INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS TERESINA CENTRAL
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

DANIEL VITOR BARROSO RODRIGUES NUNES

TOKENSENTINEL: aplicando tokenização baseada em contexto dinâmico usando geolocalização em gateways de pagamento

TERESINA, PIAUÍ
2025

DANIEL VITOR BARROSO RODRIGUES NUNES

TOKENSENTINEL: APLICANDO TOKENIZAÇÃO BASEADA EM CONTEXTO DINÂMICO USANDO GEOLOCALIZAÇÃO EM GATEWAYS DE PAGAMENTO

Trabalho de Conclusão de Curso (monografia) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Central.

Orientadora: Profa. M.a. Cláutenis Carvalho Viana

TERESINA, PIAUÍ
2025

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

Nunes, Daniel Vitor Barroso Rodrigues

N972t TokenSentinel: aplicando tokenização baseada em contexto dinâmico usando geolocalização em gateways de pagamento / Daniel Vitor Barroso Rodrigues Nunes. – 2025.

52 f. : il. color.

Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) – Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Central, 2025.

Orientador: Prof. Me. Cláutenis Carvalho Viana.

1. Autenticação. 2. Tokenização. 3. Microserviço. 4. Segurança. I. Título.

CDD – 004.21

Elaborado por Tanize Maria Sales CRB 3/1024

DANIEL VITOR BARROSO RODRIGUES NUNES

TOKENSENTINEL: APLICANDO TOKENIZAÇÃO BASEADA EM CONTEXTO DINÂMICO USANDO GEOLOCALIZAÇÃO EM GATEWAYS DE PAGAMENTO

Trabalho de Conclusão de Curso (monografia) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Central.

Aprovada em 22 / 12 / 2025 .

BANCA EXAMINADORA:

Profa. M.a. Cláutenis Carvalho Viana(Orientadora)
Instituto Federal do Piauí (IFPI)

Prof. M.e. Wilson de Oliveira Junior
Instituto Federal do Piauí (IFPI)

Prof. Dra. Nádia Mendes dos Santos
Instituto Federal do Piauí (IFPI)

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, que me deu coragem, força e fé para continuar essa caminhada mesmo diante dos desafios que, por vezes, me desmotivaram. Agradeço especialmente à minha mãe, Laudimary, por todo o apoio emocional e incentivo incondicional. À minha namorada, Lays, por estar ao meu lado em todos os momentos, compreender todos eles e me encorajar. Aos meus professores do curso, que contribuíram direta e indiretamente com a elaboração desse projeto, e de modo especial à minha orientadora, Professora Cláutenis, pela orientação dedicada, paciência e constante incentivo à melhoria do meu trabalho. Acredito que a soma de todas essas contribuições foi essencial não apenas para tirar esta ideia do papel, mas também para ampliar minha visão sobre a importância desta proposta para os futuros usuários.

“Sucesso é a soma de pequenos esforços repetidos dia após dia.”
— Robert Collier

RESUMO

Este trabalho apresenta uma proposta de arquitetura de autenticação voltada a sistemas de pagamento digital, diante da crescente necessidade de fortalecer a segurança frente ao aumento de fraudes e acessos não autorizados. O intuito da pesquisa é propor um modelo capaz de gerar tokens dinâmicos vinculados a variáveis contextuais — como geolocalização, endereço IP e horário de acesso — utilizando processos de tokenização para tornar a validação mais adaptável e robusta. A solução consiste na modelagem e implementação de um microserviço responsável pela emissão e verificação desses tokens, considerando os fatores ambientais no momento da solicitação, o que reforça a proteção em ambientes distribuídos. A proposta se justifica frente aos desafios impostos pela transformação digital no setor financeiro, que demanda mecanismos mais flexíveis e responsivos diante do crescimento das transações online. Dessa forma, espera-se que o modelo contribua para a mitigação de acessos indevidos, complementando as abordagens tradicionais e promovendo maior confiabilidade nos processos de identidade digital.

Palavras-chave: autenticação; tokenização; microserviço; segurança; geolocalização.

ABSTRACT

This work presents an authentication architecture proposal designed for digital payment systems, addressing the growing need to strengthen security against the rise of fraud and unauthorized access. The aim of this research is to propose a model capable of generating dynamic tokens linked to contextual variables — such as geolocation, IP address, and access time — utilizing tokenization processes to make the authentication more adaptable and robust. The solution consists of the modeling and implementation of a microservice responsible for issuing and validating these tokens, taking into account environmental factors at the time of the request, which enhances protection in distributed environments. The proposal is justified by the challenges imposed by digital transformation in the financial sector, which demands more flexible and responsive mechanisms given the growth of online transactions. Thus, the model is expected to contribute to the mitigation of unauthorized access, complementing traditional approaches and promoting greater reliability in digital identity processes.

Keywords: authentication; tokenization; microservice; security; geolocation.

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface* (Interface de Programação de Aplicações)
ORM	*Object Relational Mapping* (Mapeamento Objeto-Relacional)
REST	*Representational State Transfer* (Transferência de Estado Representacional)
GDPR	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados)
LGPD	Lei Geral de Proteção de Dados
TLS	*Transport Layer Security* (Segurança da Camada de Transporte)
JWT	*JSON Web Token* (Token Web em JSON)
MITM	*Man-in-the-Middle* (Homem no Meio)
OTP	*One-Time Password* (Senha de Uso Único)
SSO	*Single Sign-On* (Autenticação Única)
ZTA	*Zero Trust Architecture* (Arquitetura de Confiança Zero)
AES	*Advanced Encryption Standard* (Padrão de Criptografia Avançada)
CSRF	*Cross-site Request Forgery* (Falsificação de solicitação entre sites)
XSS	*Cross-site Scripting* (Scripting entre sites)
DTO	*Data Transfer Object* (Objeto de Transferência de Dados)

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação tornou-se um dos pilares centrais para o funcionamento confiável de serviços financeiros digitais. Com o avanço da transformação digital e a disseminação de plataformas de pagamento online, surgem também novos desafios relacionados à proteção de dados e à prevenção de fraudes. Este capítulo apresenta o contexto da pesquisa, delimita o problema de investigação e discute a relevância da aplicação da tokenização baseada em contexto dinâmico como proposta de solução inovadora para reforçar a segurança em transações digitais.

1.1 CONTEXTUALIZAÇÃO

A transformação digital revolucionou os serviços financeiros, tornando as transações mais rápidas e acessíveis por meio de plataformas como PayPal, PagSeguro, Mercado Pago e PicPay. No entanto, essa modernização trouxe desafios significativos em segurança cibernética, devido ao aumento de ataques sofisticados que visam explorar vulnerabilidades nos sistemas de pagamento (1).

Tradicionalmente, a segurança dos sistemas era baseada em arquiteturas centradas em perímetro. Nesse modelo, considerava-se que tudo o que estivesse dentro da rede corporativa — como sistemas internos, servidores e aplicações locais — era seguro. No entanto, com a popularização do trabalho remoto, da computação em nuvem e do uso de dispositivos móveis, esse modelo se tornou obsoleto. Atualmente, até mesmo ambientes internos, como redes corporativas, *data centers* e sistemas legados, estão sujeitos a riscos e não podem mais ser considerados confiáveis por padrão (1). Além disso, a adoção crescente de arquiteturas baseadas em *microservices* — onde aplicações são divididas em componentes menores e independentes que se comunicam entre si — introduz novos pontos de vulnerabilidade. Cada ponto de interação entre serviços pode se tornar uma porta de entrada para agentes maliciosos, especialmente em sistemas de pagamento que lidam com dados sensíveis, como informações bancárias e credenciais de usuários (2).

Nesse cenário, os *tokens* desempenham um papel crucial na segurança das transações. Um *token* é um código gerado temporariamente que representa a identidade ou autorização de um usuário para realizar determinada ação. Ele substitui informações sensíveis — como senhas e dados bancários — durante as transações, reduzindo o risco de exposição dessas informações (3). No entanto, se um *token* for interceptado em ambientes inseguros, como redes Wi-Fi públicas ou dispositivos comprometidos, ele pode ser reutilizado por atacantes, comprometendo a segurança da transação.

Para mitigar esse risco, surge a *tokenização baseada em contexto dinâmico*. Essa abordagem associa cada *token* a variáveis contextuais específicas, como geolocalização, horário da transação, tipo de dispositivo e comportamento do usuário. Assim, o *token* só será aceito se for utilizado nas mesmas condições sob as quais foi gerado, dificultando a reutilização indevida e protegendo as transações mesmo em ambientes pouco confiáveis (4).

Diante desse cenário, esta pesquisa busca responder à seguinte pergunta: *Como a tokenização baseada em contexto dinâmico usando geolocalização pode aumentar a segurança de gateways de pagamento frente às ameaças cibernéticas atuais?* A investigação propõe desenvolver um modelo funcional que integre a tokenização baseada em contexto dinâmico aos sistemas de pagamento, visando detectar e bloquear tentativas de acesso malicioso em tempo real, sem comprometer a experiência do usuário.

1.2 PROBLEMA DE PESQUISA

Apesar de sua eficácia teórica, a **tokenização baseada em contexto dinâmico utilizando a geolocalização** ainda é pouco explorada em implementações práticas no setor de pagamentos digitais. A maioria das soluções atualmente empregadas ignora o contexto em que o *token* é reutilizado, o que facilita sua exploração por cibercriminosos, especialmente quando há falhas na rede ou dispositivos comprometidos.

A geolocalização, por sua vez, é um fator contextual relevante, pois possibilita confirmar a presença física do usuário no momento da transação, atuando como um elemento adicional de verificação de identidade. Estudos recentes mostram que o uso de geolocalização em sistemas de autenticação pode mitigar significativamente fraudes em ambientes sensíveis como caixas eletrônicos e plataformas de pagamento eletrônico, reduzindo a dependência de fatores vulneráveis como senhas e *OTPs* (*One-Time Passwords*) (5).

Além disso, muitos dos estudos existentes sobre segurança de transações concentram-se em abordagens tradicionais ou generalistas, sem aprofundar a aplicação de mecanismos contextuais dinâmicos em ambientes críticos como *gateways* de pagamento (6).

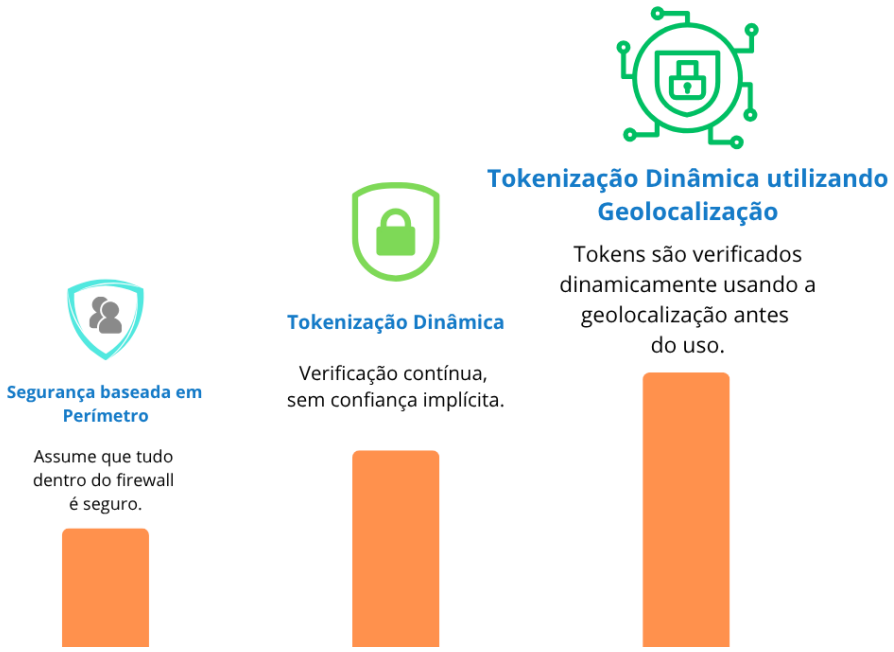
Dessa forma, o problema central desta pesquisa é formulado da seguinte maneira:

> *Como a tokenização baseada em contexto dinâmico utilizando geolocalização pode ser aplicada para fortalecer a segurança em gateways de pagamento e reduzir fraudes e acessos indevidos?*

A Figura 1 apresenta uma representação comparativa entre três modelos de segurança distintos. À esquerda, encontra-se o modelo tradicional de segurança

baseado em perímetro, no qual se assume que tudo o que está dentro da rede (interna ao firewall) é seguro, estabelecendo uma confiança implícita nos dispositivos e usuários internos. Ao centro, destaca-se a tokenização dinâmica, que introduz o conceito de verificação contínua, eliminando a confiança implícita e reforçando os mecanismos de controle e autenticação. Por fim, à direita, está o modelo proposto neste trabalho, que incorpora a tokenização dinâmica baseada em geolocalização, permitindo a validação de tokens de forma contextualizada, de acordo com a localização geográfica do usuário no momento da requisição. Essa evolução demonstra o avanço das práticas de segurança em direção a abordagens mais adaptativas, inteligentes e alinhadas aos princípios do modelo Zero Trust.

Figura 1 – Comparação entre segurança baseada em perímetro, tokenização dinâmica e tokenização dinâmica com geolocalização



Fonte: O Autor (2025).

1.3 JUSTIFICATIVA

A proteção de transações digitais tornou-se um desafio crítico, especialmente para ambientes como gateways de pagamento, que operam em cenários de alto risco e elevada sensibilidade dos dados. Apesar dos avanços em segurança, práticas amplamente utilizadas ainda apresentam limitações na proteção contra ataques que exploram a reutilização de tokens, principalmente quando esses tokens não estão vinculados ao contexto da transação.

Esse cenário evidencia uma lacuna significativa tanto na indústria quanto na academia, particularmente na aplicação de mecanismos capazes de invalidar auto-

maticamente tentativas de uso de credenciais fora dos parâmetros originais — como geolocalização, dispositivo ou tempo. A ausência de tokenização baseada em contexto permite que credenciais capturadas sejam reutilizadas por agentes maliciosos, gerando prejuízos financeiros e comprometendo a integridade das operações digitais.

A motivação para este projeto está justamente na busca por uma solução que vá além dos modelos tradicionais, entregando uma abordagem mais robusta, inteligente e contextualizada. Ao propor um microserviço focado na geração de tokens dinâmicos vinculados à geolocalização, este trabalho oferece uma contribuição prática e aplicável, que visa mitigar um dos vetores mais recorrentes de fraudes em ambientes digitais.

Além de atender a uma necessidade real do mercado, a proposta também contribui academicamente ao explorar um tema ainda pouco abordado de forma aplicada: a tokenização dinâmica baseada em fatores contextuais. Este diferencial não apenas aprimora os níveis de segurança, mas também promove uma reflexão sobre a evolução dos modelos de autenticação em ambientes distribuídos e sensíveis, como sistemas financeiros.

Portanto, este projeto se justifica tanto pela sua relevância prática — diante do aumento exponencial das fraudes e ataques a plataformas de pagamento — quanto pela sua contribuição científica, ao preencher uma lacuna existente na literatura sobre segurança aplicada a transações digitais.

1.4 OBJETIVO GERAL

Desenvolver um microserviço de segurança para gateways de pagamento que implemente tokenização dinâmica baseada em contexto, com foco na geolocalização, garantindo que os tokens de autenticação só sejam válidos sob as mesmas condições contextuais em que foram gerados.

1.5 OBJETIVOS ESPECÍFICOS

- Analisar as principais vulnerabilidades associadas aos mecanismos de autenticação utilizados em gateways de pagamento.
- Avaliar a aplicabilidade dos conceitos de tokenização baseada em contexto e dos princípios do modelo Zero Trust no fortalecimento da segurança de transações digitais.
- Projetar e implementar um microserviço que associe tokens a variáveis contextuais, como geolocalização, horário e tipo de dispositivo.
- Integrar o microserviço a um ambiente de testes que simule cenários reais de autenticação em gateways de pagamento.

- Avaliar a eficácia do modelo desenvolvido por meio de testes comparativos com métodos de segurança tradicionais.

2 FUNDAMENTAÇÃO TEÓRICA

A crescente evolução dos sistemas de pagamentos digitais tem impulsionado a necessidade de mecanismos de segurança mais robustos, especialmente frente ao aumento de fraudes e ataques direcionados. Segundo Liu et al. (2022), o comércio eletrônico enfrenta uma onda contínua de ameaças cibernéticas, como ataques de engenharia social, interceptação de dados e sequestro de sessões, evidenciando a urgência por abordagens de segurança mais adaptativas e contextuais. Nesse contexto, a **tokenização dinâmica baseada em contexto**, com foco na variável de **geolocalização**, surge como uma abordagem inovadora e eficaz para fortalecer a proteção de transações financeiras. Diferente de soluções tradicionais, essa técnica garante que tokens de autenticação sejam válidos apenas quando as condições contextuais — como localização física, dispositivo e janela temporal — coincidam com aquelas em que foram gerados. Esse paradigma eleva significativamente o nível de segurança contra ataques de interceptação, *replay* e sequestro de sessão (3, 5).

2.1 TOKENIZAÇÃO DINÂMICA BASEADA EM CONTEXTO

De acordo com o *Payment Tokenization Technical Framework* (7), desenvolvido pela EMVCo (2019), a tokenização é considerada um dos principais mecanismos de proteção para dados sensíveis em transações digitais. O documento estabelece diretrizes técnicas amplamente adotadas pela indústria de pagamentos, incluindo princípios de segurança, validade e gerenciamento de tokens.

A tokenização consiste no processo de substituir dados sensíveis por identificadores não sensíveis chamados de tokens. Entretanto, na maioria das implementações comerciais, os tokens são estáticos, sendo válidos até sua expiração, independentemente de quem, quando ou onde estão sendo utilizados. A **tokenização dinâmica baseada em contexto** rompe esse paradigma, associando a validade do token a variáveis ambientais específicas, como:

- **Geolocalização**: validação baseada em dados de GPS, IP ou triangulação de redes, garantindo que a transação ocorra no local autorizado;
- **Tempo**: restrição de validade do token para uma janela temporal muito curta (segundos ou minutos);
- **Dispositivo**: verificação do fingerprint do dispositivo, como ID único, certificado ou hardware específico;
- **Comportamento**: análise de padrões de uso e detecção de desvios no comportamento transacional.

Estudos recentes, como o de Granja (2024) (8), reforçam a importância de avançar os modelos tradicionais de tokenização para soluções mais robustas, escaláveis e adaptáveis. O trabalho propõe um framework de próxima geração, incorporando tecnologias como blockchain, algoritmos resistentes à computação quântica e inteligência artificial para criar sistemas de tokenização sensíveis ao contexto, com capacidade de detectar fraudes em tempo real. Embora essa abordagem explore uma infraestrutura altamente distribuída e complexa, ela evidencia uma tendência clara no avanço dos mecanismos de segurança para pagamentos digitais. O presente trabalho, alinhado a essa tendência, concentra-se especificamente na aplicação prática da **geolocalização como variável central do contexto**, visando oferecer uma solução de tokenização contextual mais leve, eficiente e diretamente aplicável a gateways de pagamento.

2.1.1 Foco na Geolocalização como Fator Crítico

O uso de **geolocalização** como fator determinante na geração e validação de tokens tem se destacado como uma das abordagens mais eficazes contra fraudes, especialmente no setor financeiro. Segundo Alabdulatif et al. (2023) (5), a inclusão da localização física adiciona uma camada robusta de segurança, dificultando ataques em que um token é capturado e tentado ser reutilizado de outra localidade. Da mesma forma, Granja (2024) (8) destaca que mecanismos de tokenização sensíveis ao contexto, incluindo localização, aumentam significativamente a resistência contra fraudes, principalmente aquelas envolvendo engenharia social, phishing e interceptação de dados. Por exemplo, uma transação iniciada no Brasil não poderá ser validada caso o token seja utilizado a partir de um IP da Ásia ou de um dispositivo não reconhecido, mesmo que outros dados estejam corretos.

2.1.2 Arquitetura Operacional da Tokenização Contextual

O funcionamento da tokenização dinâmica pode ser descrito nas seguintes etapas:

1. O usuário inicia uma solicitação de transação;
2. O sistema coleta variáveis contextuais: geolocalização, dispositivo, IP e tempo;
3. Um token único é gerado, vinculado diretamente a essas variáveis;
4. Durante a validação, o microserviço compara as variáveis do momento com aquelas armazenadas no ato da geração do token;
5. Caso qualquer variável não coincida (ex.: localização diferente), o token é automaticamente invalidado.

2.1.3 Comparativo entre Modelos de Tokenização

A Tabela 1 apresenta um comparativo entre diferentes modelos de tokenização utilizados em sistemas de segurança da informação, com ênfase em soluções aplicadas a ambientes de pagamento digital. Cada abordagem é analisada quanto aos seus principais benefícios e limitações, considerando fatores como simplicidade, segurança, contexto de uso e exigências tecnológicas. Destaca-se, por exemplo, a tokenização contextual com uso de geolocalização, que oferece maior segurança em transações remotas, mas impõe desafios quanto à privacidade dos dados, principalmente sob as diretrizes da LGPD e GDPR. O modelo proposto por Granja (2024), que integra blockchain e inteligência artificial, é citado por sua robustez, embora apresente elevada complexidade técnica e demanda computacional.

Tabela 1 – Comparação entre métodos de tokenização

Método	**Benefícios**	**Limitações**
Tokenização Estática	Simples; reduz exposição de dados sensíveis	Vulnerável a *replay attacks* e roubo de sessão
Tokenização Dinâmica	Contextual; impede reutilização fora do contexto	Exige processamento em tempo real; desafios com privacidade
Tokenização Contextual com Geolocalização	Melhor segurança contra fraudes remotas; proteção contra uso em local não autorizado	Dependência de acesso preciso à geolocalização; desafios legais (LGPD/GDPR)
Tokenização com Blockchain e IA (Granja, 2024)	Alta resiliência; imutabilidade; detecção de fraudes em tempo real	Elevada complexidade de implementação; alta demanda computacional

Fonte: O Autor (2025).

2.2 MODELO ZERO TRUST COMO PRINCÍPIO COMPLEMENTAR

O modelo *Zero Trust* não é o foco central deste trabalho, mas serve como **princípio orientador**. O conceito de “nunca confie, sempre verifique” complementa a tokenização contextual ao assegurar que nenhuma solicitação é implicitamente confiável, mesmo dentro de redes internas (1, 6). Dessa forma, o microserviço proposto adota práticas do Zero Trust, como:

- Validação contínua da identidade do usuário e do dispositivo;
- Restrição de privilégios por contexto;
- Monitoramento constante das variáveis ambientais associadas às transações.

2.3 DESAFIOS E CONSIDERAÇÕES SOBRE PRIVACIDADE

Apesar das vantagens, a adoção da tokenização baseada em geolocalização apresenta desafios, como:

- **Privacidade de Dados**: O uso de localização exige conformidade com a **LGPD** (Lei Geral de Proteção de Dados) e **GDPR** (General Data Protection Regulation).
- **Falsificação de Localização**: Técnicas como VPNs e GPS spoofing podem ser utilizadas para burlar sistemas que dependem exclusivamente da localização.
- **Latência**: A verificação de variáveis contextuais em tempo real pode aumentar a latência nas transações, exigindo uma arquitetura otimizada e escalável.

2.3.1 Conformidade com a LGPD e GDPR

A coleta, o armazenamento e o processamento de variáveis contextuais, como geolocalização e endereço IP, exigem estrita observância à **Lei Geral de Proteção de Dados Pessoais** (LGPD, Lei nº 13.709/2018) e ao **General Data Protection Regulation** (GDPR, Regulamento (UE) 2016/679). Essas legislações estabelecem princípios fundamentais como finalidade, adequação, necessidade, transparência e segurança, que devem orientar o desenho da solução de tokenização contextual. Assim, o sistema deve garantir que:

- O tratamento de dados pessoais ocorra com base em uma hipótese legal, como o *consentimento* do titular ou legítimo interesse claramente justificado;
- Os dados sensíveis, como informações de localização, sejam coletados de forma mínima, limitada à finalidade de autenticação contextual e prevenção de fraudes;
- O usuário tenha ciência e controle sobre quais dados são tratados, podendo revogar o consentimento ou solicitar a exclusão, conforme previsto nos direitos do titular;
- Mecanismos de segurança, como criptografia e anonimização, sejam implementados para mitigar riscos de acesso indevido ou vazamentos;
- Procedimentos de auditoria, registro de logs e governança de dados estejam alinhados com as exigências de prestação de contas (*accountability*).

Além disso, o GDPR impõe requisitos adicionais como a definição de um *Data Protection Officer* (DPO), avaliação de impacto de proteção de dados (DPIA) quando houver alto risco para os direitos dos titulares, e a obrigatoriedade de notificação de incidentes de segurança em prazos específicos. Portanto, a implementação de um

microserviço de tokenização contextual com ênfase na variável de geolocalização deve considerar tais exigências desde as etapas de concepção (*privacy by design*) e operação (*privacy by default*), garantindo a conformidade legal e a confiança do usuário final.

2.4 CONCLUSÃO DA FUNDAMENTAÇÃO

A revisão da literatura demonstra que a tokenização dinâmica baseada em contexto, com ênfase na geolocalização, representa uma evolução fundamental na proteção de sistemas de pagamento digital. Aliada a princípios do Zero Trust, essa abordagem oferece um modelo mais seguro, dinâmico e resiliente frente às ameaças cibernéticas contemporâneas. Estudos como o de Granja (2024) (8) confirmam que o futuro da segurança em pagamentos digitais está na integração de múltiplas camadas de proteção — desde blockchain até IA —, contudo, este trabalho se posiciona na proposição de um modelo prático, de menor complexidade, priorizando a geolocalização como variável principal na geração e validação de tokens. O desenvolvimento de um microserviço especializado na geração e validação desses tokens, como proposto neste trabalho, preenche uma lacuna tecnológica significativa, contribuindo diretamente para a mitigação de fraudes e aprimoramento da segurança em transações digitais.

3 TRABALHOS RELACIONADOS

A presente seção tem como objetivo apresentar e discutir trabalhos e soluções já existentes que se aproximam da proposta deste estudo, a fim de identificar os avanços, limitações e lacunas ainda presentes no cenário da segurança aplicada a sistemas de pagamento digital. A análise é dividida em duas vertentes: a primeira examina os mecanismos de segurança utilizados por gateways de pagamento amplamente adotados no Brasil e América Latina, enquanto a segunda revisa publicações acadêmicas que abordam temas como Zero Trust, tokenização e autenticação baseada em contexto.

De acordo com Liu et al. (2022), o comércio eletrônico enfrenta uma crescente variedade de ameaças cibernéticas, incluindo ataques de engenharia social, interceptação de dados, falsificação de identidade e sequestro de sessões. Esse cenário exige a constante evolução dos mecanismos de segurança, impulsionando pesquisas voltadas a soluções mais inteligentes e contextuais, como tokenização baseada em geolocalização e modelos adaptativos de autenticação.

A partir dessa análise, busca-se demonstrar em que medida o modelo proposto neste trabalho se diferencia ou complementa as abordagens existentes, evidenciando sua originalidade, relevância e aplicabilidade prática.

3.1 GATEWAYS DE PAGAMENTO E MODELOS DE SEGURANÇA

Para entender o cenário atual da segurança em pagamentos digitais, foram analisados três dos principais gateways de pagamento utilizados no Brasil e na América Latina: PagSeguro, Mercado Pago e PicPay. A seguir, são descritos os principais aspectos de segurança implementados por cada um deles, bem como suas limitações.

O *PagSeguro* oferece autenticação multifator (MFA), criptografia TLS e monitoramento de fraudes. No entanto, não adota um modelo de segurança baseado em verificação contínua, como o Zero Trust, e depende de autenticações estáticas.

O *Mercado Pago* adota medidas como *machine learning* para detecção de fraudes, autenticação em duas etapas e proteção contra chargebacks, mas não aplica os princípios do modelo Zero Trust nem utiliza tokenização contextualizada.

O *PicPay* adota autenticação biométrica e cartões virtuais temporários, mas seu sistema de segurança ainda se apoia em mecanismos estáticos e não emprega tokenização baseada em fatores dinâmicos, como geolocalização ou análise contextual.

3.2 TRABALHOS ACADÊMICOS RELACIONADOS

A revisão de literatura revelou que, embora o modelo Zero Trust seja amplamente discutido como referência para segurança moderna, há uma lacuna na aplicação

prática de técnicas como tokenização dinâmica baseada em contexto em ambientes de pagamento digital. A Tabela 2 resume os principais trabalhos analisados, agrupados por foco principal.

A fim de organizar as contribuições mais relevantes identificadas na literatura, foi elaborado um quadro comparativo que agrupa os trabalhos por áreas temáticas centrais: modelos de Zero Trust, tokenização e autenticação em pagamentos, e infraestrutura de pagamentos. A Tabela 2 apresenta um resumo dessas publicações, destacando a principal contribuição de cada estudo e suas limitações no contexto da segurança em ambientes de pagamento digital. Essa categorização facilita a identificação de lacunas específicas — especialmente quanto à ausência de abordagens que integrem autenticação contextual, uso de geolocalização e tokenização dinâmica sob os princípios do modelo Zero Trust.

Tabela 2 – Trabalhos Acadêmicos Relacionados sobre Zero Trust, Tokenização e Geolocalização

Trabalho	Contribuição	Limitações
Modelos de Zero Trust		
Kang et al. (2023)	Apresenta os fundamentos e desafios na aplicação do modelo Zero Trust	Não aborda integração com tokenização dinâmica ou uso de fatores contextuais.
Meng et al. (2022)	Protocolo de autenticação contínua para ambientes Zero Trust sem autoridade central confiável	Utiliza tokens com características estáticas, sem adaptação a contexto como geolocalização.
Chuan et al. (2020)	Apresenta método de implementação de Zero Trust em rede corporativa	Não aborda tokenização nem autenticação contextual em pagamentos.
Tokenização e Autenticação em Pagamentos		
Muresan (2020)	Técnicas de tokenização aplicadas a ambientes serverless para segurança em pagamentos	Não considera fatores contextuais nem arquitetura baseada em confiança mínima.
Alabdulatif et al. (2023)	Autenticação multifator baseada em geolocalização aplicada a terminais físicos (ATM)	Não aplica tokenização, nem trata do contexto de pagamentos online.
Infraestrutura de Pagamentos		
Ragazzo et al. (2022)	Analisa a infraestrutura de pagamentos digitais no Brasil e desafios regulatórios	Não propõe técnicas de tokenização ou autenticação contextual.
Gulyas e Kiss (2023)	Evidenciam os impactos financeiros de ataques cibernéticos em instituições financeiras europeias	Não propõem soluções técnicas específicas para pagamentos digitais ou gateways online.

Fonte: O Autor (2025).

3.3 CONTRIBUIÇÃO DO TRABALHO PROPOSTO

Este trabalho propõe um modelo inovador de tokenização dinâmica baseada em contexto, aplicável a transações financeiras em gateways de pagamento. O sistema vincula cada token de autenticação a fatores contextuais como geolocalização, tempo e dispositivo, tornando os tokens não reutilizáveis e inutilizáveis fora do seu contexto de emissão.

Ao contrário dos modelos revisados, que tratam o Zero Trust como arquitetura geral ou aplicam tokenização de forma estática, esta pesquisa propõe a união prática dessas abordagens, oferecendo:

- **tokenização baseada em contexto**, reforçando a segurança contra ataques de replay e roubo de credenciais;
- **autenticação adaptativa**, com variação dinâmica de exigências com base no risco contextual;
- **monitoramento contínuo**, com análise comportamental para detecção em tempo real de anomalias.

Além disso, conforme definido pelo framework técnico da EMVCo (U.S. Payments Forum, 2019), a tokenização substitui dados sensíveis por identificadores não sensíveis sem valor extrínseco, garantindo que, mesmo em caso de interceptação, os tokens não revelem informações originais e não permitam reutilização fora de ciclo. Tokens EMV enviados via NFC são válidos enquanto durar a transação e oferecem alta eficácia contra fraudes em múltiplos canais de pagamento (7).

O modelo se fundamenta nos princípios do Zero Trust — verificação contínua, mínima confiança e limitação de privilégios —, mas inova ao aplicar esses princípios por meio de um sistema técnico de tokenização contextual. Espera-se que essa abordagem contribua significativamente para a evolução da segurança em pagamentos digitais, oferecendo uma solução concreta e aplicável à realidade de sistemas modernos.

4 METODOLOGIA

A metodologia adotada nesta dissertação foi cuidadosamente elaborada com o intuito de garantir a validade técnica e científica da proposta de um microserviço de autenticação com tokens sensíveis ao contexto, fundamentado em geolocalização, IP e horário. Para tanto, foi delineada uma abordagem que combina princípios de pesquisa aplicada com experimentação controlada, de modo a permitir tanto o desenvolvimento prático da solução quanto sua validação por meio de testes realistas. Esta seção detalha os procedimentos adotados, as ferramentas utilizadas, a modelagem arquitetural da solução, bem como os métodos de teste, critérios de avaliação e justificativas para as decisões técnicas. A estrutura apresentada visa assegurar a reprodutibilidade e a robustez da proposta frente ao problema de segurança em ambientes de transações digitais.

4.1 TIPO DE PESQUISA

Trata-se de uma pesquisa **aplicada** pois tem como objetivo o desenvolvimento de uma solução prática para um problema real: o aumento da segurança em sistemas de autenticação de transações financeiras, como gateways de pagamento. O microserviço proposto busca aplicar conceitos técnicos já consolidados — como autenticação via tokens, análise contextual e verificação de localização — em um novo arranjo que pode contribuir diretamente para a mitigação de fraudes e acessos indevidos.

Ao mesmo tempo, caracteriza-se como uma pesquisa **experimental** uma vez que será construído um ambiente controlado para simulação de transações e ataques. Nesse ambiente, o microserviço será testado com diferentes variáveis de contexto (como endereço IP, localização geográfica e horário da requisição) para avaliar sua capacidade de identificar padrões legítimos e bloquear tentativas suspeitas. Os resultados obtidos permitirão analisar, de forma empírica, a eficácia da abordagem proposta frente a técnicas tradicionais de autenticação.

Essa combinação de pesquisa aplicada com experimentação prática visa não apenas validar o funcionamento técnico do microserviço, mas também oferecer evidências quantitativas de sua contribuição para a segurança de sistemas de pagamento.

4.2 FERRAMENTAS E TECNOLOGIAS UTILIZADAS

A implementação do microsserviço de segurança foi estruturada sobre a *stack* Node.js, selecionada por sua alta performance e adequação a arquiteturas orientadas a eventos. A escolha das ferramentas, bibliotecas e serviços pautou-se em critérios de

escalabilidade, segurança criptográfica e interoperabilidade. A seguir, detalham-se as tecnologias empregadas:

- **Linguagem e *Framework***:
  - **Node.js**: Plataforma de execução JavaScript baseada no motor V8, ideal para microsserviços devido ao seu modelo de I/O não bloqueante, permitindo o processamento eficiente de múltiplas requisições simultâneas.
  - **NestJS**: *Framework* progressivo para Node.js, utilizado para estruturar a API. Sua arquitetura modular e suporte nativo a TypeScript e Injeção de Dependências garantem um código organizado, testável e escalável.
- **Armazenamento de Dados**:
  - **PostgreSQL**: Banco de dados relacional utilizado para a persistência estruturada de usuários, *logs* de auditoria e histórico de transações.
  - **Redis**: Armazenamento chave-valor em memória, empregado para gestão de sessões e *caching* de tokens com TTL (*Time to Live*), otimizando o tempo de resposta da autenticação.
- **Segurança e Criptografia**:
  - **Argon2**: Algoritmo de *hashing* vencedor da *Password Hashing Competition*, utilizado para armazenamento seguro de senhas, oferecendo resistência a ataques de força bruta baseados em GPU/ASIC (9).
  - **AES (Advanced Encryption Standard)**: Padrão de criptografia simétrica utilizado para proteger dados sensíveis em repouso.
  - **JsonWebToken (JWT)**: Padrão para criação de tokens de acesso compactos e seguros (*stateless*).
  - **Helmet e CORS**: *Middlewares* para proteção contra vulnerabilidades *web* comuns, como XSS e injeção de cabeçalhos.
- **Serviços Externos e Integrações**:
  - **MaxMind (GeoIP)**: Serviço de geolocalização utilizado para correlacionar o endereço IP da requisição à localização física aproximada do usuário.
  - **Mercado Pago (Sandbox API)**: Plataforma de pagamentos utilizada em ambiente de testes (*sandbox*) para simular fluxos financeiros reais. Sua integração permitiu validar o comportamento do microsserviço na interceptação e autorização de transações sem a necessidade de movimentação monetária real.

  - **Amazon SES (Simple Email Service)**: Serviço de envio de e-mails da AWS, escalável e de alta disponibilidade. Utilizado no projeto para o disparo de alertas automáticos de segurança e notificações de atividades suspeitas.
  - **Axios**: Cliente HTTP baseado em *promises* para consumo de APIs externas.

- **Infraestrutura e Testes**:
  - **Docker**: Utilizado para a conteinerização da aplicação e do banco de dados, garantindo paridade entre os ambientes de desenvolvimento e produção.
  - **Kali Linux**: Distribuição Linux focada em testes de penetração, utilizada em máquina virtual para simular ataques e validar a resiliência do microsserviço.
  - **OWASP ZAP (Zed Attack Proxy)**: Ferramenta de teste de segurança de aplicações web de código aberto, utilizada para identificar vulnerabilidades comuns (como Injeção SQL, XSS, etc.) através de *scanners* automáticos e como *proxy* interceptor para testes manuais de vulnerabilidade e validação da lógica contextual do microsserviço.
  - **Insomnia**: Cliente de API para testes manuais e depuração de rotas REST.

4.3 ARQUITETURA DO MICROSERVIÇO

A arquitetura proposta consiste em um microsserviço independente, desenhado para operar de forma modular e segura. O núcleo da solução é a autenticação contextual, que transcende a validação tradicional de credenciais ao incorporar variáveis ambientais — endereço IP, geolocalização e horário — no processo de emissão e validação de tokens JWT.

A escolha por uma arquitetura de microsserviços justifica-se pela necessidade de isolar a lógica de segurança, permitindo que este componente seja escalado, atualizado e auditado independentemente dos demais sistemas (como gateways de pagamento). O fluxo de dados segue o padrão REST, com comunicação criptografada via TLS.

Componentes Arquiteturais e Fluxo de Dados

Abaixo são descritos os componentes lógicos que compõem a arquitetura e suas responsabilidades no fluxo de autenticação:

- **Camada de Controle (API Gateway)**: Implementada com NestJS, atua como o ponto de entrada único. É responsável pela validação inicial dos dados (DTOs), roteamento e aplicação de políticas de segurança (Rate Limiting e CORS) antes que a requisição atinja a lógica de negócio.

- **Módulo de Autenticação Contextual**: O "cérebro"do serviço. Recebe as credenciais e o contexto da requisição. Consulta o serviço de Geolocalização (MaxMind) para validar se a origem do acesso é condizente com o padrão histórico do usuário. Se aprovado, emite um JWT assinado.
- **Camada de Persistência e Cache**:
  - O **PostgreSQL** armazena os dados definitivos e logs de auditoria.
  - O **Redis** atua como *cache* de alta performance para listas de revogação (blocklist) e sessões ativas, reduzindo a latência na verificação de tokens em requisições subsequentes.
- **Módulo de Notificação e Alerta**: Integrado ao **Amazon SES**, este componente é acionado assincronamente sempre que uma anomalia grave é detectada (ex: tentativa de acesso de um país bloqueado), enviando um alerta imediato ao usuário ou administrador.
- **Ambiente de Simulação de Ameaças**: Uma infraestrutura segregada, utilizando Kali Linux, interage com a API pública do microsserviço para executar testes de estresse e tentativas de exploração (como *Replay Attacks*), validando a eficácia das camadas de defesa.

Padrões Adotados

- **RESTful API**: Interface padronizada para comunicação interoperável entre sistemas.
- **Stateless Authentication**: Utilização de tokens JWT autocontidos, eliminando a necessidade de sincronização de sessões no servidor.
- **Context-Aware Security**: Validação dinâmica baseada em parâmetros comportamentais e geográficos.
- **Repository Pattern**: Abstração da camada de dados (via TypeORM) para desacoplar a lógica de negócio do banco de dados específico.

4.4 PROTOTIPAÇÃO VISUAL E DEFINIÇÃO DE FLUXOS

A etapa de prototipação visual foi conduzida utilizando a ferramenta **Figma**, uma plataforma de *design* de interfaces baseada na nuvem, amplamente reconhecida pela sua capacidade de colaboração em tempo real e criação de protótipos de alta fidelidade. A escolha desta ferramenta deveu-se à sua versatilidade em simular interações complexas, permitindo a validação da experiência do usuário (*User Experience* - UX) antes do início da codificação.

No contexto deste projeto, o Figma foi essencial para tangibilizar a lógica abstrata do microsserviço. Foram desenvolvidas interfaces navegáveis que representam as duas pontas da solução:

- **Interface do Cliente**: Telas que simulam um aplicativo bancário realizando uma transação, onde é possível visualizar o comportamento do sistema diante de aprovações ou bloqueios de segurança.
- **Painel Administrativo (*Dashboard*)**: Interface de gestão onde o administrador pode visualizar os *logs* de acesso, a geolocalização dos usuários em um mapa interativo e os alertas de fraude gerados pelo sistema.

Os protótipos permitiram testar visualmente o comportamento do sistema em cenários críticos, tais como:

- **Fluxo Nominal**: Autenticação e transação realizadas com sucesso, com *feedback* visual imediato;
- **Bloqueio por Geolocalização**: Simulação de uma tentativa de acesso vinda de uma região não permitida, acionando as telas de erro correspondentes;
- **Alerta de Fraude**: Demonstração visual de como o sistema notifica o usuário e o administrador via e-mail (simulado na interface) ao detectar anomalias.

Essa abordagem não apenas validou a lógica de negócio, mas serviu como documentação visual para o desenvolvimento da API. Os campos definidos nas telas do Figma orientaram a criação dos DTOs (*Data Transfer Objects*) e dos *payloads* de resposta do *backend*, garantindo que todas as variáveis contextuais necessárias (como IP, País, Estado, Cidade, *timestamp*) fossem corretamente capturadas e processadas.

4.4.1 Justificativa para a Arquitetura de Microsserviços

A escolha pela arquitetura de microsserviços justifica-se por fatores determinantes para a segurança, escalabilidade e manutenibilidade do projeto, conforme detalhado a seguir:

- **Modularidade e Isolamento**: A responsabilidade de autenticação e segurança reside em um serviço autônomo. Isso isola o "núcleo de segurança", impedindo que falhas ou vulnerabilidades em outros módulos da aplicação comprometam o mecanismo de proteção.
- **Escalabilidade Granular**: Permite escalar horizontalmente apenas o serviço de autenticação (‘auth-service‘) em momentos de pico de acessos (*login storms*), otimizando o uso de recursos de infraestrutura sem a necessidade de replicar todo o sistema.

- **Independência Tecnológica**: O microsserviço opera de forma agnóstica, expondo seus serviços via API REST. Isso possibilita sua integração com sistemas legados, novos *gateways* de pagamento ou aplicações desenvolvidas em diferentes linguagens de programação.
- **Testabilidade e Simulação de Ameaças**: A arquitetura desacoplada facilita a execução de testes de intrusão (*Pentest*) em ambientes isolados (utilizando *containers* ou VMs Kali Linux), permitindo validar a robustez da segurança sem oferecer riscos ao ambiente de produção.
- **Segurança por Design**: A separação estrita entre o contexto da transação e a validação de segurança reduz a superfície de ataque e garante que dados sensíveis sejam processados em um ambiente dedicado e monitorado.

Essa abordagem alinha-se às práticas modernas de desenvolvimento seguro (*DevSecOps*), sendo a estratégia ideal para ecossistemas que exigem alta integridade e auditabilidade na validação de requisições.

4.5 DIAGRAMA DE CASOS DE USO

Para fundamentar a modelagem funcional do microsserviço, foi elaborado um Diagrama de Casos de Uso utilizando a notação UML. O diagrama ilustra as fronteiras do sistema e as interações entre as entidades externas e as funcionalidades de segurança, integrando cenários de uso legítimo e tentativas de abuso (*misuse cases*).

As entidades envolvidas na interação foram categorizadas da seguinte forma:

- **Usuário (Ator Primário)**: Entidade que inicia o fluxo de autenticação e requisita a validação de transações. Seu objetivo é obter um token válido para operar dentro do contexto permitido.
- **Atacante (Ator de *Misuse*)**: Representação de uma ameaça externa ou agente malicioso. Este ator interage com o sistema tentando explorar vulnerabilidades, como a reutilização de tokens (ataques de *Replay*) ou falsificação de geolocalização.
- **Sistema de Tokenização (Sujeito)**: Compreende o perímetro da aplicação desenvolvida, responsável por orquestrar a lógica de validação, consulta ao banco de dados e comunicação com serviços externos.

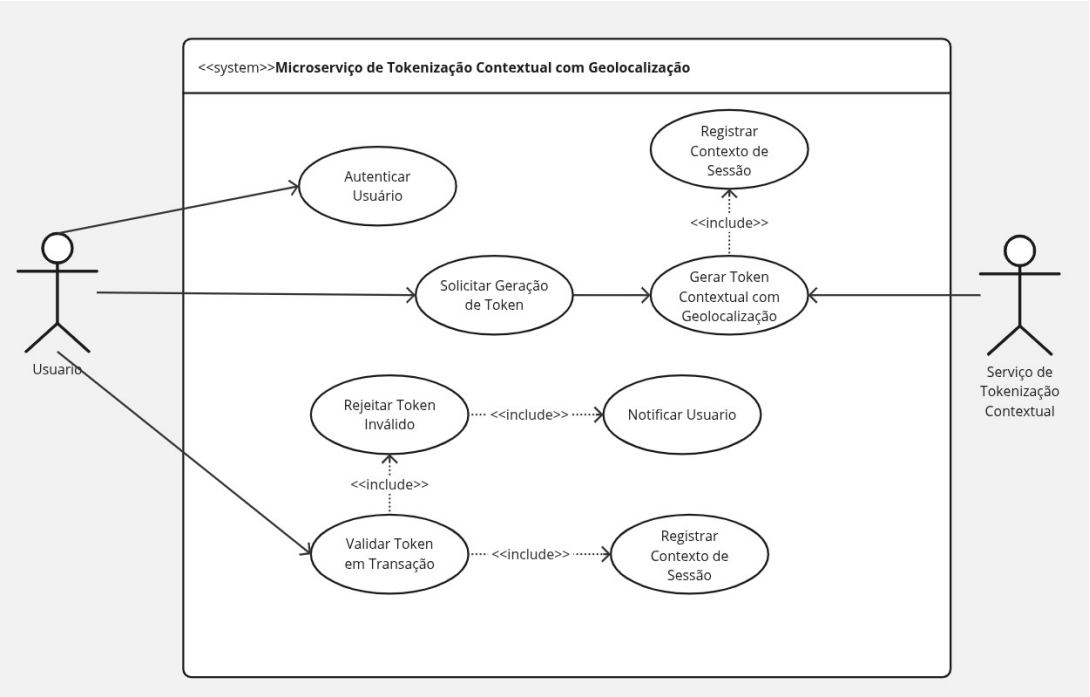
Os principais casos de uso mapeados detalham o ciclo de vida da segurança contextual:

- **Autenticar Usuário**: Ponto de entrada onde o sistema valida as credenciais básicas (login/senha) antes de iniciar a análise contextual.

- **Emitir Token Contextual**: Processo de geração do JWT. Neste momento, o sistema captura e "assina"os dados do ambiente (Endereço IP, Coordenadas GPS e *Timestamp*) dentro do *payload* do token.
- **Validar Token em Requisições**: Funcionalidade crítica que intercepta cada chamada protegida. O sistema decodifica o token e verifica sua integridade criptográfica e validade temporal (TTL).
- **Comparar Geolocalização e Contexto**: Subprocesso da validação que confronta os dados atuais da requisição com os dados originais gravados no token. Verifica se a mudança de posição geográfica é humanamente possível dentro do intervalo de tempo decorrido.
- **Rejeitar Transações Fora do Contexto**: Caso de uso de exceção. Se a comparação geográfica indicar anomalia, o sistema nega a transação e invalida a sessão preventivamente.
- **Notificar Atividade Suspeita**: Ação automatizada que dispara alertas via e-mail (utilizando o serviço Amazon SES) para o usuário titular, informando sobre a tentativa de acesso bloqueada.

Essa modelagem foi essencial para garantir que os requisitos de segurança fossem traduzidos em fluxos funcionais claros, facilitando a comunicação das regras de negócio contextual para todos os *stakeholders* do projeto. A Figura 2 apresenta o diagrama elaborado.

Figura 2 – Diagrama de Casos de Uso: Fluxos de Autenticação e Segurança Contextual



Fonte: O Autor (2025).

4.6 DIAGRAMA DE ATIVIDADES

4.6.1 Dados Relevantes para Geração do Token

Nesta etapa, são definidos os dados essenciais que compõem o token de autenticação gerado pelo microserviço. Esses dados são determinantes para garantir a integridade da sessão e a validação contextual das transações.

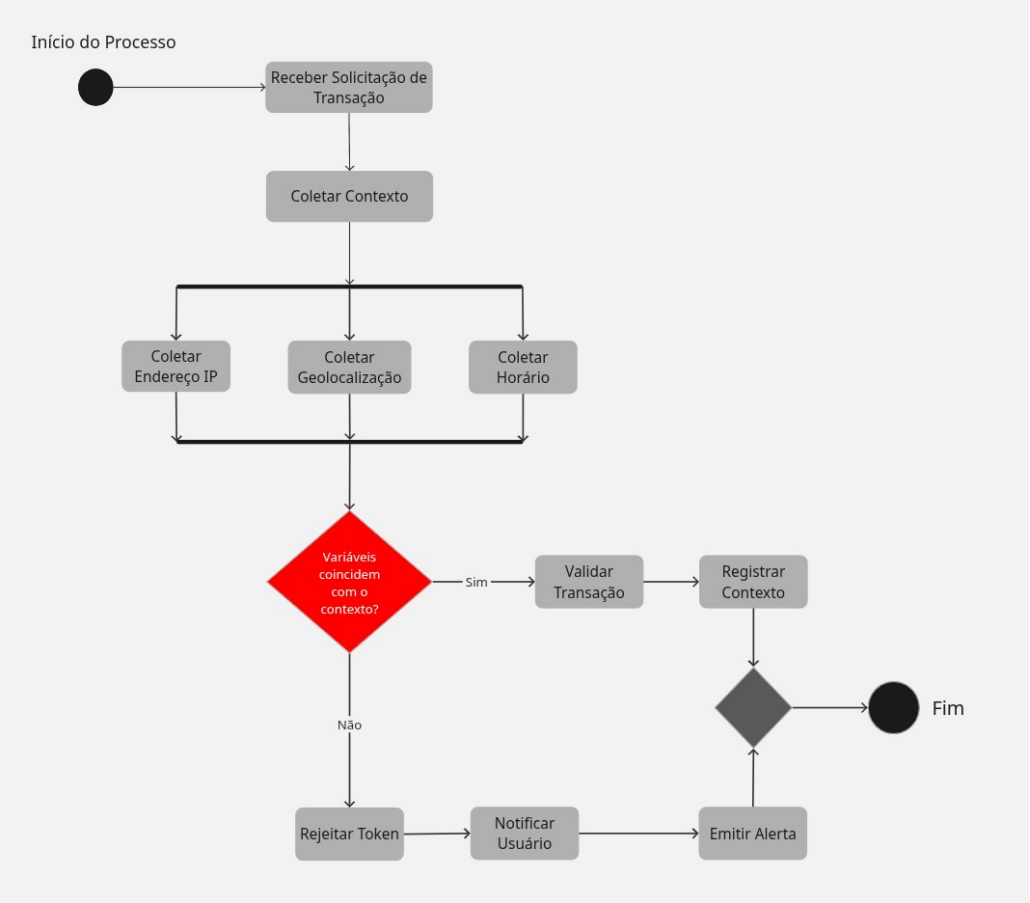
De modo geral, o token inclui informações mínimas de identificação do usuário, como ID único e permissões de acesso, bem como variáveis contextuais que reforçam o modelo de autenticação dinâmica, tais como:

- Geolocalização: registra a localização geográfica do dispositivo no momento da geração;
- Endereço IP: armazena o IP de origem da solicitação para comparações de segurança em sessões subsequentes;
- Horário de emissão: define o timestamp de geração e validade do token, essencial para expiração automática.

A escolha desses dados busca equilibrar a robustez da validação contextual com a proteção à privacidade do usuário, seguindo as boas práticas de segurança da informação. O conjunto dessas informações é utilizado pelo microserviço para detectar

inconsistências comportamentais, emitir alertas e, quando necessário, invalidar ou regenerar o token conforme o fluxo descrito no Diagrama de Atividades. A Figura 3 apresenta o Diagrama de Atividades proposto.

Figura 3 – Diagrama de Atividades do Microserviço de Tokenização Contextual com Geolocalização



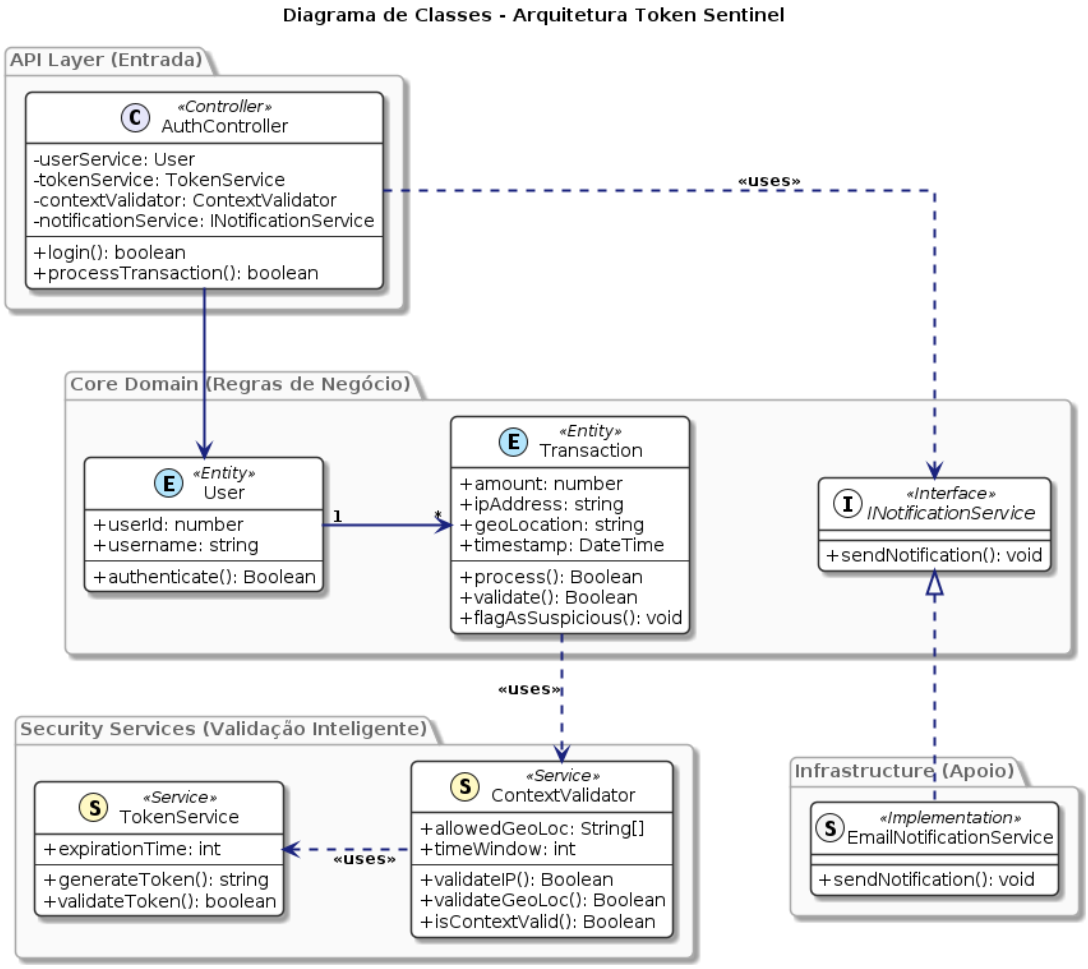
Fonte: O Autor (2025).

A inclusão deste diagrama permite uma visualização mais clara da sequência de ações e decisões, fortalecendo o entendimento do fluxo de autenticação baseado em contexto.

4.7 DIAGRAMA DE CLASSES

O diagrama de classes, apresentado na Figura 4, demonstra a estrutura estática do sistema desenvolvido, descrevendo as principais classes, seus atributos e métodos, bem como os relacionamentos entre elas. Essa modelagem foi elaborada com base na orientação a objetos, respeitando os princípios SOLID, a fim de promover coesão, baixo acoplamento e escalabilidade da solução proposta.

Figura 4 – Diagrama de Classes do Sistema



Fonte: O Autor (2025).

Entre os principais componentes, destacam-se: a classe `TokenService`, responsável pela geração, validação e invalidação de tokens; a classe `ContextValidator`, que executa a verificação de fatores contextuais, como endereço IP, geolocalização e horário, em alinhamento ao modelo Zero Trust; a classe `User`, que representa os dados do usuário e contém operações de autenticação; e a classe `Transaction`, que modela as tentativas de transações financeiras, contemplando operações para validação e sinalização de atividades suspeitas. Além dessas, o diagrama evidencia a utilização de um serviço de notificação desacoplado, representado pela interface `INotificationService` e pela implementação concreta `EmailNotificationService`, possibilitando o envio de alertas via correio eletrônico.

Ressalta-se que essa estrutura fundamenta a metodologia do trabalho, uma vez que permite a implementação de um mecanismo de tokenização dinâmica baseada em contexto, com validações contínuas que visam reduzir fraudes em gateways de pagamento digitais. A arquitetura orientada a serviços garante flexibilidade e evolução contínua do sistema, atendendo aos objetivos de segurança, integridade e escalabili-

dade da pesquisa.

4.8 PROCESSO DE DESENVOLVIMENTO E GESTÃO

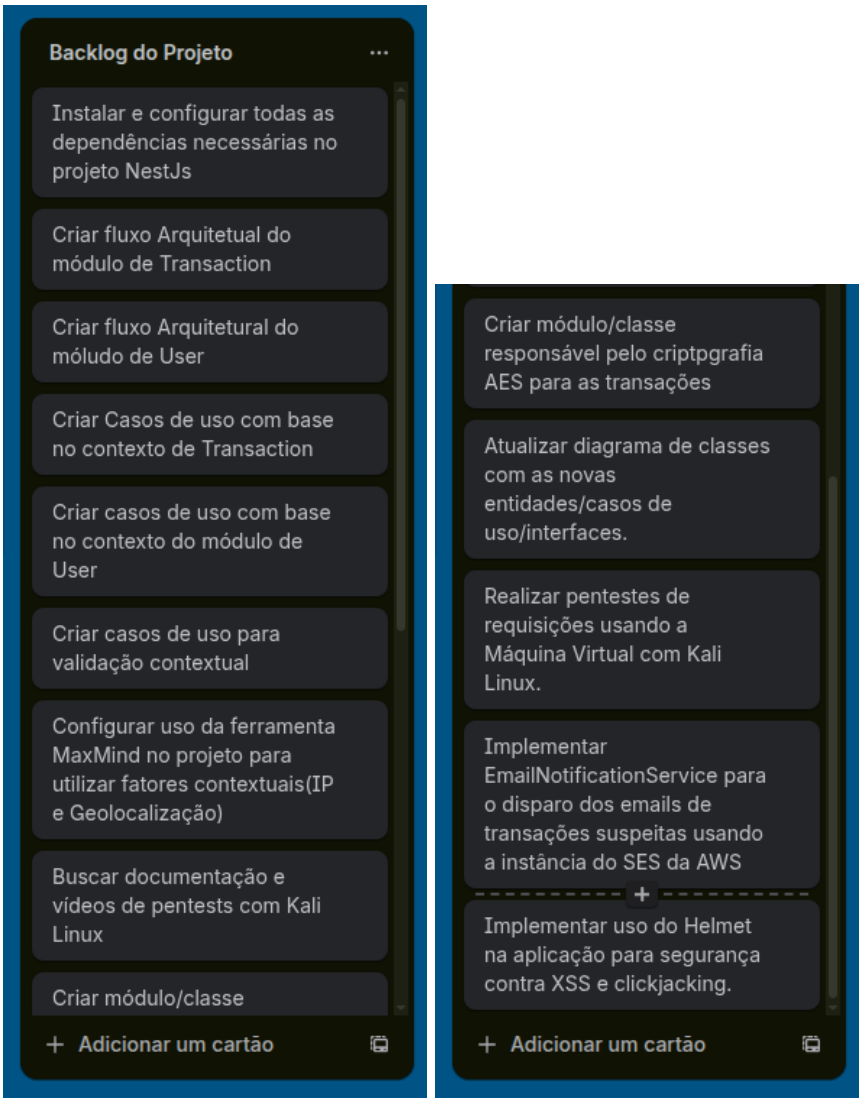
O desenvolvimento do microserviço foi conduzido com base em uma abordagem incremental, utilizando o framework **Scrum** adaptado para a realidade de um projeto individual. O objetivo foi manter a organização, a disciplina de execução e a rastreabilidade das etapas.

4.8.1 Organização do Backlog e Sprints

O processo de definição do escopo foi realizado de maneira sequencial. Inicialmente, foram identificadas todas as tarefas necessárias para a implementação do sistema (Requisitos), organizando-as em uma lista denominada *Product Backlog*.

Conforme ilustrado na Figura 5, o backlog serviu como repositório central de funcionalidades, priorizadas com base nos requisitos de segurança crítica.

Figura 5 – Recorte do Product Backlog priorizado no Trello.



Fonte: O Autor (2025).

Subsequentemente, as funcionalidades foram distribuídas em ciclos iterativos denominados *sprints*. Cada sprint foi planejada para conter um conjunto coeso de tarefas, movendo-se do backlog para a execução quinzenal. A Figura 6 demonstra a organização visual dessas sprints.

Figura 6 – Exemplo de estruturação e planejamento das Sprints.

Fonte: O Autor (2025).

4.8.2 Execução e Monitoramento

Para garantir a cadência de entregas, optou-se por *sprints* com **duração fixa de 15 dias**. Essa escolha visou equilibrar o tempo necessário para o desenvolvimento de lógicas complexas (como validação contextual) com a necessidade de feedbacks rápidos.

A gestão visual do fluxo de trabalho ocorreu mediante quadros Kanban. Ao final de cada ciclo quinzenal, as tarefas na coluna "Concluído"passavam por testes unitários e de integração antes de serem consideradas finalizadas. A Figura 7 evidencia o fluxo de uma sprint em fase de conclusão.

Figura 7 – Visualização do fluxo de trabalho (Kanban) durante a execução do projeto.

Fonte: O Autor (2025).

4.8.3 Cronograma de Execução

O planejamento temporal do projeto foi estruturado para ocorrer em um horizonte de dois meses e meio, compreendendo o período de 01 de setembro a 15 de novembro. O cronograma foi segmentado em cinco ciclos de desenvolvimento (*sprints*) ininterruptos.

A distribuição temporal das atividades, que guiou a execução metodológica do trabalho, está detalhada na Tabela 3.

Tabela 3 – Cronograma de execução das sprints

Ciclo	Data de Início	Data de Término	Foco Principal
Sprint 1	01 de setembro	15 de setembro	Configuração de Dependências
Sprint 2	16 de setembro	30 de setembro	Criação do Software
Sprint 3	01 de outubro	30 de outubro	Integração e Tokenização
Sprint 4	16 de outubro	15 de dezembro	Testes de Segurança
Sprint 5	01 de novembro	15 de dezembro	Refatoração e Documentação

Fonte: O Autor (2025).

O cumprimento rigoroso destas datas permitiu que as etapas de levantamento de requisitos, prototipação, codificação e validação fossem concluídas de forma sequencial, garantindo a integridade dos resultados apresentados no capítulo seguinte.

4.8.4 Etapas do Processo de Desenvolvimento

O desenvolvimento do microserviço foi organizado em etapas sequenciais, que visaram atender aos objetivos de segurança e confiabilidade propostos nesta pesquisa:

- **Levantamento de requisitos**: análise das necessidades relacionadas à autenticação segura em ambientes de transação digital, considerando o uso de contexto (geolocalização, IP, horário) e comparações com abordagens tradicionais;
- **Prototipação**: criação de um protótipo funcional de baixo custo, com o intuito de validar o fluxo de autenticação e a viabilidade da tokenização contextual em ambiente controlado;
- **Desenvolvimento incremental**: implementação do microserviço em ciclos curtos (sprints), utilizando tecnologias como Node.js, Redis e PostgreSQL, com foco na modularização e testabilidade dos componentes;
- **Testes contínuos**: realização de testes unitários, de integração e de segurança ao final de cada sprint, assegurando estabilidade e conformidade dos módulos críticos, especialmente os responsáveis por geração e validação de tokens.

4.9 PROCEDIMENTOS DE TESTE E VALIDAÇÃO

Para garantir a robustez da proposta, serão utilizados diferentes métodos de teste e validação, abrangendo desde aspectos funcionais até a segurança diante de ataques reais. Os procedimentos planejados incluem:

- **Testes unitários e de integração:** Cada módulo do microserviço será testado individualmente e depois em conjunto, garantindo o correto funcionamento das rotinas de geração, validação e expiração dos tokens;
- **Testes de segurança:** Serão simulados ataques por meio de uma máquina virtual com Kali Linux, utilizando ferramentas como Burp Suite, SQLMap e scripts personalizados para testar injeções, interceptações e reutilização de tokens;
- **Casos de teste de contexto:** Serão definidos cenários de autenticação com e sem correspondência contextual (por exemplo, geolocalização divergente, timestamp inválido, origem desconhecida), com o objetivo de verificar se o sistema rejeita acessos fora do perfil esperado;
- **Comparação com autenticação tradicional:** Será feita uma comparação com um modelo de autenticação baseado apenas em credenciais estáticas, sem tokens contextuais, de forma a identificar ganhos de segurança e desempenho com a proposta.

4.10 CRITÉRIOS DE AVALIAÇÃO

A proposta será avaliada com base em indicadores quantitativos e qualitativos, que possibilitem mensurar a eficácia e viabilidade da solução. Os principais critérios considerados serão:

- **Taxa de rejeição de tokens inválidos:** Verifica a capacidade do sistema em identificar e bloquear tentativas de acesso com tokens malformados, expirados ou com informações de contexto inválidas;
- **Tempo médio de autenticação:** Mede o tempo decorrido entre a requisição de autenticação e o retorno da validação, permitindo avaliar o impacto do uso de contexto no desempenho do sistema;
- **Comparativo com sistemas tradicionais:** Serão comparados os resultados do microserviço com os de um sistema base convencional, analisando a eficácia da proposta em termos de segurança e desempenho;
- **Falsos positivos e negativos:** Serão monitoradas as ocorrências de rejeição indevida de tokens válidos (falsos positivos) e de aceitação de tokens inválidos (falsos negativos), para avaliação da precisão do sistema.

5 RESULTADOS

Este trabalho visa desenvolver um microserviço de segurança com foco na tokenização dinâmica baseada em contexto, utilizando variáveis como geolocalização, endereço IP, horário de acesso e padrões comportamentais. Espera-se, com isso, aumentar significativamente a robustez do processo de autenticação frente a acessos não autorizados e a ataques cibernéticos em ambientes distribuídos, especialmente em sistemas de pagamento sensíveis à fraude.

A seguir, são apresentados os principais resultados esperados divididos por componentes-chave da aplicação. Cada subseção é acompanhada por diagramas e representações visuais desenvolvidas na ferramenta Figma, além de textos descritivos explicando o funcionamento e a importância de cada etapa.

5.1 TOKENIZAÇÃO BASEADA EM CONTEXTO DINÂMICO

Espera-se que a principal inovação deste trabalho seja a geração dinâmica de tokens sensíveis ao contexto da transação de pagamento, com ênfase na geolocalização como variável-chave para a validação de cada operação. Diferentemente das abordagens tradicionais, onde o token é emitido no momento do login com validade generalizada, a proposta deste trabalho prevê a criação de um token *contextual e específico para cada transação*, contendo atributos que representem o ambiente físico e digital do usuário no instante da solicitação.

Entre as variáveis contextuais consideradas — como endereço IP, tipo de dispositivo e horário —, destaca-se a geolocalização por sua maior dificuldade de falsificação e por refletir com precisão o ambiente físico da transação.

Início – Solicitação de Transação: O usuário inicia uma transação financeira no sistema, acionando automaticamente o microserviço de autenticação contextual.

Meio – Captura da Geolocalização e Demais Variáveis: O sistema coleta, em tempo real, a geolocalização do dispositivo, além de outras variáveis como endereço IP, sistema operacional e tipo de navegador, formando a base para a emissão condicional do token.

Fim – Geração do Token e Validação Condicional: O microserviço gera um token do tipo JWT, contendo *claims* específicos de geolocalização (País, Cidade e Estado). A validade desse token é restrita a uma zona geográfica pré-definida e a um curto intervalo de tempo. Tentativas de uso fora desse escopo devem ser automaticamente rejeitadas, com registro da atividade suspeita.

5.2 SIMULAÇÃO DE ATAQUES E INTEGRAÇÃO FINANCEIRA

Para validar a robustez da aplicação em um cenário realista, foram conduzidos testes de caixa preta (*black-box testing*) utilizando a distribuição **Kali Linux** integrados à API de *Sandbox* do Mercado Pago.

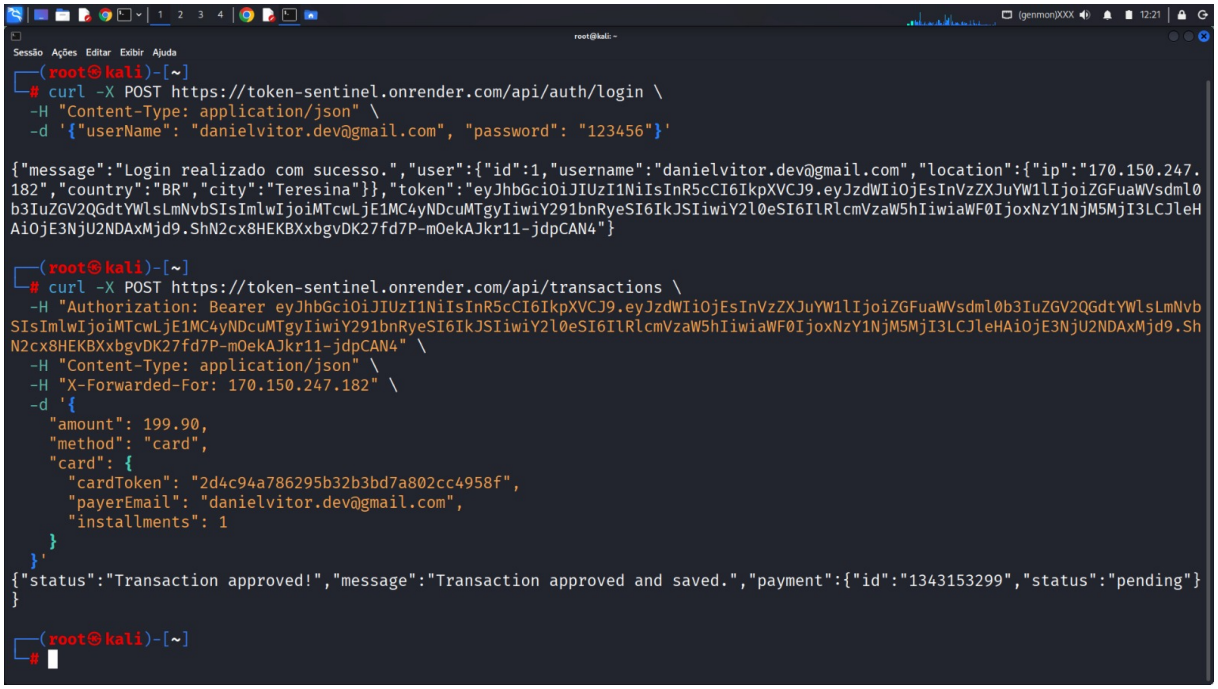
O objetivo foi verificar se a camada de segurança contextual é capaz de interoperar com um *gateway* de pagamento real, processando dados sensíveis de cartão de crédito e impedindo fraudes (*Replay Attacks*) antes que elas gerem prejuízo financeiro.

5.2.1 Cenário A: Transação Legítima (Contexto Válido)

A primeira etapa consistiu em estabelecer o comportamento padrão (linha de base), simulando um usuário legítimo realizando uma compra com cartão de crédito. O processo iniciou-se com o *login* e a subsequente requisição de pagamento partindo do mesmo endereço IP (`170.150.247.182`), situado em Teresina-PI.

A Figura 8 apresenta a resposta do terminal, onde o microsserviço validou o contexto e encaminhou a requisição ao Mercado Pago, retornando o ID do pagamento gerado.

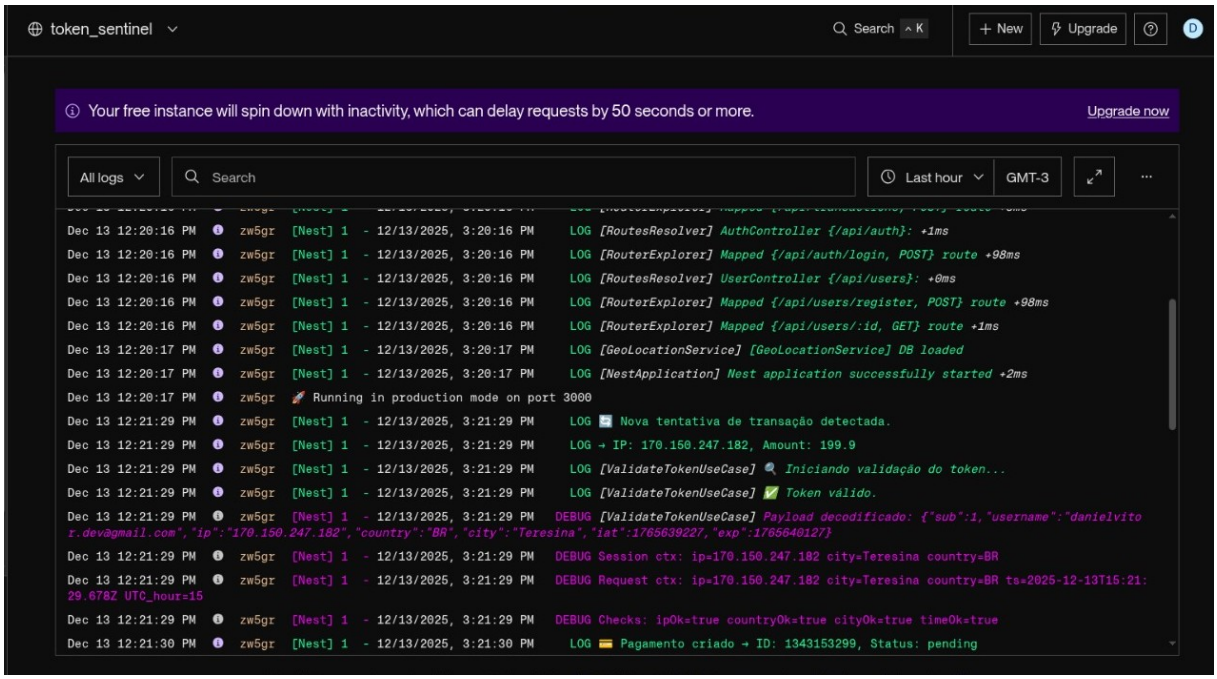
Figura 8 – Sucesso: Transação com cartão de crédito aprovada e registrada no Gateway.



Fonte: O Autor (2025).

Para corroborar a validação interna, a Figura 9 exibe os *logs* do servidor durante o processamento. Nota-se que todas as verificações booleanas de segurança (`ipOk`, `countryOk`, `cityOk`) retornaram `true`, permitindo a comunicação com a API externa.

Figura 9 – Logs do servidor confirmando a validação bem-sucedida do token e criação do pagamento.



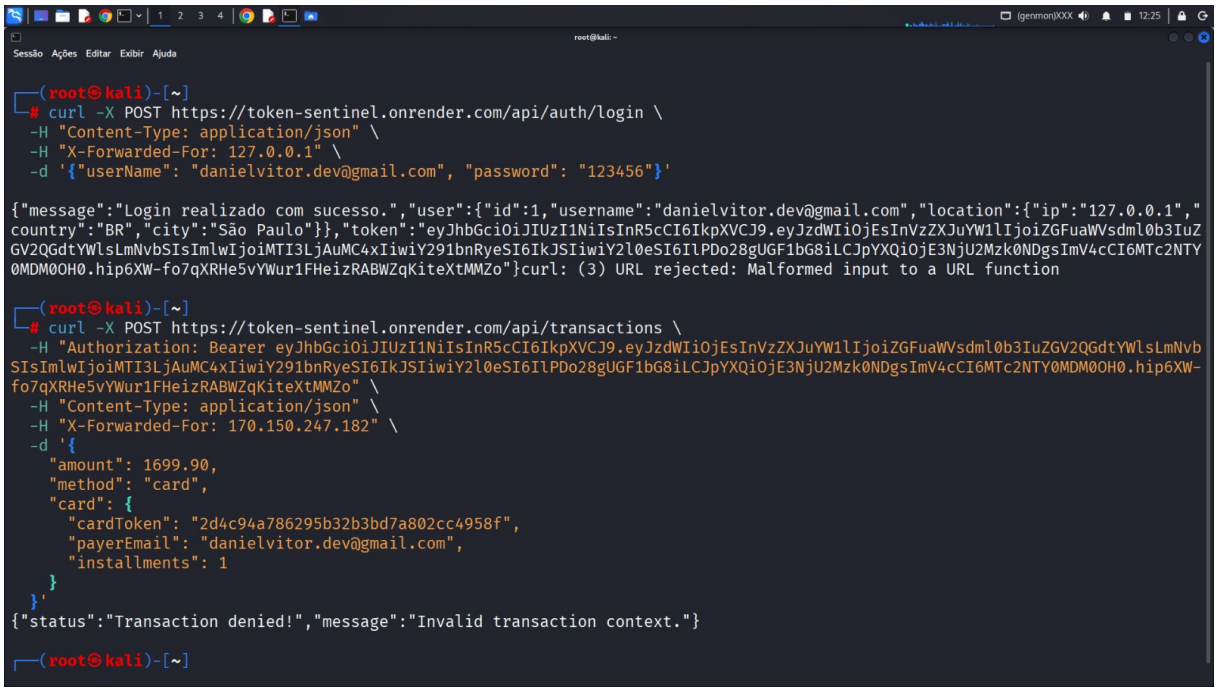
Fonte: O Autor (2025).

5.2.2 Cenário B: Bloqueio de Replay Attack (Contexto Inválido)

Na segunda etapa, simulou-se um ataque de repetição (*Replay Attack*) com alteração de contexto. O cenário reproduz uma situação onde um atacante intercepta um token válido (gerado em São Paulo), mas tenta utilizá-lo para efetuar uma compra a partir de uma localização divergente (Teresina).

A Figura 10 demonstra a reação do microsserviço diante dessa anomalia:

Figura 10 – Bloqueio: Transação negada devido à divergência de contexto (São Paulo vs Teresina).



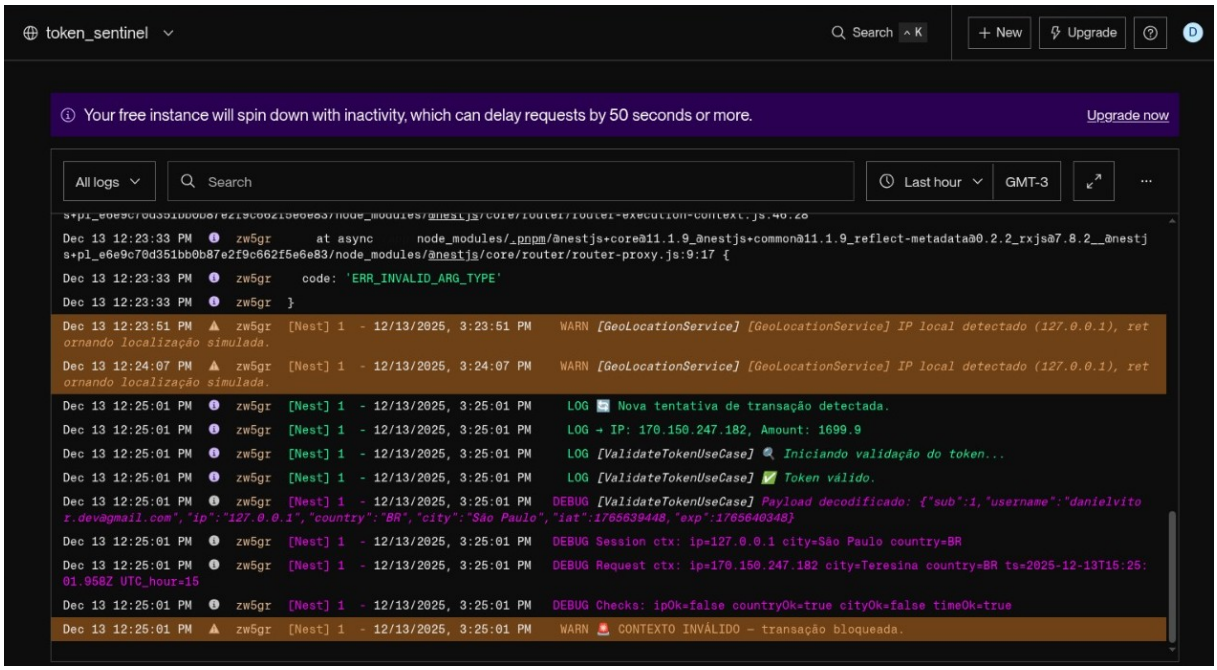
Fonte: O Autor (2025).

A análise técnica do bloqueio revela a eficácia da proteção:

1. **Origem do Token:** O login inicial simulou uma conexão via *localhost* (IP `127.0.0.1`), geolocalizada em **São Paulo - SP**.
2. **Tentativa de Fraude:** A requisição de compra utilizou o mesmo token, mas partiu do IP `170.150.247.182` (**Teresina - PI**).
3. **Interrupção:** O microsserviço detectou a impossibilidade de deslocamento físico e bloqueou a transação com a mensagem *"Invalid transaction context"*, antes mesmo de contatar o Mercado Pago.

A análise dos *logs* de erro (Figura 11) confirma que a divergência geográfica disparou um alerta de segurança (`WARN CONTEXTO INVÁLIDO`).

Figura 11 – Logs de auditoria registrando o bloqueio e a inconsistência geográfica detectada.



Fonte: O Autor (2025).

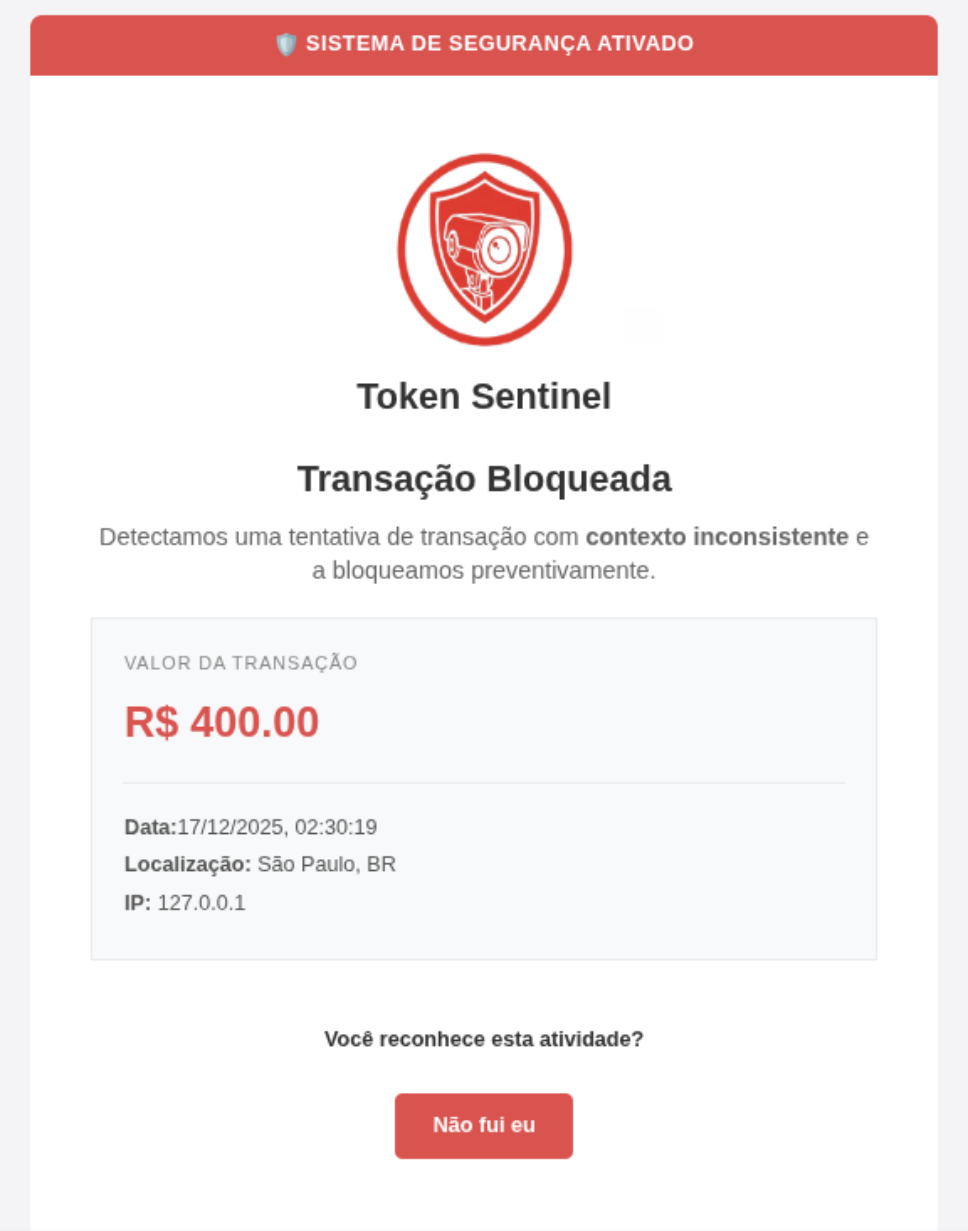
Este resultado demonstra uma vantagem econômica significativa: ao bloquear a fraude internamente, o sistema evita o tráfego desnecessário e possíveis taxas de disputa (*chargeback*) junto ao provedor financeiro.

5.2.3 Cenário C: Notificação de Atividade Suspeita via AWS SES

Como parte integrante da estratégia de defesa em profundidade, o microsserviço foi configurado para disparar notificações automáticas sempre que uma inconsistência crítica de contexto é detectada. Este mecanismo utiliza o serviço **Amazon SES** para garantir a entrega e a integridade do alerta.

A Figura 12 exemplifica o e-mail recebido pelo usuário imediatamente após a tentativa de *Replay Attack* bloqueada no cenário anterior.

Figura 12 – Notificação de segurança enviada ao usuário após detecção de contexto inválido.



Fonte: O Autor (2025).

A eficácia desta abordagem reside nos seguintes pontos observados nos testes:

- **Tempo de Resposta:** O disparo do e-mail ocorreu de forma assíncrona, não impactando a performance do bloqueio, mas chegando à caixa de entrada do usuário em poucos segundos.
- **Conteúdo Transacional:** O alerta contém informações detalhadas, como a geolocalização da tentativa (Teresina-PI) e o horário, permitindo que o usuário identifique prontamente que não foi o autor da requisição.

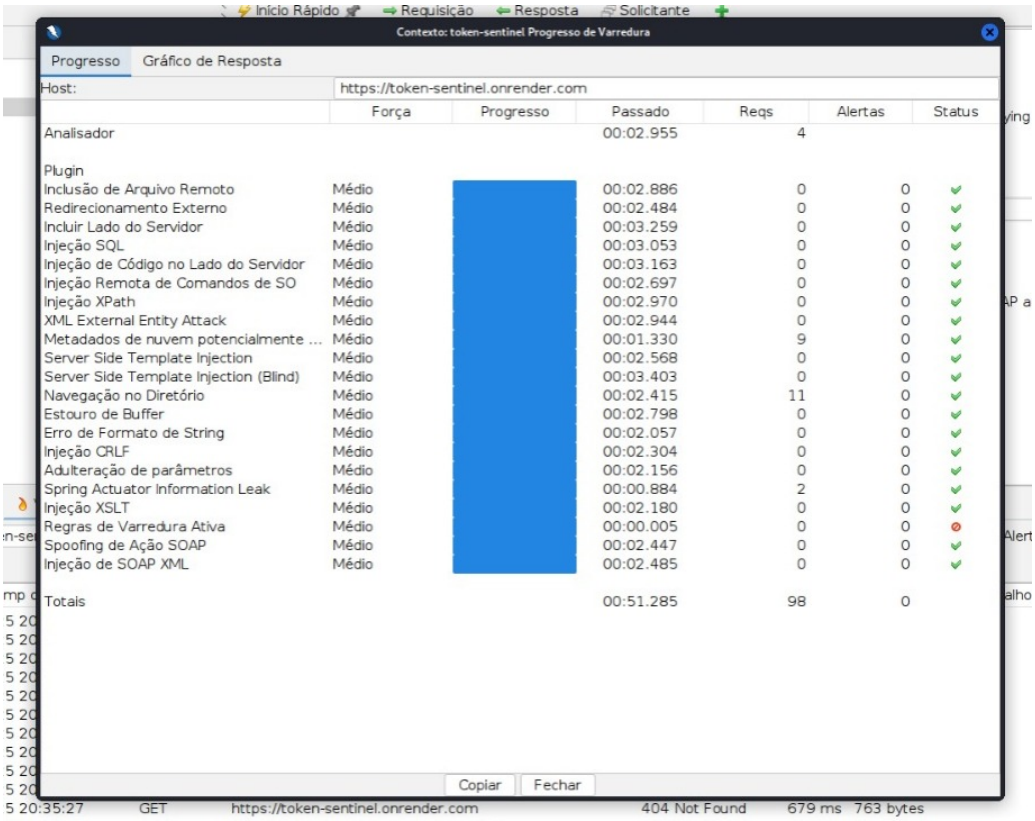
- **Prevenção de Danos:** Além do bloqueio técnico do token, a notificação permite que o usuário tome medidas preventivas, como a alteração de sua senha principal, caso o token tenha sido interceptado devido a uma vulnerabilidade no dispositivo do cliente.

5.3 ANÁLISE DE VULNERABILIDADES COM OWASP ZAP

Para complementar os testes manuais de contexto, foi realizada uma varredura de segurança automatizada utilizando o **OWASP ZAP (Zed Attack Proxy)**. O objetivo desta etapa foi submeter o microsserviço a uma bateria de testes de intrusão (*Active Scanning*) para identificar falhas comuns em aplicações web, conforme definido no *OWASP Top 10*.

A Figura 13 apresenta o progresso e o resumo da varredura realizada no ambiente de homologação (`token-sentinel.onrender.com`).

Figura 13 – Progresso da varredura e análise de plugins do OWASP ZAP.



Fonte: O Autor (2025).

A análise dos resultados detalhados na interface do ZAP revela a eficácia das camadas de segurança implementadas:

- **Plugins de Injeção:** Foram realizados testes exaustivos de Injeção SQL, Injeção de Código no Lado do Servidor, Injeção de Comandos de SO e XSLT. Em todos

os casos, o sistema não apresentou vulnerabilidades, confirmando a robustez do *TypeORM* e da validação de *schemas* do *NestJS*.

- **Segurança de Dados e Entidades:** Testes de *XML External Entity (XXE)* e *Server Side Template Injection (SSTI)* retornaram negativos, demonstrando que o microsserviço trata corretamente entradas complexas de dados.
- **Configuração de Cabeçalhos:** A ausência de alertas de risco alto ou médio indica que os *middlewares* **Helmet** e **CORS** estão configurados corretamente, protegendo a aplicação contra ataques de *Clickjacking* e injeção de *scripts*.
- **Resumo de Alertas:** Conforme observado na coluna "Alertas"da Figura 13, o total de vulnerabilidades críticas identificadas foi zero, validando a resiliência da infraestrutura conteinerizada frente a ferramentas de ataque automatizadas.

Este resultado corrobora que, além de possuir uma lógica de autenticação contextual inovadora, o microsserviço segue as melhores práticas de desenvolvimento seguro (*Secure Coding*), minimizando a superfície de ataque para cibercriminosos.

5.4 CONTRIBUIÇÕES ESPERADAS

O microserviço a ser desenvolvido busca fornecer uma camada adicional de proteção para sistemas de autenticação, utilizando tecnologias já consolidadas (como JWT e Node.js) e abordagens inovadoras, como a validação contextual por geolocalização. A combinação de análise de contexto com respostas automatizadas poderá oferecer uma solução eficaz e adaptável para diferentes tipos de aplicações web, especialmente em ambientes de pagamento eletrônico.

Espera-se, ainda, contribuir para o debate técnico sobre autenticação adaptativa, apresentando uma arquitetura replicável e segura que pode ser aplicada a sistemas bancários, fintechs e plataformas de e-commerce que demandem autenticação sensível ao contexto.

6 CONCLUSÃO

Este trabalho apresentou a proposta de um microserviço de autenticação contextual voltado à segurança de sistemas sensíveis a fraudes, como plataformas de pagamento. A inovação está centrada na geração de tokens dinâmicos sensíveis ao contexto, com destaque para o uso da geolocalização como principal variável de validação.

A arquitetura sugerida baseia-se em uma abordagem modular por meio de microserviços, permitindo maior escalabilidade e manutenção. A tokenização contextual proposta considera variáveis ambientais no momento da transação, restringindo o uso do token a um espaço geográfico e temporal pré-determinado.

É importante ressaltar que os resultados apresentados são fruto de simulações e protótipos visuais, construídos com o objetivo de demonstrar a viabilidade e o funcionamento esperado da solução. Essas representações, baseadas em ferramentas como Figma e fluxogramas teóricos, buscam ilustrar o comportamento do sistema frente a diferentes contextos de acesso, incluindo tentativas de ataques como replay, spoofing e uso indevido de sessões.

Dessa forma, conclui-se que a abordagem proposta tem potencial para fortalecer mecanismos de autenticação tradicionais, contribuindo com uma camada adicional de segurança adaptativa e situacional. Embora os testes reais ainda não tenham sido realizados, os protótipos indicam caminhos promissores para futuras implementações.

7 TRABALHOS FUTUROS

A conclusão deste trabalho abre diversas frentes para a evolução do microsserviço de segurança contextual. Com o avanço das tecnologias de pagamento e a migração massiva das transações para dispositivos portáteis, as propostas de trabalhos futuros focam na expansão da arquitetura para o ambiente móvel e no refinamento da análise de dados comportamentais.

7.1 EXPANSÃO PARA ECOSSISTEMAS MOBILE

A principal vertente para pesquisas futuras consiste na portabilidade e integração nativa do microsserviço em aplicações móveis (iOS e Android). Embora a lógica de geolocalização via IP tenha se mostrado eficaz no ambiente web, o ambiente mobile oferece variáveis ainda mais precisas:

- **Geolocalização via GPS:** A implementação de bibliotecas nativas permitiria que o microsserviço recebesse coordenadas de GPS diretamente do hardware do dispositivo, reduzindo a margem de erro e a suscetibilidade a VPNs (*Virtual Private Networks*) que camuflam o endereço IP.
- **Integração com Biometria Nativa:** O microsserviço poderia ser expandido para exigir a validação de biometria (FaceID ou impressão digital) sempre que o contexto geográfico for identificado como "incomum", criando uma camada de autenticação adaptativa multifator (*Risk-based Authentication*).

7.2 BIOMETRIA COMPORTAMENTAL E INTELIGÊNCIA DE DADOS

Outra oportunidade de evolução reside na inclusão de padrões comportamentais do usuário como variáveis contextuais. Através de técnicas de *Machine Learning*, seria possível mapear os hábitos de consumo e horários habituais de cada cliente.

Dessa forma, o sistema não bloquearia apenas por divergência geográfica absoluta, mas também por comportamentos anômalos dentro de uma localização conhecida, como uma frequência de transações muito acima da média histórica do usuário.

7.3 OTIMIZAÇÃO DE LATÊNCIA E INFRAESTRUTURA

Por fim, sugere-se o estudo de tecnologias de *Edge Computing* para hospedar partes da lógica do microsserviço. Ao aproximar o processamento da validação contextual do local de origem da requisição, seria possível reduzir ainda mais a latência,

garantindo que o sistema de segurança seja praticamente imperceptível para o usuário final, mesmo em redes móveis com oscilações de sinal.

Esta evolução contínua garantirá que a solução proposta permaneça resiliente frente às novas técnicas de fraude, consolidando-se como uma ferramenta essencial na proteção de ecossistemas financeiros digitais.

REFERÊNCIAS

1 KANG, H. et al. Theory and application of zero trust security: A brief survey. *Entropy*, v. 25, n. 12, 2023. ISSN 1099-4300. Disponível em: <https://www.mdpi.com/1099-4300/25/12/1595>. 11, 18

2 LIU, X. et al. Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in psychology*, Frontiers Media SA, v. 13, p. 927398, 2022. Disponível em: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.927398>. 11

3 MURESAN, A. Tokenization techniques and their effect on risk reduction for payment data in serverless e-commerce frameworks. *Nuvern Applied Science Reviews*, v. 4, n. 1, p. 1–12, 2020. Disponível em: <https://nuvern.com/index.php/nasr/article/view/2020-01-04>. 11, 16

4 SAHA, A.; SANYAL, S. Survey of strong authentication approaches for mobile proximity and remote wallet applications-challenges and evolution. *arXiv preprint arXiv:1412.2845*, 2014. Disponível em: <https://arxiv.org/abs/1412.2845>. 12

5 ALABDULATIF, A.; SAMARASINGHE, R.; THILAKARATHNE, N. N. A novel robust geolocation-based multi-factor authentication method for securing atm payment transactions. *Applied Sciences*, MDPI, v. 13, n. 19, p. 10743, 2023. Disponível em: <https://www.mdpi.com/2076-3417/13/19/10743>. 12, 16, 17

6 MENG, L. et al. A continuous authentication protocol without trust authority for zero trust architecture. *China Communications*, IEEE, v. 19, n. 8, p. 198–213, 2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9861234>. 12, 18

7 U.S. Payments Forum / EMVCo. *Payment Tokenization Technical Framework*. 2019. <https://www.emvco.com/emv-technologies/payment-tokenisation/>. White paper disponível no site da U.S. Payments Forum. 16, 24

8 GRANJA, E. N. C. Developing a next-generation tokenization framework to secure digital payments. 2024. Disponível em: <https://doi.org/10.22541/au.172538393.36628865/v1>. 17, 20

9 BIRYUKOV, A.; DINU, D.; KHOVRATOVICH, D. *Argon2: the memory-hard function for password hashing and other applications*. [S.l.], 2015. Acesso em: 13 dez. 2025. Disponível em: <https://password-hashing.net/argon2-specs.pdf>. 26