**Segurança bancária online: uma visão da IA sobre o problema e algumas soluções**

**Por Nathanael Virgílio Andrade Silva com a colaboração do MS COPILOT**

## Introdução

A segurança bancária online é um tema de crescente relevância no cenário atual, especialmente para instituições financeiras como a Caixa Econômica Federal, que desempenha um papel crucial nas políticas sociais do governo brasileiro. A Caixa, ao atender uma vasta parcela da população, incluindo os mais pobres e vulneráveis, enfrenta desafios significativos no combate aos crimes cibernéticos. Estes crimes, que têm se tornado cada vez mais sofisticados, representam uma ameaça constante tanto para os clientes quanto para a própria instituição.

Os crimes cibernéticos no setor bancário incluem uma variedade de práticas ilícitas, como phishing, malware e ataques de engenharia social, que visam roubar informações pessoais e financeiras dos clientes. A vulnerabilidade dos clientes da Caixa é exacerbada pela falta de conhecimento sobre medidas de segurança digital e pela confiança excessiva em comunicações aparentemente legítimas. Segundo um relatório recente, houve um aumento de 45% nos ataques cibernéticos direcionados a instituições financeiras no Brasil nos últimos dois anos[1].

Os prejuízos causados por esses crimes são múltiplos e profundos. Financeiramente, a Caixa enfrenta perdas significativas devido a fraudes e reembolsos necessários para compensar os clientes afetados. Além disso, a imagem e a reputação da instituição são gravemente prejudicadas, resultando em uma perda de confiança por parte do público. Para os clientes, os impactos vão além das perdas financeiras. A experiência de ser vítima de um crime cibernético pode causar estresse psicológico, ansiedade e uma sensação de vulnerabilidade contínua.

Portanto, é imperativo que a Caixa Econômica Federal implemente políticas robustas de segurança online, não apenas para proteger seus ativos, mas também para garantir a segurança e o bem-estar de seus clientes. A adoção de tecnologias avançadas de segurança, aliada a programas de educação digital para os clientes, pode mitigar os riscos e fortalecer a confiança na instituição. Estudos indicam que instituições que investem em segurança cibernética e educação digital conseguem reduzir significativamente a incidência de fraudes e melhorar a satisfação dos clientes[2].

## Cenário Atual dos Crimes Virtuais

Os crimes virtuais têm evoluído rapidamente, acompanhando o avanço tecnológico e a crescente digitalização dos serviços financeiros. O cenário atual dos crimes virtuais é alarmante, com um aumento significativo na frequência e sofisticação dos ataques. Entre as principais ocorrências estão o phishing, ransomware, vazamentos de dados e ataques de engenharia social

Entre os tipos mais comuns de crimes cibernéticos estão:

1. **Phishing**: Ataques que utilizam e-mails, mensagens de texto ou sites falsos para enganar os usuários e obter informações sensíveis, como senhas e dados bancários.
2. **Ransomware**: Software malicioso que criptografa os dados da vítima e exige um resgate para restaurar o acesso.
3. **Vazamentos de Dados**: Incidentes em que informações pessoais e financeiras são expostas ou roubadas, muitas vezes devido a falhas de segurança.
4. **Ataques de Engenharia Social**: Técnicas que manipulam as pessoas para que revelem informações confidenciais ou realizem ações que comprometam a segurança, dentre outros

Os prejuízos causados por esses crimes são imensos. Em 2021, o Brasil registrou mais de 3,8 milhões de ataques de ransomware, com danos estimados em US$ 20 bilhões globalmente[3]. Além disso, houve mega vazamentos de dados, incluindo um incidente em que mais de 223 milhões de CPFs foram expostos[3]. Esses crimes resultam em prejuízos financeiros substanciais, perda de dados sensíveis e danos à reputação das instituições afetadas.

Em 2022, estima-se que as perdas globais devido a crimes cibernéticos ultrapassaram US$ 6 trilhões. Além dos prejuízos financeiros diretos, as instituições enfrentam custos adicionais relacionados à recuperação de dados, reforço de segurança e danos à reputação.

## A Caixa Econômica Federal no Mercado Financeiro Nacional

A Caixa Econômica Federal, como uma das principais instituições financeiras do Brasil, desempenha um papel crucial no atendimento a todas as camadas da população. Com uma posição consolidada no mercado financeiro nacional, sustentada por vasta rede de agências e pontos de atendimento, a CAIXA é reconhecida por sua atuação em programas sociais e pelo apoio a iniciativas de inclusão e desenvolvimento sustentável[4]

A instituição, como braço financeiro do governo, atua em diversas políticas públicas, como o Bolsa Família, o Minha Casa Minha Vida e o Auxílio Emergencial, beneficiando milhões de brasileiros[4].

- **Bolsa Família**: Programa de transferência de renda que beneficia milhões de famílias em situação de pobreza e extrema pobreza.
- **Minha Casa Minha Vida**: Programa habitacional que facilita o acesso à moradia para famílias de baixa renda.
- **Auxílio Emergencial**: Benefício concedido durante a pandemia de COVID-19 para apoiar financeiramente trabalhadores informais, microempreendedores individuais e desempregados.

A CAIXA continua a ser uma referência no mercado financeiro brasileiro, não apenas pela sua solidez e abrangência, mas também pelo seu compromisso com a segurança e o bem-estar de seus clientes. A combinação de investimentos em tecnologia e educação digital é essencial

para enfrentar os desafios impostos pelos crimes cibernéticos e garantir a proteção dos ativos e dados dos clientes.

**Investimentos em Segurança**

Nos últimos anos, a CAIXA tem investido significativamente em segurança cibernética para proteger seus clientes e reduzir a vulnerabilidade a ataques. Esses investimentos incluem a adoção de tecnologias avançadas de segurança, tais como as apresentadas abaixo[4]. Esses esforços têm sido fundamentais para mitigar os riscos e fortalecer a confiança dos clientes na instituição.

- **Tecnologias Avançadas de Segurança**: Implementação de sistemas de detecção de intrusões, autenticação multifator, cadastro biométrico massivo e criptografia de dados.
- **Educação Digital**: Programas de conscientização e treinamento para clientes e funcionários sobre práticas seguras online.
- **Parcerias Estratégicas**: Colaboração com empresas de tecnologia e órgãos de segurança para fortalecer a proteção contra ameaças cibernéticas.

Com a adoção destas medias, os resultados têm sido positivos, com uma redução significativa no número de ataques bem-sucedidos e uma maior confiança dos clientes na segurança dos serviços oferecidos pela CAIXA.

## IA – um novo capítulo da evolução humana

A Inteligência Artificial (IA) tem se tornado uma das forças mais transformadoras do mundo atual, impactando profundamente diversos setores da sociedade e da economia. Sua capacidade de processar grandes volumes de dados, aprender com padrões e tomar decisões informadas está remodelando a maneira como vivemos, trabalhamos e interagimos com a tecnologia.

Como uma área da ciência da computação, a IA se dedica ao desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Isso inclui habilidades como aprender, raciocinar, resolver problemas, perceber e tomar decisões. A IA funciona através de várias técnicas e abordagens, que podem ser classificadas em diferentes categorias.

**Principais Técnicas e Abordagens da IA**

1. **Aprendizado de Máquina (Machine Learning)**
    - **Definição**: É uma subárea da IA que permite aos sistemas aprenderem e melhorarem automaticamente com a experiência, sem serem explicitamente programados.

- **Funcionamento**: Utiliza algoritmos para analisar dados, identificar padrões e fazer previsões. Exemplos incluem recomendações de produtos, diagnósticos médicos e previsão de fraudes[5].

2. **Aprendizado Profundo (Deep Learning)**
   - **Definição**: Uma subárea do aprendizado de máquina que utiliza redes neurais artificiais para imitar o funcionamento do cérebro humano.
   - **Funcionamento**: Processa grandes volumes de dados através de várias camadas de redes neurais, permitindo o reconhecimento de padrões complexos, como em imagens e voz[6].
3. **Processamento de Linguagem Natural (NLP)**
   - **Definição**: Técnica que permite às máquinas entenderem e interpretarem a linguagem humana.
   - **Funcionamento**: Utiliza algoritmos para analisar e gerar texto, facilitando a comunicação entre humanos e máquinas. Exemplos incluem chatbots e assistentes virtuais[6].
4. **Visão Computacional**
   - **Definição**: Área da IA que permite às máquinas interpretarem e entenderem o mundo visual.
   - **Funcionamento**: Utiliza algoritmos para processar e analisar imagens e vídeos, permitindo o reconhecimento de objetos, rostos e cenas[6].

**Importância da IA na Vida Moderna**

A IA está presente em diversos aspectos da vida moderna, trazendo benefícios significativos em várias áreas:

1. **Saúde**: A IA está revolucionando a medicina com diagnósticos mais precisos, tratamentos personalizados e avanços na pesquisa médica. Algoritmos de aprendizado de máquina podem analisar grandes conjuntos de dados para identificar padrões que seriam difíceis de detectar por métodos tradicionais, melhorando significativamente os cuidados com a saúde [7].
2. **Educação**: Sistemas de IA estão proporcionando aprendizado personalizado, adaptando o conteúdo de ensino com base no desempenho e nas necessidades individuais dos alunos. Isso não apenas melhora a eficácia do ensino, mas também promove uma educação mais inclusiva [8].
3. **Indústria**: A automação de tarefas repetitivas e processos complexos aumenta a eficiência e reduz custos. Na manufatura, por exemplo, a IA pode otimizar a produção, melhorar a qualidade dos produtos e prever falhas em equipamentos, minimizando o tempo de inatividade[8.]

4. **Entretenimento**: Plataformas de streaming utilizam IA para oferecer recomendações personalizadas de filmes, séries e músicas, melhorando a experiência do usuário e aumentando o engajamento[7]
5. **Segurança**: A IA desempenha um papel crucial na detecção e prevenção de ameaças cibernéticas. Algoritmos de aprendizado de máquina podem analisar padrões de comportamento para identificar atividades suspeitas e proteger sistemas contra ataques, o que é particularmente importante na era digital[8].

No mundo corporativo, a IA se destaca na solução de problemas relacionados à segurança digital. Algumas das principais aplicações incluem:

- **Detecção de Fraudes**: Monitoramento de transações em tempo real para identificar atividades suspeitas.
- **Autenticação Biométrica**: Uso de reconhecimento facial, impressão digital e voz para garantir a segurança dos acessos.
- **Análise de Dados**: Processamento de grandes volumes de dados para identificar padrões e prever ameaças.

A constante evolução da IA e o investimento em tecnologias avançadas são essenciais para enfrentar os desafios do futuro e garantir um ambiente seguro e eficiente para todos.

## Propostas de IA para Segurança Digital Bancária

A aplicação de Inteligência Artificial (IA) na segurança digital bancária tem o potencial de causar um impacto social significativo com a redução dos prejuízos financeiros (direcionando esforços e recursos para outras ações sociais de impacto do banco como inclusão e educação bancária, por exemplo, dentre outros), especialmente para proteger clientes vulneráveis.

Com o aumento dos crimes cibernéticos, a necessidade de proteger dados sensíveis e sistemas críticos nunca foi tão grande. Da mesma forma é preciso garantir a segurança física e emocional dos clientes. A seguir, são apresentadas algumas propostas que utilizam tecnologias existentes e soluções imaginadas para melhorar a segurança digital e física dos clientes.

Algumas propostas com uso da IA:

**1. Detecção de Fraudes em Tempo Real por meio da análise de dados e padrões**

A IA pode ser utilizada para monitorar transações em tempo real e identificar padrões suspeitos que possam indicar fraudes. Algoritmos de aprendizado de máquina podem analisar grandes volumes de dados e detectar anomalias com alta precisão.

Por exemplo, se um cliente que normalmente realiza transações pequenas de repente tenta transferir uma grande quantia de dinheiro, o sistema pode sinalizar essa transação para revisão. Da mesma forma, o monitoramento pode detectar um movimento anormal de sucessivas transferências e saques para contas incomuns normalmente em outras localidades, seja por meio de aplicativos ou meios físicos tais como os terminais de autoatendimento das agências e bancos 24horas.

Outra possibilidade seria o uso para detectar origem de chamadas suspeitas de forma a combater as fraudes por meio da modalidade de “engenharia social”.

**2. Autenticação Biométrica Avançada**

A autenticação biométrica, como reconhecimento facial, impressão digital e reconhecimento de voz, pode ser integrada aos sistemas bancários para garantir que apenas o titular da conta tenha acesso. A IA pode melhorar a precisão desses sistemas, tornando-os mais seguros e convenientes para os clientes, especialmente aqueles com pouca familiaridade com senhas e códigos PIN.

**3. Sistemas de bloqueio e alerta para clientes Isolados**

Para clientes em áreas rurais ou remotas, a IA pode ser integrada a dispositivos de forma a emitir/disparar alertas que notificam pessoas conhecidas previamente cadastradas ou mesmo os bancos sobre atividades suspeitas ou mesmo ações de sequestro/coação.

Uma outra solução, já adotada por algumas instituições (como o C6, por exemplo), e que seria relevante no portfolio de segurança dos apps CAIXA é o chamado Geofencing, uma tecnologia que cria perímetros virtuais ao redor de uma localização geográfica específica. Utilizando sistemas de posicionamento global (GPS) e identificadores de radiofrequência locais, como nós de Wi-Fi ou beacons Bluetooth, o geofencing permite que dispositivos móveis ou outros equipamentos respondam a esses limites virtuais de acordo com parâmetros predefinidos.

No caso da segurança bancária o uso da geolocalização pode determinar perímetros seguros para a exibição de informações e realização de operações seguras. Uma possibilidade seria a não visualização dos saldos de contas e aplicações (ou a amostragem de saldos limitados a um determinado valor) e a limitação de operações de compras e transferências quando o cliente está fora de um perímetro considerado seguro.

O geofencing é uma ferramenta poderosa que, quando utilizada de forma ética e responsável, pode trazer inúmeros benefícios em diversas áreas, desde a segurança até o marketing e a automação residencial

4. **Educação digital e assistentes virtuais inteligentes sob medida**

Programas de educação digital personalizados, baseados em IA, podem ser desenvolvidos para ensinar práticas seguras a clientes com diferentes níveis de conhecimento tecnológico. Esses programas podem adaptar o conteúdo e a complexidade das lições com base no progresso e nas necessidades individuais dos clientes, garantindo que todos recebam a educação necessária para se protegerem online.

Da mesma forma, os assistentes inteligentes podem fornecer dicas personalizadas, responder a perguntas sobre segurança e guiar os clientes na configuração de medidas de proteção, como autenticação multifator e senhas fortes e outras dicas de movimentação segura

## Algumas soluções Imaginadas com IA

### 1. IA para Inclusão Financeira

Desenvolver plataformas de IA que ofereçam serviços bancários simplificados e acessíveis para pessoas com pouca familiaridade com tecnologia. Essas plataformas podem usar interfaces de voz e linguagem natural para facilitar o uso, permitindo que clientes vulneráveis realizem transações e acessem serviços bancários com facilidade.

### 2. Redes de Suporte Comunitário Baseadas em IA

Criar redes de suporte comunitário que utilizem IA para conectar clientes vulneráveis com voluntários e profissionais que possam oferecer assistência. Essas redes podem ajudar a resolver problemas técnicos, fornecer orientação sobre segurança digital e oferecer suporte emocional, criando uma comunidade de apoio para aqueles que mais precisam.

### 3. IA para Prevenção de Fraudes em Áreas de Risco

Usando a tecnologia de Geolocalização, desenvolver sistemas de IA que analisem dados de transações e comportamentos em áreas de risco para identificar padrões de fraude específicos dessas regiões. Esses sistemas podem ajudar a criar estratégias de prevenção mais eficazes e direcionadas, protegendo melhor os clientes que vivem em áreas vulneráveis.

### 4. Blockchain e IA para Segurança de Transações

Integrar IA com tecnologia blockchain para criar um sistema de transações bancárias mais seguro e transparente. A IA pode monitorar e analisar todas as transações em uma rede blockchain, identificando rapidamente qualquer atividade suspeita ou tentativa de fraude. Isso não apenas aumenta a segurança, mas também melhora a confiança dos clientes na integridade das transações.

### 5. IA para Prevenção de Fraudes em Dispositivos Móveis

Desenvolver aplicativos bancários que utilizem IA para monitorar a segurança dos dispositivos móveis dos clientes. A IA pode detectar malware, aplicativos suspeitos e comportamentos de uso anômalos, alertando os clientes e os bancos sobre possíveis ameaças. Além disso, pode recomendar ações corretivas, como a atualização de software ou a remoção de aplicativos maliciosos.

### 6. IA para Monitoramento de Redes Sociais

Utilizar IA para monitorar redes sociais e outras plataformas online em busca de informações sobre possíveis ameaças cibernéticas. A IA pode identificar discussões sobre novas técnicas de fraude, ataques planejados e outras atividades suspeitas, permitindo que os bancos tomem medidas preventivas antes que os ataques ocorram.

Algumas destas medidas devem ser pensadas em termos de privacidade

## Conclusão

As medidas tecnológicas baseadas em Inteligência Artificial (IA) têm um impacto significativo na redução de prejuízos financeiros e emocionais causados por crimes cibernéticos. A implementação de sistemas de detecção de fraudes em tempo real, autenticação biométrica avançada e assistentes virtuais inteligentes permite identificar e neutralizar ameaças rapidamente, minimizando as perdas financeiras. Além disso, essas tecnologias aumentam a confiança dos clientes na segurança dos serviços bancários, reduzindo o estresse e a ansiedade associados ao risco de fraudes.

O constante investimento em barreiras inteligentes é crucial para manter a eficácia dessas medidas. À medida que os criminosos cibernéticos desenvolvem novas técnicas, é essencial que as instituições financeiras, como a Caixa Econômica Federal, continuem a aprimorar suas defesas. Isso inclui a adoção de tecnologias emergentes, a atualização contínua dos sistemas de segurança e a educação dos clientes sobre práticas seguras online.

Em resumo, as soluções de IA não apenas protegem os ativos financeiros, mas também promovem o bem-estar emocional dos clientes, especialmente os mais vulneráveis. O compromisso contínuo com a inovação e a segurança é fundamental para criar um ambiente bancário mais seguro e resiliente, capaz de enfrentar os desafios impostos pelos crimes cibernéticos e garantir a confiança e a tranquilidade dos clientes.

## Referencias


1. CAIXA ECONÔMICA FEDERAL. Cartilha de Segurança CAIXA. Disponível em: https://www.caixa.gov.br/Downloads/seguranca/Cartilha-seguranca.pdf. Acesso em: 20 jan. 2025.
2. CAIXA ECONÔMICA FEDERAL. Segurança na internet - CAIXA. Disponível em: https://www.caixa.gov.br/seguranca/na-internet/Paginas/default.aspx. Acesso em: 20 jan. 2025.
3. SIMONI, Emílio. Crimes virtuais durante a pandemia: o aumento dos vazamentos e ataques no Brasil. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/apresentacoes-em-eventos/apresentacoes-de-convidados-em-eventos-de-2021/02-12-2021-sm-combate-aos-crimes-ciberneticos-no-brasil/emilio-simoni-psafe. Acesso em: 20 jan. 2025.
4. CAIXA ECONÔMICA FEDERAL. Sobre a CAIXA. Disponível em: https://www.caixa.gov.br/sobre-a-caixa/apresentacao/Paginas/default.aspx. Acesso em: 20 jan. 2025.
5. TODA MATÉRIA. Inteligência Artificial. Disponível em: https://www.todamateria.com.br/inteligencia-artificial/. Acesso em: 20 jan. 2025.
6. TECNOBLOG. Como funciona a inteligência artificial?. Disponível em: https://tecnoblog.net/responde/como-funciona-a-inteligencia-artificial/. Acesso em: 20 jan. 2025.

7. MILAGRE DIGITAL. Qual a importância da inteligência artificial?. Disponível em: https://milagredigital.com/qual-a-importancia-da-inteligencia-artificial/. Acesso em: 20 jan. 2025.
8. DIO. A importância da inteligência artificial para o mundo moderno. Disponível em: https://www.dio.me/articles/a-importancia-da-inteligencia-artificial-para-o-mundo-moderno. Acesso em: 20 jan. 2025.
9. WIKIPEDIA. Geofence. Disponível em: https://en.wikipedia.org/wiki/Geofence. Acesso em: 20 jan. 2025.
10. RECLUS, Florian. Who is part of geofencing? Actors: their roles and interactions in connected freight transport systems. Disponível em: https://research.chalmers.se/publication/526906/file/526906_Fulltext.pdf. Acesso em: 20 jan. 2025.
11. IJARnD. Location-based services using geofencing. Disponível em: https://www.ijarnd.com/manuscripts/v3i4/V3I4-1196.pdf. Acesso em: 20 jan. 2025.