewey, que defendia a aprendizagem através de desafios e problemas que provocam dúvidas e incentivam a descoberta e a reflexão (López *et al*., 2020).

Além da ABP, a aprendizagem baseada em jogos e brincadeiras tem se mostrado eficaz no desenvolvimento de habilidades sociais, emocionais e cognitivas dos alunos (Pinto *et al*., 2021). Os jogos didáticos simplificam e tornam mais atrativos os conteúdos trabalhados em sala de aula, ajudando a atingir objetivos pedagógicos (Canto *et al*., 2021). Transformar o aprendizado em uma tarefa lúdica é um dos grandes desafios dos professores, exigindo

criatividade e ferramentas que atendam às necessidades pedagógicas e atraiam o interesse dos alunos (Santos *et al*., 2020).

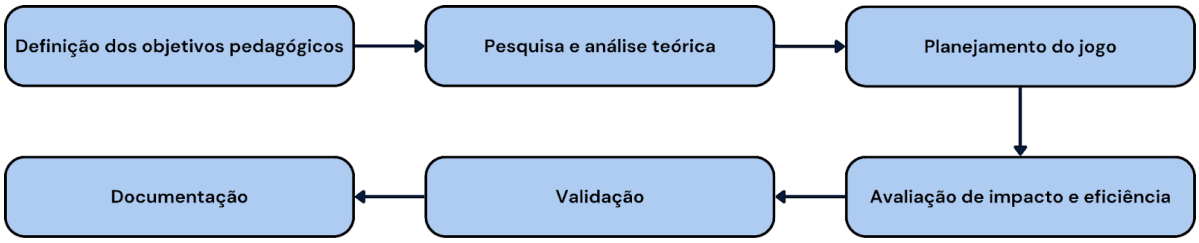
Nesse contexto, o conceito de gamificação surge como uma abordagem inovadora que aplica a mecânica e a estética dos jogos em contextos educacionais para engajar os alunos, motivar ações e promover a aprendizagem. Segundo, Kapp (2012), um jogo é um sistema em que os jogadores enfrentam desafios abstratos definidos por regras, interatividade e feedbacks, resultando em um desfecho quantificável que muitas vezes provoca reações emocionais. Essa abordagem cria um ambiente de aprendizagem que é tanto estimulante quanto educativo, tornando o processo de aquisição de conhecimento mais eficiente e agradável.

O uso de jogos como ferramentas educacionais preenche lacunas deixadas pelo ensino tradicional, promovendo a socialização e a construção de novos conhecimentos (Ferreira *et al*., 2020). A aplicação de jogos didáticos requer planejamento cuidadoso, com a delimitação de temas e a seleção de recursos e materiais apropriados. O professor deve esclarecer os objetivos educacionais do jogo, planejar as etapas, prever momentos de trabalho em grupo, duplas e individual, estabelecer critérios de avaliação e registrar a participação dos alunos ao longo da atividade.

3 Metodologia

Em um jogo educacional que visa auxiliar no ensino de práticas de segurança da informação em RFID, é fundamental que os alunos compreendam e apliquem esses conceitos para proteger as informações transmitidas. O jogo proposto neste trabalho utilizará uma abordagem lúdica e interativa para ensinar os conceitos de criptografia de dados, autenticação e integridade dos dados em RFID. Os jogadores serão desafiados a realizar autenticação de dispositivos, estabelecer conexões seguras e aplicar diferentes algoritmos de criptografia para garantir a integridade e confiabilidade dos dados transmitidos. A metodologia desempenha um papel fundamental na realização deste trabalho, fornecendo a estrutura necessária para alcançar os objetivos propostos e, através dela, espera-se que os alunos desenvolvam um entendimento profundo das práticas de segurança da informação e sejam capazes de aplicá-las em contextos reais. A Figura 4 apresenta o fluxograma da metodologia proposta para o desenvolvimento e aplicação do jogo.

Figura 4 - Metodologia empregada



Fonte: Autoria própria, 2024.

De início, é essencial determinar o que os alunos devem aprender com o jogo proposto. A definição dos objetivos pedagógicos envolve a análise das necessidades educacionais dos estudantes e a identificação de como os princípios da criptografia e da tecnologia RFID podem ser integrados ao currículo de maneira eficaz. Os objetivos devem estar alinhados com as competências desejadas, a fim de garantir que o aprendizado seja relevante e aplicável (Silva e Schluter, 2023).

Na etapa de pesquisa e análise teórica, será realizada uma revisão da literatura sobre criptografia, segurança da informação e jogos educacionais, com ênfase especial nos jogos que utilizam RFID ou tecnologias relacionadas. Além disso, busca-se compreender como essas ideias podem aumentar a motivação dos alunos e a absorção do conhecimento. A comparação com jogos atuais fornece informações sobre características de design bem-sucedidas e possíveis dificuldades a serem evitadas.

O próximo passo é o planejamento do jogo. O desenvolvimento da estrutura do jogo, a definição das mecânicas e a criação de cenários que simulam os reais desafios da implementação da criptografia em RFID são os principais componentes desta fase. Para garantir que cada componente contribua para os objetivos de aprendizagem, são tomadas decisões sobre como o jogo deve ser conduzido, quais desafios serão enfrentados, quais tipos de interações podem ocorrer e quais feedbacks serão apresentados ao jogador.

Para compreender se o jogo é eficaz como ferramenta educacional, é necessário avaliar seu impacto considerando múltiplas perspectivas, como as bases cognitivas e motivacionais (Plass; Homer; Kinzer, 2015). Será desenvolvido um plano de avaliação detalhado, que incluirá métodos para medir a aquisição de conhecimento, o desenvolvimento de habilidades e a interação dos alunos com o jogo. A avaliação pode ser quantitativa, medindo os resultados de aprendizagem após o uso do jogo, ou qualitativa, fornecendo informações para possíveis melhorias no jogo.

A fase de validação é essencial para garantir a eficácia e a relevância do jogo proposto como uma ferramenta educacional. Para isso, serão conduzidos testes piloto com grupos de estudantes que representam o público-alvo, permitindo a coleta de dados qualitativos e

quantitativos sobre a experiência de uso do jogo. Os feedbacks dos alunos serão obtidos por meio de questionários, com o objetivo de compreender o nível de aprendizagem e a usabilidade do jogo. Essa etapa também envolve a análise dos resultados obtidos para identificar padrões e verificar se os objetivos pedagógicos serão alcançados. As informações coletadas durante a validação serão fundamentais para realizar ajustes e melhorias no jogo proposto.

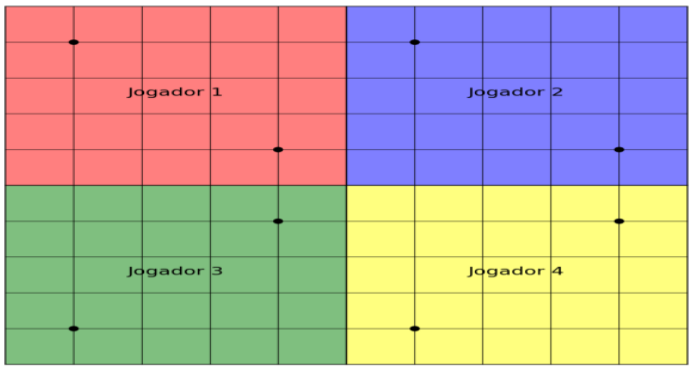
Por fim, na fase de documentação, é necessário juntar e apresentar todos os pontos importantes observados durante o desenvolvimento do jogo em um formato acessível e informativo. A descrição detalhada do jogo, os fundamentos teóricos, as técnicas de aplicação e de avaliação, e os resultados dos testes serão todos incluídos na documentação. Isso servirá como um registro do processo de criação do jogo e servirá também como um recurso para educadores que estão interessados em desenvolver estratégias semelhantes.

4 Proposta de jogo

A proposta deste jogo educacional é criar um ambiente lúdico e interativo que simula a comunicação segura em um cenário que utiliza a tecnologia de Identificação por Rádio Frequência (RFID), utilizando peças que representam diferentes elementos da comunicação, além de cartas que representam diferentes protocolos de segurança. O principal objetivo do jogo é permitir que os jogadores apliquem conceitos de criptografia e segurança da informação, como a integridade, confidencialidade e autenticidade dos dados transmitidos entre duas ou mais partes. Os jogadores devem utilizar peças e cartas para estabelecer conexões seguras e proteger os dados contra ameaças.

O jogo é composto por um tabuleiro, ilustrado na Figura 5, que representa a rede de comunicação com diferentes caminhos e pontos de conexão. As peças incluem representações de leitores RFID, tags RFID e middlewares. Além disso, há peças que representam chaves de criptografia (simétricas e assimétricas), cartas que representam protocolos que fornecem instruções para garantir a segurança da comunicação, cartas de ameaça que simulam possíveis ataques à comunicação, e peças de mensagem que representam os dados que precisam ser transmitidos de um ponto a outro. Esses elementos permitem que os jogadores pratiquem a configuração e a proteção de uma rede de comunicação RFID, aplicando protocolos de segurança e estratégias de criptografia para defender contra ameaças.

Figura 5 - Tabuleiro proposto



Fonte: Autoria própria.

Cada partida pode ser jogada por 2 a 4 pessoas. No início, cada jogador recebe três peças de dispositivos, que representam os principais componentes de um sistema RFID: o *middleware* (um *software* responsável por gerenciar e interpretar os dados do sistema), a tag (uma pequena etiqueta eletrônica que armazena informações), e o leitor RFID (o dispositivo que lê as informações da *tag*). Além dessas peças, cada jogador recebe representações de chaves de criptografia, que são usadas para proteger as informações trocadas durante o jogo. Essas chaves incluem uma chave simétrica (que utiliza a mesma chave para codificar e decodificar informações) e um par de chaves assimétricas, composto por uma chave pública e uma chave privada (onde uma é usada para encriptar e a outra para decriptar as informações).

O tabuleiro é colocado no centro da mesa e os jogadores têm um tempo limite de três minutos para posicionar e organizar suas peças, criando a rede de comunicação inicial. A definição desse tempo visa manter o ritmo do jogo, essencial para garantir que a experiência dos jogadores seja contínua e dinâmica, conforme discutido no estudo de Salen e Zimmerman (2004). O jogo é dividido em turnos e, em cada turno, os jogadores podem realizar apenas uma das ações: (i) mover uma peça de dispositivo para estabelecer as novas conexões; (ii) trocar as peças-chave para criptografia de dados; (iii) utilizar uma carta de protocolo para implementar uma medida de segurança; (iv) jogar uma carta de ameaça para tentar interceptar ou comprometer a comunicação dos adversários e (v) tentar transmitir uma mensagem.

Para transmitir uma mensagem, o jogador deve garantir que a mesma siga um caminho seguro no tabuleiro, utilizando as chaves e protocolos apropriados. A comunicação segura é alcançada através da aplicação correta dos protocolos representados pelas cartas, que fornecem instruções específicas para criptografar os dados. Por exemplo, uma carta de protocolo pode instruir o jogador a "Estabelecer uma conexão segura utilizando criptografia assimétrica".

Os jogadores ganham pontos ao transmitir mensagens com sucesso e pela utilização eficaz dos protocolos de segurança. Transmitir uma mensagem com sucesso concede 3 pontos.

No entanto, caso o jogador tente transmitir uma mensagem e falhar, perde 1 ponto. Ataques também contabilizam pontos: se o atacante tiver sucesso, ele ganhará 2 pontos, mas se o ataque falhar, o atacante perderá 1 ponto. Se um jogador for atacado com sucesso, ele perderá 2 pontos, mas se o ataque falhar, o jogador que sofreu a tentativa de ataque ganhará 1 ponto. O primeiro jogador a alcançar 10 pontos vence o jogo.

Ao final de cada partida, os jogadores podem discutir as estratégias utilizadas, os desafios enfrentados e as lições aprendidas, promovendo uma reflexão sobre a aplicação dos conceitos de segurança da informação. Dessa forma, o jogo não apenas reforça o aprendizado técnico, mas também desenvolve habilidades de pensamento crítico e resolução de problemas, essenciais para profissionais que lidam com tecnologias emergentes.

5 Discussão

Espera-se que a proposta de implementar o jogo apresentado neste artigo, que simula a comunicação segura utilizando tecnologia RFID, permita que os alunos visualizem e pratiquem a aplicação de protocolos de segurança em um ambiente controlado e interativo. Através da ludicidade, os alunos poderão experimentar e entender melhor os desafios e as estratégias necessárias para proteger dados e garantir a integridade, confidencialidade e autenticidade da informação transmitida.

Avaliar o jogo de forma qualitativa e quantitativa será essencial para compreender seu impacto educacional. As avaliações qualitativas, através de feedbacks dos alunos, podem revelar como o jogo influencia a motivação e o engajamento no aprendizado. Já as avaliações quantitativas podem medir a aquisição de conhecimento e habilidades antes e depois da utilização do jogo, permitindo uma análise mais precisa de sua eficácia. Assim, espera-se que o jogo não apenas reforce o aprendizado teórico, mas também desenvolva habilidades práticas e de resolução de problemas, que são cruciais para os profissionais que lidam com tecnologias emergentes.

6 Considerações finais

Este estudo apresentou a proposta de um jogo educacional lúdico para o ensino de criptografia de dados e segurança da informação em um cenário que utiliza a tecnologia RFID. Através da simulação de comunicação segura, os jogadores serão incentivados a aplicar conceitos teóricos em um contexto prático, o que pode promover um aprendizado mais significativo e duradouro. É possível que a utilização de métodos de ensino lúdico, como o jogo

proposto, possa aumentar a motivação dos alunos e facilitar a compreensão de tópicos complexos.

Pesquisas futuras podem explorar a implementação do jogo em diferentes contextos educacionais e com públicos diversos, além de investigar outras metodologias de avaliação de seu impacto. Adicionalmente, a adaptação do jogo para outras tecnologias emergentes pode ampliar seu alcance e relevância no ensino de segurança da informação.

Agradecimentos

O presente trabalho foi realizado com apoio da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

Referências

ALMEIDA, F. S.; OLIVEIRA, P. B. de; REIS, D. A. A importância dos jogos didáticos no processo de ensino aprendizagem: Revisão integrativa. **Research, Society and Development**, v. 10, n. 4, p. e41210414309–e41210414309, abr. 2021. Disponível em:https://rsdjournal.org/index.php/rsd/article/download/14309/12833/186858. Acesso em: 27 fev. 2025.

CANTO, C. G. S.; NUNES, P. O. C.; RODRIGUES, A. C. S. O lúdico como ferramenta de aprendizagem de leitura e escrita. **Revista eletrônica pesquiseduca**, v. 13, n. 29, p. 284–299, mar, 2021. Disponível em:https://periodicos.unisantos.br/pesquiseduca/article/view/1023. Acesso em: 27 fev. 2025.

CYRINO, E. G.; TORALLES-PEREIRA, M. L. Trabalhando com estratégias de ensino-aprendizado por descoberta na área da saúde: a problematização e a aprendizagem baseada em problemas. **Cadernos de saúde pública, SciELO Public Health**, v. 20, n. 3, p. 780–788, jun. 2004. Disponível em:https://www.scielo.br/j/csp/a/mrrzr85SM93thZzwGFBm56q/. Acesso em: 27 fev. 2025.

FERREIRA, S. M.; NASCIMENTO, C.; PITTA, A. P. Jogos didáticos como estratégia para construção do conhecimento: uma experiência com o 6° ano do ensino fundamental. **Giramundo: Revista de Geografia do Colégio Pedro II**, v. 5, n. 9, p. 87–94, jul. 2020. Disponível em:https://portalespiral.cp2.g12.br/index.php/GIRAMUNDO/article/view/2690. Acesso em: 27 fev. 2025.

FONSECA, L. S.; FERREIRA, J. V. M. Utilização de RFID para controle de áreas industriais. **Universidade de Taubaté**, 2021. Disponível em: http://repositorio.unitau.br/jspui/bitstream/20.500.11874/6033/1/Joao%20Vitor%20Ferreira%20Moraes%20-%20Lucas%20dos%20Santos%20Fonseca.pdf. Acesso em: 12 ago. 2024.

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

HAIBI, A. *et al*. A new RFID middleware architecture based on a hybrid security technique using data encryption and RBAC for modern real-time tracking applications. ***Frontiers in***

Mechanical Engineering., v. 9, out. 2023. Disponível em: https://www.frontiersin.org/articles/10.3389/fmech.2023.1242612/pdf. Acesso em: 27 fev. 2025.

KAPP, K. M. **The gamification of learning and instruction:** game-based methods and strategies for training and education. [S.l.], John Wiley & Sons, 2012.

KAUR, R.; KAUR, A. Digital signature. **2012 International Conference on Computing Sciences**. [S.l.: s.n.], p. 295–301, set. 2012. Disponível em: https://ieeexplore.ieee.org/abstract/document/6391693. Acesso em: 27 fev. 2025.
KHATTAB, A. *et al*. **Rfid security threats and basic solutions**. A Lightweight Paradigm: Springer International Publishing, 2017.

LÓPEZ, P. V. S. *et al*. Metodologías activas en la formación inicial de docentes: Aprendizaje basado en proyectos (abp) y educación artística. **Profesorado: Revista de Curriculum y Formación del Profesorado, Universidad de Granada**, Granada, v. 6, 2020. Disponível em:https://digibug.ugr.es/handle/10481/63803. Acesso em: 27 fev. 2025.

MAULANA, A.; AISYAH, S.; WIKANTA, P. Web-based item tracking system using RFID. **Jurnal Rekayasa Elektrika**, Banda Aceh/Indonesia, v. 19, n. 3, set. 2023. Disponível em:https://jurnal.usk.ac.id/JRE/article/view/27050. Acesso em: 27 fev. 2025.

MEHTA, S. *et al*. Mitigating staff risk in the workplace: the use of RFID technology during a COVID-19 pandemic and beyond. **BMJ Health Care Inform**, Bethesda/Maryland, v. 27, n. 3, nov. 2020. Disponível em:https://pmc.ncbi.nlm.nih.gov/articles/PMC7667999/. Acesso em: 27 fev. 2025.

MUSCI, M. *et al*. Automação em portos: uso da tecnologia RFID, **Revista Contemporânea**, v. 3, n. 12, p. 26183-26203, dec. 2023. Disponível em:https://ojs.revistacontemporanea.com/ojs/index.php/home/article/download/2549/1793. Acesso em: 27 fev. 2025.

NARCISO, M. G. Aplicação da tecnologia de identificação por radiofreqüência (RFID) para controle de bens patrimoniais pela web. **Global Science and Technology**, v. 1, n. 7, p. 50-59, dez./mar. 2008.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital**, v. 31, p. 11–15, mar. 2012. Disponível em:https://ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf. Acesso em: 27 fev. 2025.

PAAR, C.; PELZL, J. **Understanding cryptography**. [S.l.]: Springer, 2010.

PATIL, P. *et al*. A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. **Procedia Computer Science**, **Elsevier**, v. 78, p. 617–624, abr. 2016. Disponível em:https://www.sciencedirect.com/science/article/pii/S1877050916001101. Acesso em: 27 fev. 2025.

PINHEIRO, J. M. S. Identificação por Radiofreqüência: Aplicações e Vulnerabilidades da Tecnologia RFID. **Cadernos UniFOA** , Volta Redonda, v. 1, n. 2, p. 18-32, mar. 2017.

Disponível em:http://revistas.unifoa.edu.br/cadernos/article/view/889. Acesso em: 27 fev. 2025.

PINTO, L. Q. *et al*. Descobrindo os elementos: a elaboração de jogos didáticos como alternativa de ensino. **Brazilian Journal of Development**, v. 7, n. 1, p. 2247–2253, jan. 2021. Disponível em:https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/22795. Acesso em: 27 fev. 2025.

PLASS, J. L.; HOMER, B. D.; KINZER, C. K. Foundations of game-based learning. **Educational psychologist**, v. 50, n. 4, p. 258–283, fev. 2015. Disponível em:https://www.tandfonline.com/doi/abs/10.1080/00461520.2015.1122533. Acesso em: 27 fev. 2025.

SALEN, K.; ZIMMERMAN, E. **Rules of Play: Game Design Fundamentals**. [s.l.] Cambridge, Mass. The Mit Press, 2004.

SANTANA, T. A. **Implementação da integração PNRD e iPNRD para mundo de blocos**. 2023. 58 f. Trabalho de Conclusão de Curso (Graduação) - Faculdade de Engenharia Mecânica, Universidade Federal de Uberlândia, Uberlândia, 2023. Disponível em:https://repositorio.ufu.br/handle/123456789/39748. Acesso em: 27 fev. 2025.

SANTOS, A. C.; SANTOS, J. O.; ARAUJO, M. J. B. Lúdico como ferramenta da psicopedagogia no desenvolvimento integral das crianças. **Educte: Revista Científica do IFAl,** v. 10, n. 1, p. 1175-1183, nov. 2020. Disponível em:https://periodicos.ifal.edu.br/educte/article/download/1648/1228. Acesso em: 27 fev. 2025.

SILVA, D. S.; SCHLUTER, M. R. Impacto da tecnologia RFID na gestão de estoques em uma empresa alimentícia. In: **XIV FATECLOG** – Logística e Sociedade: Presença Feminina, Diversidade, Inclusão Social e Sustentabilidade, 2023, Americana. Anais [...]. Americana: FATEC Americana, 2023. ISSN 2357-9684. Disponível em:https://ric.cps.sp.gov.br/handle/123456789/15030. Acesso em: 27 fev. 2025.

SILVA, G. B. Taxonomia de bloom: Uma revisão literária das adaptações e dos instrumentos para definir objetivos instrucionais. **Revista Amor Mundi**, Santo Ângelo-RS. v. 4, n. 12, p. 3-13, dez. 2023. Disponível em:https://scholar.archive.org/work/cbgalunp7neflpj7qxfvq6y7rm/access/wayback/https://journal.editorametrics.com.br/index.php/amormundi/article/download/262/315. Acesso em: 27 fev. 2025.

STALLINGS, W.; BROWN, L. **Computer security: principles and practice**. [S.l.]: Pearson, 2015.