Departamento de
Informática e Estatística
CTC • UFSC

Análise de segurança do aplicativo KIM: uma abordagem prática em Segurança da Computação

---

Aluna(o): Jessica Regina dos Santos
Matrícula: 22100626
Curso: Ciências da Computação
Disciplina: INE5429 - Segurança em Computação
Professora(or): Thaís Bardini Idalino e Jean Everson Martina
Data de entrega: 25/03/2025

---

1. Objetivo(s)

O objetivo desse relatório é realizar uma análise de segurança do aplicativo KIM, uma plataforma de mobilidade e pagamentos amplamente utilizada no Brasil.

Para isso, abordarei os seguintes aspectos:

- Identificação dos ativos críticos do sistema: determinar os principais recursos, dados e funcionalidades que precisam ser protegidos.
- Análise de possíveis adversários: identificar interessados em atacar o sistema e quais seriam seus motivos.
- Avaliação do gerenciamento de riscos: discutir como o sistema pode identificar, avaliar e mitigar riscos de segurança.
- Propor contramedidas técnicas e não técnicas: sugerir medidas de segurança que possam ser implementadas para proteger o sistema.
- Avaliação do custo/benefício das medidas de segurança: analisar o equilíbrio entre os custos de implementação das medidas de segurança e os benefícios obtidos em termos de proteção e confiabilidade do sistema.

---

2. Introdução

A segurança da informação é um dos pilares fundamentais para o funcionamento confiável de sistemas digitais, especialmente em aplicações que envolvem transações financeiras e dados sensíveis de usuários.

No contexto atual, onde a mobilidade urbana e os pagamentos digitais estão cada vez mais integrados, a proteção desses sistemas contra ameaças cibernéticas torna-se essencial.

O KIM é uma plataforma de mobilidade e pagamentos que oferece soluções inovadoras para a recarga de cartões de transporte, mapeamento de ônibus, pagamento de passagens com QR Code, recarga de celular e outros serviços digitais. Fundada em 2017, a startup já possui mais de 1 milhão de clientes e está presente em mais de 70 cidades do Brasil, destacando-se no mercado de tecnologia de mobilidade por sua praticidade e eficiência (USE KIM, 2025).

No entanto, como qualquer sistema digital, o KIM está sujeito a vulnerabilidades e ataques cibernéticos que podem comprometer a confidencialidade, integridade e disponibilidade dos dados dos usuários. Ataques como vazamento de informações, fraudes financeiras e interrupções de serviço podem não apenas causar prejuízos financeiros, mas também danos à reputação da empresa e à confiança dos usuários (SHOSTACK, 2014).

Nesse contexto, este relatório tem como objetivo realizar uma análise de segurança do aplicativo KIM, identificando seus ativos críticos, possíveis adversários, riscos associados e medidas de proteção.

A análise será embasada nos fundamentos discutidos em aula, como a hierarquia de insegurança e a importância de pensar como um atacante e como um defensor (MARTINA, 2025). Além disso, serão consideradas as melhores práticas de segurança da informação, como a adoção de políticas de segurança, criptografia e autenticação multifator (NIST, 2017).

Ao final, espera-se que esta análise contribua para uma compreensão mais clara dos desafios de segurança enfrentados pelo KIM e ofereça ideias para a melhoria contínua de sua infraestrutura de proteção.

---

3. Descrição do sistema

O KIM é uma plataforma digital que oferece soluções integradas para mobilidade urbana e pagamentos, visando simplificar a rotina dos usuários no transporte público e em transações cotidianas (USE KIM, 2025).

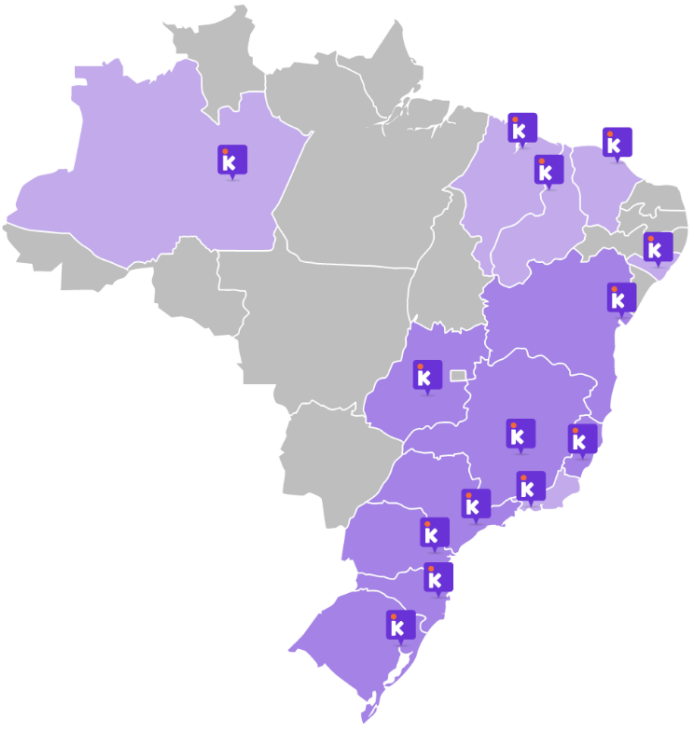

Imagem 1. Estados onde o aplicativo KIM está presente.

Com o lançamento recente do KIM 2.0, a plataforma passou por uma série de melhorias e atualizações, incluindo uma interface mais intuitiva, novas funcionalidades e maior integração com sistemas de transporte e pagamento. Essa versão reforça o compromisso da empresa com a inovação e a segurança, buscando oferecer uma experiência ainda mais eficiente e segura para os usuários (USE KIM, 2025).

Imagem 2. Front-end da nova versão do aplicativo.

3.1 Principais funcionalidades do KIM 2.0

- Gerenciamento de cartões: permite que os usuários visualizem e gerenciem seus cartões de transporte, tanto físicos quanto virtuais. Os cartões físicos são os tradicionais utilizados no dia a dia, enquanto os cartões virtuais geram QR Codes para pagamento em linhas que aceitam essa forma de pagamento (USE KIM, 2025).

Imagem 3. Área destinada ao gerenciamento de cartões no aplicativo KIM.

- Recarga de cartões: os usuários podem recarregar seus cartões de transporte diretamente pelo aplicativo, eliminando a necessidade de deslocamento até pontos físicos de recarga. O saldo é validado no próprio ônibus, garantindo praticidade e agilidade (USE KIM, 2025).

Imagem 4. Área destinada à recarga de cartões no aplicativo KIM.

- Geração de QR code: o aplicativo permite a geração de QR Codes para pagamento de passagens, oferecendo uma alternativa moderna e segura aos métodos tradicionais de pagamento (USE KIM, 2025).

Imagem 5. Área destinada à geração de QR Codes no aplicativo KIM.

- Acompanhamento de pedidos: os usuários podem acompanhar o status de suas recargas e outras transações diretamente no aplicativo (USE KIM, 2025).

Imagem 6. Área destinada ao acompanhamento no aplicativo KIM.

- Consulta de linhas e paradas: são fornecidas informações atualizadas sobre rotas, horários e paradas de ônibus, ajudando os usuários a planejar seus deslocamentos de forma eficiente (USE KIM, 2025).

Imagem 7. Área destinada a consulta de linhas e paradas no aplicativo KIM.

- Recarga de celular pré-pago: além dos serviços de transporte, o aplicativo também permite a recarga de créditos para celulares pré-pagos (USE KIM, 2025).

Imagem 8. Área destinada à recarga de pré-pagos no aplicativo KIM.

- KIM Shop: o aplicativo também oferece acesso ao Kim Shop, onde os usuários podem encontrar descontos e promoções em parceria com outras empresas (USE

KIM, 2025).

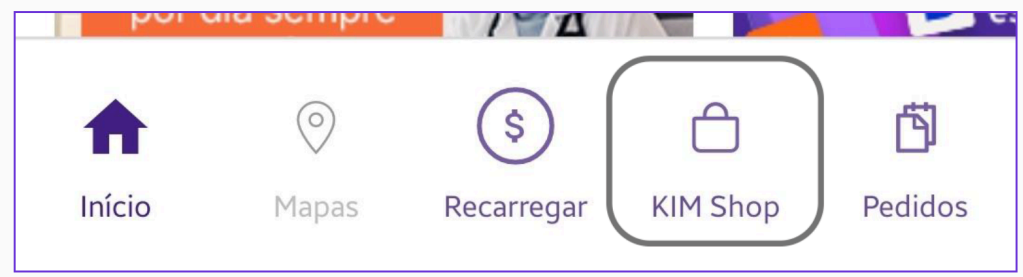

Imagem 9. Área destinada à KIM Shop.

3.2 Estrutura e Tecnologia

O KIM 2.0 opera por meio de um aplicativo móvel disponível para dispositivos Android e iOS, com uma interface redesenhada e funcionalidades de fácil acesso. A plataforma utiliza tecnologias modernas, como APIs de integração com sistemas de transporte e gateways de pagamento seguros, para garantir uma experiência fluida e confiável aos usuários. Além disso, o KIM 2.0 conta com uma infraestrutura de nuvem para armazenamento e processamento de dados, o que permite escalabilidade e alta disponibilidade do serviço (USE KIM, 2025).

No entanto, essa dependência de tecnologias digitais também expõe o sistema a riscos de segurança, como vazamento de dados e ataques cibernéticos (MARTINA, 2025).

3.3 Importância no contexto de Mobilidade Urbana

Aplicativos com o KIM desempenham um papel importante na melhoria da mobilidade urbana, especialmente em grandes cidades onde o transporte público é essencial para a locomoção diária. Ao oferecer soluções práticas e inovadoras, o aplicativo contribui para a otimização do tempo e a redução de custos para os usuários, além de promover a inclusão digital e financeira (USE KIM, 2025).

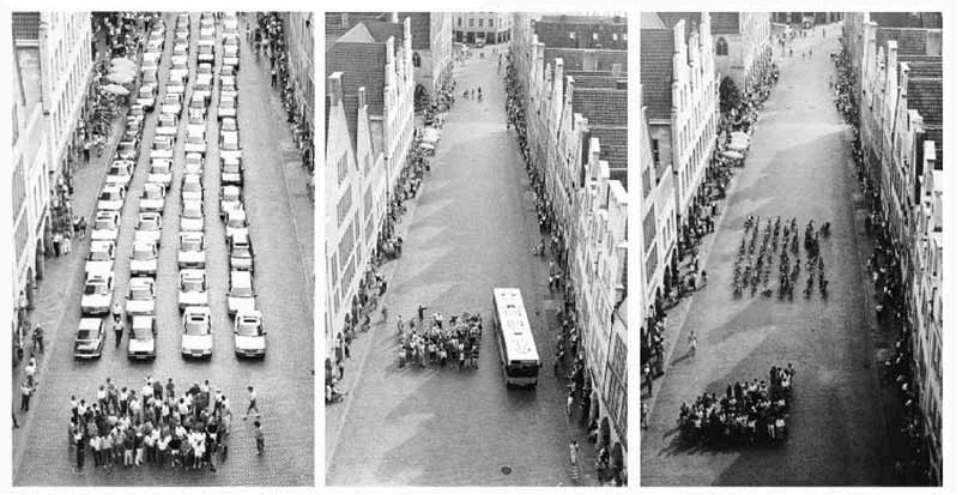

Imagem 10. Em 1990, o programa "Cidade amiga das bicicletas" da cidade de Müenster produziu uma imagem que virou um ícone da luta por melhorias na mobilidade urbana. A clássica imagem comparou os espaços ocupados para transportar 72 indivíduos em 60 carros, em um ônibus ou em 72 bicicletas. Fonte.

No entanto, a crescente dependência de sistemas digitais como este também traz desafios significativos em termos de segurança da informação. A proteção dos dados dos usuários e a garantia da continuidade dos serviços são aspectos críticos que demandam atenção constante e investimentos em medidas de segurança robustas (SHOSTACK, 2014).

---

4. Ativos

"E o que são ativos?". Os ativos são os recursos, dados e funcionalidades de um sistema que possuem valor e, portanto, precisam ser protegidos contra ameaças e vulnerabilidades.

No caso do aplicativo, seus ativos podem ser categorizados em três grupos principais: dados dos usuários, infraestrutura tecnológica e funcionalidades críticas. Sigamos a tabela abaixo:

Tabela 1: Categorização de ativos (Segurança e Infraestrutura do KIM 2.0)	
Categoria	**Descrição**
Dados dos usuários	-
Dados pessoais	Coleta nome, CPF, e-mail, endereço e telefone para a criação e gerenciamento de contas. São altamente sensíveis.
Dados de pagamento	Permite a recarga de cartões de transporte e celulares, o que envolve o armazenamento de informações financeiras, como números de cartão de crédito e dados de transações.

Tabela 1: Categorização de ativos (Segurança e Infraestrutura do KIM 2.0)	
	Armazenam informações financeiras, exigindo criptografia.
Histórico de uso	Armazena o histórico de viagens, recargas e transações dos usuários. Esses dados podem ser utilizados para personalizar a experiência do usuário, mas também representam um risco se forem acessados por terceiros não autorizados.
Infraestrutura Tecnológica	-
Servidores e Banco de Dados	Dependência de uma infraestrutura de servidores e bancos de dados para armazenar e processar informações. A proteção desses sistemas é essencial para garantir a disponibilidade e a integridade dos dados.
APIs de Integração	Utiliza APIs para se integrar com sistemas de transporte e gateways de pagamento. Estes, são pontos críticos que podem ser explorados por atacantes se não forem devidamente protegidos.
Aplicativo Móvel	O aplicativo em si é um ativo importante, pois é a interface principal entre o usuário e o sistema. Vulnerabilidades no código do aplicativo podem ser exploradas para obter acesso não autorizado aos dados dos usuários.
Funcionalidades Críticas	-
Recarga de Cartões	Funcionalidade essencial para o funcionamento do aplicativo. Qualquer interrupção ou comprometimento dessa funcionalidade pode causar prejuízos financeiros e danos à reputação da empresa.
Geração de QR Code	A geração de QR Codes para pagamento de passagens é uma funcionalidade inovadora porém, representa um risco se os códigos forem interceptados ou falsificados.

Tabela 1: Categorização de ativos (Segurança e Infraestrutura do KIM 2.0)	
Consulta de Linhas e Paradas	Funcionalidade crítica para a experiência do usuário. A disponibilidade e a precisão dessas informações são essenciais para a confiança no sistema.

---

5. Adversários

Adversários são os indivíduos ou grupos que podem tentar explorar vulnerabilidades em sistemas para obter benefícios próprios ou causar danos. Eles podem variar desde hackers individuais até grupos organizados, e seus motivos podem ser financeiros, políticos, ou até mesmo pessoais.

“E quem são eles?”. Podemos analisar como diferentes perfis de atacantes poderiam representar ameaças específicas, já que cada categoria apresenta riscos distintos que merecem atenção:

Indícios sugerem que atacantes com habilidades básicas podem representar um risco potencial. Esses indivíduos, muitas vezes movidos por curiosidade ou busca de reconhecimento, tendem a utilizar ferramentas pré-existentes para explorar vulnerabilidades conhecidas. Um caso que ilustra essa possibilidade ocorreu em 2023, quando indivíduos exploraram falhas em um sistema de transporte similar (TECH CRUNCH, 2023). Embora seu impacto possa ser limitado, sistemas com proteções básicas insuficientes podem ser afetados.

Também existem relatos de que organizações criminosas focadas em ganhos financeiros podem direcionar seus esforços para aplicativos de transporte. Esses grupos possuem capacidades técnicas mais sofisticadas, utilizando métodos como *ransomware* e *phishing*. Um exemplo recente foi o ataque do grupo *Anonymous* ao sistemas de transporte público de Tbilisi, que resultou em prejuízos financeiros e vazamento de dados (GEORGIAN NEWS, 2025). No entanto, a probabilidade de tal ataque dependeria da percepção do KIM como um alvo lucrativo.

Empresas concorrentes também podem considerar o uso de táticas agressivas. Isso poderia envolver desde espionagem até ataques diretos para interromper serviços. Um incidente em 2008, onde uma empresa foi supostamente acusada de sabotar concorrentes (ABC NEWS, 2009), sugere que esse risco não pode ser totalmente descartado, especialmente em mercados competitivos.

Alguns grupos também podem ver o KIM como um alvo potencial para protestos ou chamar atenção para causas específicas. Esses atores costumam empregar táticas como DDoS ou vazamento de dados. O histórico de ações do grupo *Anonymous* contra sistemas de transporte

(THE GUARDIAN, 2011) indica que esse tipo de ameaça, embora menos comum, pode ocorrer em contextos de tensão social ou política.

Imagem 11. Emblema comumente associado ao grupo hacker Anonymous. O "homem sem cabeça" representa o anonimato e a organização sem líder.

Também devemos levar em consideração que funcionários ou ex-funcionários com acesso privilegiado podem, em tese, representar um risco significativo. Casos como o de 2023, onde um colaborador vendeu dados de usuários (JAKARTA GLOBE, 2023), mostram que essa possibilidade de ataque existe, mas sua materialização depende de fatores como controles internos e clima organizacional.

Embora menos provável para um aplicativo de transporte, não se pode ignorar completamente a possibilidade de ataques patrocinados por nações-estado. Esses atores, com recursos avançados, poderiam mirar o KIM como parte de operações maiores, como demonstrado por incidentes em outros países (THE KYIV INDEPENDENT, 2024). No entanto, o risco real precisaria ser avaliado considerando o perfil estratégico do aplicativo.

---

6. Gerenciamento de Riscos e suas Contramedidas

O gerenciamento de riscos é um processo essencial para identificar, avaliar e mitigar os riscos associados ao sistema. Ele envolve a análise de possíveis ameaças, a avaliação de sua probabilidade e impacto, e a implementação de medidas para reduzir ou eliminar esses riscos (KAPLAN, 1981).

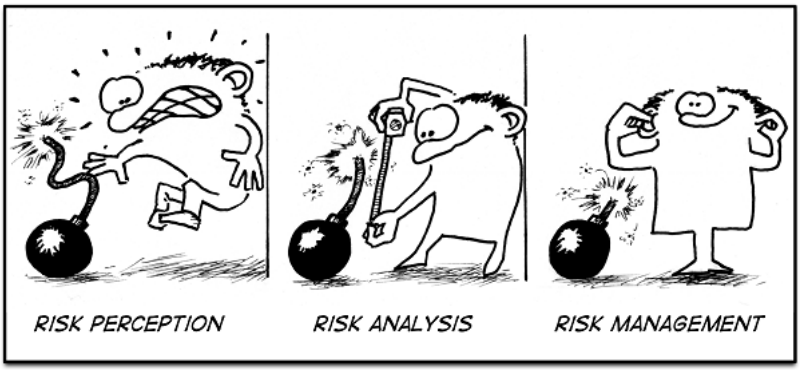

Imagem 12. Fundamentos da gestão de riscos. Fonte.

As contramedidas são as ações e tecnologias implementadas justamente para proteger sistemas contra ameaças e vulnerabilidades. Elas podem ser técnicas (como criptografia e firewalls) ou não técnicas (como políticas de segurança e treinamento de funcionários) (PFLEEGER, 2015).

Abaixo está uma tabela com os principais riscos associados ao KIM 2.0 e possíveis contramedidas:

Tabela 2: Riscos e Estratégias de Mitigação (contramedidas) para o sistema

Risco	Descrição	Probabilidade	Impacto	Estratégias de Mitigação
Vazamento de dados dos usuários	Dados sensíveis (pessoais/financeiros) podem ser acessados por hackers.	Alta	Crítico	- Criptografia de ponta a ponta. - Auditorias regulares de segurança. - Conformidade com a LGPD (MARTINA, 2025).
Ataques Ransomware	Dados criptografados com exigência de resgate para liberação.	Média	Alto	- Backups seguros e regulares. - Detecção de ameaças em tempo real. - Treinamento de funcionários (SHOSTACK, 2014)..
Interrupção do Serviço (DDoS)	Ataque sobrecarrega servidores,	Média	Alta	- Proteção contra DDoS (CLOUDFLARE),

Tabela 2: Riscos e Estratégias de Mitigação (contramedidas) para o sistema				
	tornando o aplicativo indisponível.			2023). - Monitoramento contínuo da rede (NIST, 2017).
Fraudes e uso indevido do sistema	Recargas falsas ou uso indevido de cartões virtuais.	Média	Moderado	- Autenticação de dois fatores (2FA) (NIST, 2017). - Algoritmos de detecção de fraudes (IBM, 2023). - Educação dos usuários (SHOSTACK, 2014).
Vulnerabilidades no código do aplicativo	Falhas no código permitem acesso não autorizado.	Alta	Crítico	- Revisões de código e testes de segurança (OWASP, 2024). - Desenvolvimento seguro (MARTINA, 2025). - Atualizações contínuas de patches (NIST, 2017).

6.1 Recomendações de contramedidas para o sistema (estudo de caso)

Para fortalecer a segurança de um sistema como o do KIM 2.0, algumas contramedidas poderiam ser implementadas:

Uma das primeiras medidas recomendadas seria a implementação de criptografia robusta para proteção de dados, conforme orientado por NIST (2017). Em um cenário ideal, todos os dados sensíveis deveriam ser criptografados tanto em trânsito quanto em repouso, utilizando algoritmos modernos. Isso significa que mesmo em caso de violação de dados, as informações permanecerão ilegíveis sem as chaves de descriptografia adequadas.

A adoção de autenticação multifator (MFA) representaria outro avanço significativo na segurança. Além do tradicional login com senha, o sistema poderia solicitar um segundo fator de autenticação, como um código temporário enviado por SMS ou gerado em um aplicativo autenticador, seguindo as melhores práticas descritas por Stallings e Brown (2018).

Para proteção da infraestrutura, a implementação de firewalls e sistemas de detecção/prevenção de intrusões (IDS/IPS) seria altamente recomendável. Essas soluções poderiam monitorar constantemente o tráfego de rede, identificando e bloqueando padrões suspeitos de atividade que poderiam indicar tentativas de ataque.

A criação e aplicação de políticas de segurança e privacidade claras e abrangentes seria fundamental, com especial atenção ao cumprimento da LGPD (BRASIL, 2018). Essas políticas deveriam definir procedimentos padrão para o tratamento de dados sensíveis. Por fim, a realização de treinamentos de conscientização em segurança para os envolvidos no projeto completaria o conjunto de recomendações. Essas capacitações ajudariam a equipe a reconhecer e evitar ameaças comuns, como as tentativas de *phishing* (tentativas de fraude online onde criminosos se passam por instituições confiáveis para roubar dados pessoais).

6.1 Pensando como um atacante: e se alguém mal intencionado atacasse o KIM?

Atualmente, um dos principais riscos identificados está relacionado ao processo de autenticação. Se não forem implementados mecanismos robustos, como autenticação multifator ou políticas de senha fortes, um atacante poderia realizar ataques de força bruta (utilizando ferramentas como a *Hydra*, por exemplo, para testar combinações de usuário e senha) ou *Credential stuffings*, aproveitando credenciais vazadas em outros vazamentos de dados (OWASP, 2023), comprometendo contas de usuários e possíveis fraudes financeiras.

Além disso, há possíveis vulnerabilidades na geração de QR Codes. O uso de QR Codes para validação de bilhetes apresenta riscos se não houver validação segura no servidor. Um atacante poderia gerar QR Codes falsos, por exemplo, redirecionando usuários para páginas maliciosas, além de explorar falhas na leitura do código para burlar o sistema de cobrança (KOTVAL, 2025).

Também há a possibilidade de existirem vulnerabilidades na funcionalidade de recarga, a mais importante do sistema como um todo. Se a interface de recarga não for protegida, um atacante poderia realizar recargas fraudulentas explorando falhas na API, ou pior, roubar dados de cartões de crédito em transações inseguras, gerando perdas financeiras diretas e aumento de fraudes. Consequentemente, se a consulta de saldo não for protegida adequadamente, um atacante também poderia acessar saldos explorando falhas (CSO ONLINE, 2016), violando o direito de privacidade do cliente.

7. Análise de custo-benefício em Segurança Cibernética: vale a pena investir?

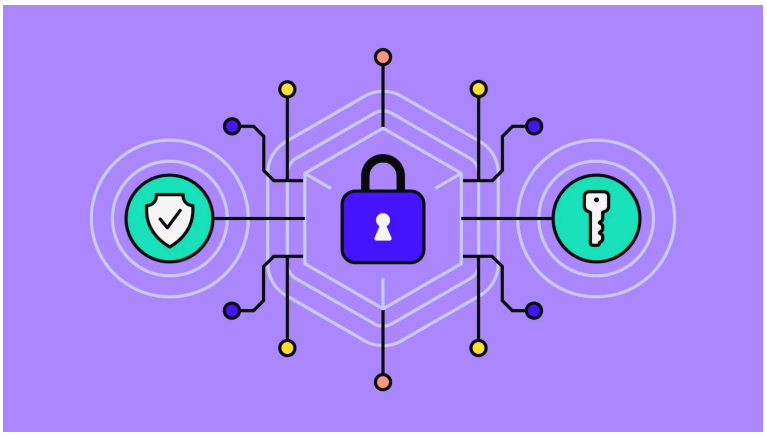

Imagem 13. Do Enigma ao AES-256: como a criptografia evoluiu para blindar sua vida digital. Fonte.

A segurança cibernética não é um luxo, mas uma necessidade em aplicativos como o KIM que lida com dados sensíveis e transações financeiras. As medidas discutidas aqui formam nada mais que um ecossistema de defesa. Implementá-las demandará recursos, porém o custo da inação é incalculável, ainda mais para um aplicativo que lida com dados de milhares de usuários diariamente.

7.1 Criptografia

Seria como um cofre digital. A criptografia transforma dados em códigos indecifráveis, protegendo informações mesmo que caiam em mãos erradas. Implementá-la exige conhecimento técnico, e, embora o investimento inicial possa ser significativo, o retorno é claro. Além de evitar multas pesadas da LGPD, a criptografia fortalece a confiança dos usuários. Um vazamento de dados não só gera prejuízos financeiros, mas também mancha a reputação de uma empresa e recuperar a confiança do público pode custar muito mais do que a proteção antecipada.

7.2 Autenticação de Dois Fatores (2FA)

Senhas são frágeis e basta um vazamento em outro serviço para que criminosos testem as mesmas credenciais em diversos sistemas. A 2FA adiciona uma segunda barreira, exigindo um código temporário ou biometria além da senha. Para um aplicativo de transporte, onde usuários recarregam créditos regularmente, essa camada extra de segurança pode significar a diferença entre um serviço confiável e um alvo constante de fraudes.

7.3. Firewalls e Detecção de Ameaças

Um firewall age como um guarda-costas digital, filtrando acessos suspeitos antes que cheguem ao sistema. Já um IDS (Sistema de Detecção de Intrusões) funciona como um alarme, alertando sobre atividades anormais em tempo real. A configuração dessas

ferramentas demanda manutenção contínua, mas o preço da negligência pode ser enorme. Um ataque bem-sucedido pode derrubar o aplicativo, interrompendo serviços e paralisando operações. Algo que, em um sistema de transporte público, afetaria milhares de pessoas diariamente.

7.4 Atualizações

Muitos ataques exploram falhas antigas, já corrigidas em versões mais recentes. Negligenciar atualizações seria como deixar uma porta aberta para invasores. É preciso uma equipe dedicada para testar e aplicar atualizações sem afetar a experiência do usuário, o que custa caro. Mas o risco de não fazer isso é ainda maior, já que uma falha não corrigida às vezes pode ser a brecha que derruba todo o sistema.

7.5 Políticas de Segurança

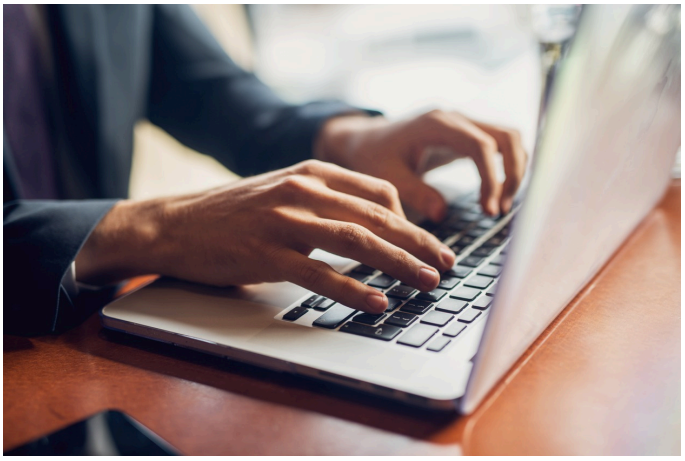

Imagem 14. A tecnologia sozinha não protege.

De nada adiantam firewalls e criptografia se um funcionário clicar em um link malicioso e vazar informações importantes sem querer.

Humanos continuam sendo o alvo preferido de hackers, logo, treinar equipes para reconhecer golpes é essencial.

Políticas claras de segurança e privacidade são a base de uma defesa eficiente. Elas orientam desde a forma como os dados são armazenados até como os colaboradores devem agir em caso de suspeita de ataque. Implementá-las exige tempo e, muitas vezes, consultoria especializada, mas o maior benefício é a criação de uma mentalidade preventiva em toda a organização.

---

8. Resultados

Após a análise de segurança do sistema, entre os principais resultados obtidos estão:

- Identificação de ativos críticos: os dados dos usuários (pessoais e financeiros), a infraestrutura tecnológica (servidores, APIs e aplicativo móvel) e as funcionalidades críticas (recarga de cartões e geração de QR Codes) foram classificados como os ativos mais valiosos e sensíveis do sistema.
- Perfil dos adversários: foram identificados diferentes perfis de atacantes, desde hackers individuais até grupos organizados, com motivações diversas.
- Riscos prioritários: vazamento de dados, ataques de ransomware, interrupção de serviços (DDoS), fraudes e vulnerabilidades no código foram os riscos mais críticos, com probabilidade e impacto elevados.
- Contramedidas propostas: foram sugeridas medidas como criptografia robusta, autenticação multifator (MFA), firewalls, sistemas de detecção de intrusões (IDS/IPS), políticas de segurança e treinamentos de conscientização.

---

9. Discussão

Os resultados destacaram a necessidade de um enfoque proativo na segurança do KIM, alinhado às melhores práticas de segurança da informação.

Implementação de criptografia e MFA pode reduzir significativamente os riscos de vazamento de dados e acesso não autorizado; no entanto, é essencial avaliar o equilíbrio entre segurança e usabilidade, garantindo que as medidas não prejudiquem a experiência do usuário.

Ferramentas como IDS/IPS e firewalls exigem manutenção contínua, o que pode representar um custo adicional para a empresa.

A conscientização de funcionários e usuários é tão crucial quanto às soluções técnicas.

Por fim, embora as medidas de segurança demandem investimento, o custo de um ataque bem-sucedido (multas, perda de reputação, interrupção de serviços) pode ser muito maior. A análise demonstra que a proteção antecipada é um investimento estratégico.

---

10. Conclusão

A segurança do aplicativo KIM é fundamental para garantir a confiança dos usuários e a sustentabilidade do negócio. Este relatório evidenciou que, embora o sistema ofereça funcionalidades inovadoras e úteis, ele está exposto a ameaças cibernéticas significativas.

A implementação das contramedidas propostas pode fortalecer a resiliência do sistema contra ataques. Além disso, a adoção de uma cultura organizacional focada em segurança é essencial para mitigar riscos humanos.

Em um cenário onde a mobilidade urbana e os pagamentos digitais estão em constante crescimento, a segurança não pode ser negligenciada. Com essas ações, o KIM estará melhor preparado para enfrentar os desafios de segurança do ambiente digital atual.

---

11. Referências bibliográficas

ABC NEWS. **Rubert Murdoch Firm Goes on Trial for Alleged Tech Sabotage.** 2009. Disponível em: <https://abcnews.go.com/Technology/story?id=4694808&page=1>. Acesso em: 24 mar. 2025.

BRASIL. **Lei Geral de Proteção de Dados (LGPD).** Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br>. Acesso em: 24 mar. 2025.

CLOUDFLARE. **O que é ataque de DDoS?** Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/>. Acesso em: 24 mar. 2025.

COLEMAN, Gabriella. **Gabriella Coleman on Anonymous.** Brian Lehrer Live, 9 fev. 2011. Disponível em: <https://vimeo.com/19806469>. Acesso em: 24 mar. 2025.

CSO ONLINE. **App developers not ready for iOS transport security requirements.** 2016. Disponível em: <https://www.csoonline.com/article/559113/app-developers-not-ready-for-ios-transport-security-requirements.html>. Acesso em: 24 mar. 2025.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). **Ransomware Guide.** 2023. Disponível em: <https://www.cisa.gov>. Acesso em: 24 mar. 2025.

ENISA. **Privacy and data protection in mobile applications.** 2018. Disponível em: <https://www.enisa.europa.eu>. Acesso em: 24 mar. 2025.

GEORGIAN NEWS. Cyberattack on public transport in Tbilisi. 2025. Disponível em: <https://www.youtube.com/watch?v=HbCeH-bWVgk>. Acesso em: 25 mar. 2025.

IBM. **Fraud Detection and Prevention.** Disponível em: <https://www.ibm.com/fraud-prevention>. Acesso em: 24 mar. 2025.

JAKARTA GLOBE. **Man Arrested for Selling Internet Banking Customers' Data to Dark Website.** 2023. Disponível em: <https://jakartaglobe.id/news/man-arrested-for-selling-internet-banking-customers-data-to-dark-website>. Acesso em: 24 mar. 2025.

KAPLAN, S.; GARRICK, B. J. **On The Quantitative Definition of Risk.** Risk Analysis, v. 1, n. 1, 1981. Disponível em:

<https://www.risksciences.ucla.edu/archive-publications/2015/1/22/on-the-quantitative-definition-of-risk>. Acesso em: 24 mar. 2025.

KOTVAL, Liliana. **Be Aware – QR Codes Have Become a Vector for Phishing Attacks.** 2023. Disponível em: <https://cybersecforum.eu/2023/12/13/be-aware-qr-codes-have-become-a-vector-for-phishing-attacks/>. Acesso em: 24 mar. 2025.

MARTINA, Jean Everson. **Noções Básicas de Segurança.** Slides da disciplina INE5429 – Segurança em Computação. UFSC, 2025.

MARTINA, Jean Everson. **Aspectos Legais e Éticos.** Slides da disciplina INE5429 – Segurança em Computação. UFSC, 2025.

NIST. **Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management.** 2017. Disponível em: <https://doi.org/10.6028/NIST.SP.800-63b>. Acesso em: 24 mar. 2025.

OWASP. **OWASP Top Ten.** 2024. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 24 mar. 2025.

PFLEEGER, C. P.; PFLEEGER, S. L. **Security in Computing.** 5. ed. Pearson, 2015.

SHOSTACK, Adam. **Threat Modeling: Designing for Security.** Wiley, 2014.

STALLINGS, W.; BROWN, L. **Computer Security: Principles and Practice.** 4. ed. Pearson, 2018.

TECH CRUNCH. **Bugs in transportation app Moovit gave hackers free rides.** 2023. Disponível em: <https://techcrunch.com/2023/08/13/moovit-transportation-app-moovit-hackers-free-rides/>. Acesso em: 24 mar. 2025.

THE GUARDIAN. **Anonymous hackers breach San Francisco's Bart transport website.** 2011. Disponível em: <https://www.theguardian.com/technology/2011/aug/15/anonymous-hackers-breach-bart-website>. Acesso em: 24 mar. 2025.

THE KYIV INDEPENDENT. **Ukrainian hackers disrupt transport services in Russian cities.** 2024. Disponível em: <https://kyivindependent.com/ministry-ukrainian-hackers-disrupt-payment-system-in-moscow-subway/>. Acesso em: 24 mar. 2025.

USE KIM. **Sobre nós.** Disponível em: <https://usekim.com.br>. Acesso em: 23 mar. 2025.

USE KIM. **Conheça o Kim 2.0.** Disponível em: <https://usekim.com.br/novo-app-kim-2-0/>. Acesso em: 23 mar. 2025.