AS CONTRIBUIÇÕES DO NFC PARA A SEGURANÇA DA INFORMAÇÃO E PRÁTICAS SUSTENTÁVEIS

THE CONTRIBUTIONS OF NFC TO INFORMATION SECURITY AND SUSTAINABLE PRACTICES

Luís Enrique de Oliveira
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
luis.oliveira110@fatec.sp.gov.br

Carlos Eduardo de Brito Dias
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
carlos.dias22@fatec.sp.gov.br

João Emmanuel D Alkmin Neves
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
joao.neves11@fatec.sp.gov.br

Resumo

A Comunicação por Campo de Proximidade (NFC), do inglês *Near Field Communication*, configura-se como uma tecnologia que possibilita a comunicação entre dispositivos ativos e passivos, viabilizando aplicações diversas, como transações financeiras, transferência de dados e controle de acesso. Neste estudo, o enfoque reside na implementação da tecnologia NFC como meio de pagamento, em comparação com cartões físicos, sob as perspectivas de Segurança da Informação e impacto ambiental. Utilizando uma metodologia bibliográfica, exploratória e quantitativa, baseada na revisão de estudos relevantes. Os resultados mostram que a NFC oferece um nível de segurança semelhante aos cartões físicos, com potencial de superação, além de se destacar em sustentabilidade ambiental pela significativa redução de plásticos.

Palavras-chave: NFC; Cartões físicos; Segurança da Informação; Sustentabilidade.

Abstract

Near Field Communication (NFC) technology facilitates communication between active and passive devices, enabling a variety of applications, including financial transactions, data transfer, and access control. This study centers on the adoption of NFC technology as a payment method, comparing it with traditional physical payment cards in terms of Information Security and environmental impact. The research employs a bibliographic, exploratory, and quantitative methodology, rooted in the review and analysis of relevant studies. Findings indicate that NFC offers a level of security similar to that of physical cards, with the potential to surpass them, in addition to standing out in environmental sustainability due to its significant reduction in plastics.

Keywords: *NFC; Physical cards; Information Security; Sustainability.*

1. INTRODUÇÃO

A humanidade já experienciou vários momentos em sua história em que se viram necessário de um meio de pagamento. No período Neolítico o escambo foi muito popular, tratando-se de um meio de troca, o qual não envolve uma moeda padrão. Durante o império romano, o sal foi muito usado, inclusive sendo de onde surgiu a palavra salário. Com o passar dos séculos, os meios de transações foram evoluindo com a criação do dinheiro em espécie, o qual se tornou um padrão em todo mundo, com cada país definindo sua própria moeda. No Brasil, os cartões físicos de pagamento só começaram a se popularizar na década de 70.

De acordo com Desmadirega e Hermana (2023), cartões de crédito oferecem várias vantagens, sendo essas o seu fácil manuseio, portabilidade, significativamente seguro, não possuindo valor intrínseco. Os cartões físicos de pagamento (débito e crédito) sendo considerados um meio eletrônico de pagamento, foram criados com o intuito de reduzir a circulação do dinheiro em papel. Sendo um meio de pagamento bastante utilizado pela maioria das pessoas, é notório dizer que se tornou muito popular. Contudo, pode-se dizer que apresentam algumas inseguranças, como fraude, roubo, clonagem de cartão, assim como o fato de gerarem plástico em demasia, sendo um meio considerado pouco sustentável.

De acordo com Neves (2018), atualmente, vivencia-se a era da informação, onde o avanço do conhecimento possibilita o desenvolvimento de novos processos e tecnologias. Esses desenvolvimentos contribuem significativamente para a facilitação de diversas atividades, aumento da segurança e ampliação das possibilidades para a humanidade. Tendo em vista isso, a tecnologia NFC, considerada uma modalidade sem contato, derivada do termo inglês

contactless, opera uma comunicação entre dispositivos habilitados com essa tecnologia, mediante rádio frequências (NFC Fórum, 2024). Isso envolve o emprego de dois dispositivos, os quais, em sua grande maioria, constituem-se de um dispositivo ativo e um dispositivo passivo. Faz-se necessário uma proximidade mínima de 4 cm para ocorrer a comunicação entre tais dispositivos. As suas aplicações são diversas, sendo extremamente utilizada para a realização de pagamentos. A implementação de robustos protocolos de segurança é essencial para proteger contra fraudes e ataques cibernéticos, garantindo a integridade e a confidencialidade das informações transmitidas. Contudo, também pode ser utilizada para a transferência de dados, controle de acesso, assim como para etiquetas inteligentes de *IoT* (Moura; D' Alkmin Neves, 2021). A tecnologia NFC, sendo relativamente nova, foi desenvolvida em uma época em que a Segurança da Informação se tornou essencial. Em consonância com Neves *et al.* (2023), Pedro *et al.* (2024) e Souza *et al.* (2024), por isso, assim como a Inteligência Artificial, o *Blockchain* e a Agricultura de Precisão, a NFC já incorpora mecanismos de Segurança da Informação desde sua criação.

Para esse trabalho, a tecnologia NFC em si, terá um direcionamento a como uma ferramenta de pagamento, a qual uma análise será feita em como pode ser melhor e mais econômico do que um cartão físico de pagamento, sendo débito ou crédito, comumente usados pela maioria das pessoas.

Uma vez apresentado toda e qualquer informação que seja relacionada a tecnologia NFC e cartões físicos de pagamento, sendo ainda pertinente ao objetivo desse trabalho, poderá ser concluído que a tecnologia NFC é uma alternativa mais segura, tanto no quesito Segurança da Informação, quanto em práticas mais sustentáveis?

Os cartões ainda continuam sendo amplamente aceitos pela maioria das pessoas, justamente pela sua facilidade do uso, quase agindo como um substituto ao próprio dinheiro em cédula. Quanto a tecnologia NFC, do mesmo modo, também possui essa vantagem. Contudo, não são todos os dispositivos que têm implantados a si a tecnologia NFC.

Portanto, o objetivo geral desse trabalho consiste em investigar, analisar e avaliar se a implementação da tecnologia NFC é uma alternativa mais segura, tanto no quesito ambiental, quanto da Segurança da Informação, em comparação aos cartões físicos de pagamento.

A justificativa para a realização deste estudo é de suma importância, considerando-se que as tecnologias associadas aos cartões físicos de pagamento e à NFC são amplamente empregadas em transações financeiras, demandando uma análise criteriosa quanto à segurança, ancorada nos preceitos da Segurança da Informação. Além disso, é imperativo avaliar qual destas tecnologias acarreta maior impacto ambiental, levando-se em conta que os cartões físicos, confeccionados predominantemente em material plástico, suscitam indagações acerca do processo de fabricação e descarte, e seus desdobramentos no ecossistema. Por outro lado, a tecnologia NFC apresenta-se como uma alternativa de natureza digital, o que demanda uma reflexão sobre suas implicações ambientais.

2. REFERENCIAL TEÓRICO

A partir da Introdução, observa-se a necessidade de uma fundamentação teórica que permita a compreensão das funcionalidades dos cartões físicos de pagamentos e a tecnologia NFC, com o seu enfoque voltado para seus benefícios, assim como a própria Segurança da Informação. Além disso, faz-se relevante a explanação sobre possível impactos que essas tecnologias poderiam causar ao meio ambiente.

2.1 CARTÃO FÍSICOS DE PAGAMENTO

Antes da implementação de chips como fator de autenticação em cartões físicos de pagamento, era de uso comum a utilização da tarja magnética. Cartões de tarja magnética contêm uma faixa de material magnético que permite armazenar pequenas quantidades de dados. Os dados são codificados como uma sequência de estados de magnetização no plano (bits) impressos na tarja magnética (Scaife *et al.*, 2018). A utilização da tarja magnética é desencorajada por inúmeras razões, tendo como principal motivo que o cartão com tarja magnética não pede senha para concluir a transação. Para finalizar a compra, basta passar a tarja na maquininha e assinar o recibo - o que pode facilitar a ação de criminosos que falsificam assinaturas (Nubank, 2023). Sendo considerado uma tecnologia inferior aos chips que, por suas vezes, são capazes de armazenar dados de uma forma mais segura, usando de criptografia muito difícil de ser interpretada.

Segundo Stripe (2023), a introdução de chips em cartões de crédito representou uma

revolução significativa na indústria financeira. Ao substituir as tradicionais tarjas magnéticas, os chips proporcionaram maior segurança nas transações, reduzindo significativamente fraudes. Além disso, a tecnologia agilizou os processos de pagamento, oferecendo conveniência aos consumidores e estabelecendo um novo padrão de eficiência no cenário financeiro global. Essa transformação decorre da tecnologia EMV presente nos chips, desenvolvida na década de 1990 pelas empresas Europay, Mastercard e Visa, atualmente integrantes do grupo EMVCo (que também inclui as bandeiras American Express, Discover, JCB e Union Pay). Em conjunto com a tecnologia dos leitores de cartões, essa inovação possibilita um processo de validação e pagamento seguro, no qual os cartões com chip EMV não transmite o número do cartão durante as transações. Em vez disso, para cada compra, é gerado um código diferente para o leitor de cartões, códigos esses que não podem ser replicados e são difíceis de falsificar. Para realizar o pagamento, basta inserir o cartão no leitor com o chip voltado para cima, permitindo que o chip transmita um código criptografado com as informações do cartão. Em seguida, o cliente fornece seu PIN para obter a autorização. Após esse processo, o leitor transmite os dados ao PDV da empresa, que os envia ao pagamento. Este, por sua vez, entra em contato com o emissor do cartão, que retorna com a aprovação ou rejeição da transação.

2.2 NFC

Segundo o NFC Fórum (2024), a *Near Field Communication* (NFC) é uma tecnologia de comunicação sem contato que opera numa distância máxima de 2 cm (ou uma polegada), através de ondas de rádio frequência, permitindo que seja efetuada uma troca de informações entre dispositivos que tem essa tecnologia habilitada. Sendo ainda mais pertinente a esse estudo, para a realização de pagamentos. A transmissão dessas informações ocorre por modulação de amplitude quando um dispositivo está ativo, utilizando uma frequência de 13,56 MHz, ideal para distâncias curtas. O *baud rates* determina a taxa de transmissão de dados, com o código Miller preferido por sua eficiência energética, compatibilidade e simplicidade, enquanto o esquema de Manchester é utilizado em taxas superiores a 106 *kBaud*. Ambos os códigos codificam um *bit* de informação por intervalo de tempo, com diferenças na representação de zeros e uns. Em *baud rates* mais altos, o sinal de Radiofrequência (RF) durante uma pausa é 82% do nível de um sinal ativo.

Muito semelhantemente a tecnologia de identificação por radiofrequência (RFID) a tecnologia NFC também trabalha com dois modos em que os dispositivos conseguem se comunicar, sendo o modo ativo e modo passivo. Segundo Singh, Adzman e Hassan (2018), no modo ativo, ambos os dispositivos NFC geram sua própria frequência de rádio para transferir dados, enquanto no modo passivo, apenas um dos dispositivos NFC gera o campo de frequência de rádio. Os padrões da tecnologia NFC estabelecem três modos de operação distintos: Leitura/Escrita, Emulação de Cartão e Ponto a Ponto. No modo Leitura/Escrita, um dispositivo, geralmente um *smartphone*, atua como leitor, enquanto a etiqueta ou o cartão sem contato funciona como escritor, sendo utilizado em pagamentos sem contato e identificação de produtos. A Emulação de Cartão, relevante para este estudo que avalia a NFC como substituto dos cartões físicos, permite que dispositivos móveis funcionem como cartões de débito ou crédito, um método altamente seguro. No modo Ponto a Ponto, dois dispositivos NFC trocam informações, permitindo interações como compartilhamento de arquivos e troca de informações de contato. Para realizar pagamentos, segundo Wong (2018), o usuário utiliza seu dispositivo seguro, seja um celular habilitado com NFC ou um cartão inteligente, e o aproxima perto da etiqueta NFC de outro dispositivo para que o pagamento seja completado. O usuário precisa de um telefone com NFC para ler e armazenar o código de acesso do leitor, conectado a um servidor de *tickets*, permitindo ler e armazenar o *ticket* do leitor. Conforme o NFC Fórum (2024), muitas empresas utilizam cartões de identificação para controlar o acesso às suas instalações e redes, e a tecnologia NFC pode reduzir os custos de emissão e gerenciamento desses cartões. Dispositivos com NFC simplificam o acesso às redes empresariais, tornando-se uma alternativa superior ao reduzir o descarte de plástico e facilitar o uso, eliminando a necessidade de novos cartões.

3. MATERIAIS E MÉTODOS

A pesquisa para a elaboração deste artigo científico foi de natureza bibliográfica, exploratória e quantitativa. Os dados foram coletados e analisados numericamente, principalmente a partir de estudos e pesquisas previamente realizados por outros pesquisadores, bem como de sites de instituições bancárias. As informações foram obtidas de estudos e artigos

publicados entre os anos de 2018 e 2023, assegurando a qualidade e a atualidade dos dados. Conforme apresentado na Tabela 1, foram contabilizados um total de 17.407 artigos relacionados ao NFC e cartões de crédito e débito.

Tabela 1 - Base de dados

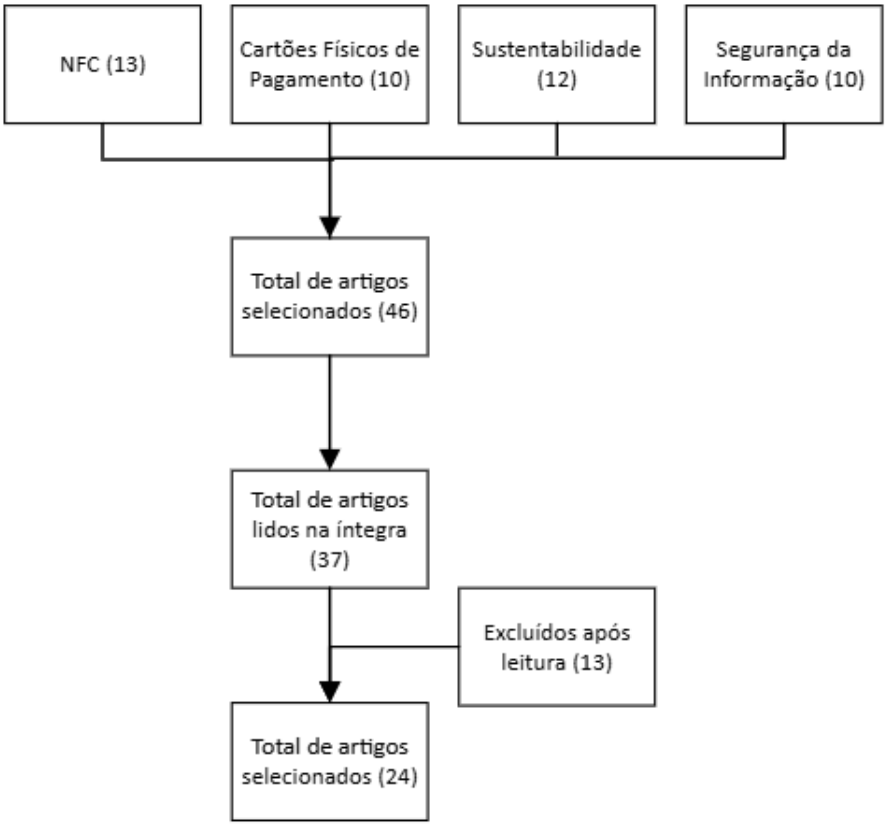
Bases	Termos de busca	N.º de artigos
IEEE Xplore	NFC	1. 828
	Credit/Debit card	3. 057
Academia.edu	NFC	1. 055
	Credit/Debit card	1. 830
ScienceDirect	NFC	1. 717
	Credit/Debit card	7. 920

Fonte: Elaborada pelos autores (2024)

Durante a pesquisa, a coleta de dados abrangeu tópicos relacionados a tecnologia de Comunicação por Campo de Proximidade (NFC) e cartões físicos de pagamento. Os aspectos mais relevantes considerados para essas tecnologias incluíram a sua usabilidade, Segurança da Informação e sustentabilidade. Para esses, informações foram extraídas de artigos, *blogs* e sites de instituições bancárias. No que tange à emissão de poluentes pelo descarte inadequado desses cartões, foram considerados estudos sobre os perigos do plástico para a natureza e para o ser humano. A análise dos dados resultou na identificação das principais informações sobre os cartões e a NFC, avaliando se a tecnologia NFC é superior aos cartões de crédito e débito em termos de Segurança da Informação e impactos ambientais.

Conforme pode ser visto na Figura 1, foi feito um fluxograma sobre os artigos que foram pesquisados e selecionados, depois lidos na sua totalidade, alguns excluídos após a leitura e então, os que foram usados para a realização deste trabalho.

Figura 1: Fluxograma (PRISMA) do processo de seleção dos artigos pesquisados.



Fonte: Elaborada pelos autores (2024)

4. RESULTADOS E DISCUSSÕES

Com base no estudo realizado, este artigo apresenta as discussões teóricas sobre a implementação da tecnologia NFC como meio de pagamento, comparando-a com cartões físicos, sob a perspectiva da Segurança da Informação e do impacto ambiental.

4.1 A SEGURANÇA DA INFORMAÇÃO, OS CARTÕES FÍSICOS DE PAGAMENTOS E A TECNOLOGIA NFC

Segundo Stripe (2023), os cartões EMV são mais seguros devido à necessidade de inserção de um número PIN durante as transações e à geração de códigos únicos a cada compra, o que dificulta a falsificação. Além disso, esses cartões possuem um microchip integrado para processamento e armazenamento seguros de dados. De acordo com Chaves e Matsuno (2024), os cartões EMV empregam diversos mecanismos de autenticação, incluindo protocolos para

autenticar dados do cartão e do usuário, bem como para autenticar transações e o emissor do cartão. Esses protocolos visam garantir a integridade e segurança das transações, utilizando assinaturas digitais estáticas e dinâmicas, códigos PIN *offline* e *online*, e códigos de autenticação de mensagens. Conforme evidenciado por Chargeflow (2023), os cartões EMV proporcionam uma proteção adicional contra atividades fraudulentas, como ataques de *Skimming*, devido à geração de códigos únicos a cada transação, o que dificulta a falsificação desses cartões.

Com relação às vulnerabilidades, a tecnologia EMV foi desenvolvida para aprimorar a segurança dos cartões físicos de pagamento, contudo, apesar das medidas de segurança implementadas, como defesa a ataques de *Skimming*, os fraudadores conseguiram desenvolver técnicas para contornar o sistema de segurança (Santos; Neves, 2023). Durante a inserção do cartão físico na máquina de pagamento e a digitação da senha pelo titular, os fraudadores capturam o PIN por meio de câmeras ocultas ou sobreposições de teclado, permitindo o registro do PIN do titular. Yunusov (2024) destaca que as instituições bancárias empregam tecnologias como o ATC para monitorar transações e evitar fraudes. No entanto, mesmo com a utilização do ATC, os cibercriminosos desenvolveram métodos para contornar essa autenticação, como os Ataques de Criptogramas, que envolvem a clonagem de transações legítimas para posterior uso em diferentes ocasiões, muitas vezes passando despercebidos.

Segundo Singh, Adzman e Hassan (2018), a tecnologia NFC é baseada por comunicação sem contato, agindo como uma extensão da tecnologia de Identificação por Rádio Frequência (RFID), essa que opera em comunicações de curto alcance. Adicionalmente, os autores ressaltam que por mais que se trata de uma tecnologia promissora, a tecnologia NFC é propensa a ataques de segurança como, por exemplo, o *man in the middle*, ataques de negação de serviços etc. A possibilidade de interceptação de dados por atacantes é uma preocupação real, tornando a criptografia dos dados essencial para proteger informações sensíveis (Pires; Neves, 2023). Segundo IBM (2021), é possível usar funções de hashing para codificar os dados, transformando-os em uma sequência única de símbolos, garantindo que haja integridade desses dados.

As vulnerabilidades próprias da tecnologia NFC ocorrem por se tratar de uma tecnologia de comunicação sem fio. Segundo Wong (2018) essa característica possibilita que terceiros

próximos aos dispositivos em comunicação interceptem os dados transmitidos. Adicionalmente, o autor ressalta o potencial de corrupção de dados que acontece quando o atacante obstrui o transmissor do dispositivo NFC, no tempo correto, com ondas de rádio, fazendo com que os dados sejam perdidos. No entanto, é importante notar que esses tipos de ataques não permitem a manipulação dos dados, mas sim interrupções na comunicação, o que os torna mais comparáveis a ataques de negação de serviço (Barbosa; Ferreira; Neves, 2023). Essas vulnerabilidades, embora identificadas, não invalidam a tecnologia NFC, mas destacam a necessidade de medidas de segurança para mitigar tais ameaças e garantir a integridade e confidencialidade das informações transmitidas.

Como exibido na Tabela 2, foi realizado um comparativo entre os problemas de Segurança da Informação entre ambas as tecnologias.

Tabela 2 - Problemas de Segurança da Informação relacionados ao NFC e Cartões Físicos de Pagamento

Problemas de SI	**Como acontece**	**Afeta quais Tecnologias?**	**Impactos Resultantes**
Autenticação (ATC)	Ataques de criptogramas clonam as transações	Somente Cartões Físicos de Pagamento	Invasores acessam dados para novas transações
Corrupção de dados	Alcançada através da transmissão de frequências válidas do espectro de dados	Somente NFC	Erro na comunicação, comprometendo dados do dispositivo
Skimming	Captura de dados magnéticos do cartão	Somente Cartões Físicos de Pagamento	Roubo de PIN
Espionagem	Monitoramento de dados via NFC	Somente NFC	Exposição de informações sigilosas

Fonte: Elaborada pelos autores (2024) com base em Wong (2018), Chargeflow (2023), Yunusov (2024)

4.2 A SUSTENTABILIDADE, OS CARTÕES FÍSICOS DE PAGAMENTO E A TECNOLOGIA NFC

A maioria dos cartões de crédito e débito é atualmente fabricada com plásticos PVC não recicláveis, que contêm metais em sua composição, contribuindo para a emissão de poluentes durante o processo de fabricação (Science News Explores, 2022). A produção desses cartões demanda anualmente cerca de 30.000 toneladas de plástico PVC, um material que não é biodegradável, comprometendo o meio ambiente (Thales Group, 2020). Além disso, a indústria

de cartões de crédito/débito é uma grande contribuinte para as mudanças climáticas devido ao descarte inadequado de cartões de plástico, embalagens e à energia consumida em transações eletrônicas (Payments Dive, 2021). Esses resíduos plásticos acabam em aterros sanitários e oceanos, emitindo gases de efeito estufa e representando uma ameaça ao meio ambiente.

A tecnologia NFC necessita de *smartphones* para ser utilizada como meio de pagamento. Segundo a ONU News (2019), no ano de 2016, foram descartadas cerca de 435 mil toneladas de celulares no mundo. Os celulares produzem pegadas de carbono, cerca de 80% da pegada de carbono se dá pela produção dos *smartphones*, aproximadamente 16% ao uso e 3% ao transporte, nesse contexto os celulares estão sendo descartados com maior frequência, pois a demanda para aparelhos melhores e mais atualizados é constante. Os componentes dos *smartphones* têm em sua composição: ouro, prata, cobalto, entre outros elementos, na extração desses metais é utilizada uma abundância de óleo combustível pesado, contribuindo com a mudança climática.

Consoante o site Pensamento Verde (2018), 80% dos componentes de *smartphones* podem ser reciclados. Os plásticos dos aparelhos podem ser retirados e reutilizados para produzir outros equipamentos, como peças para impressoras. As placas de circuitos são feitas de metais e são enviados para outros países, que contenham centros de reciclagens especializados em metais.

Como ilustrado na Tabela 3, foi realizado um comparativo entre os problemas ambientais associados a ambas as tecnologias, apontando questões relacionadas, desde as adversidades causadas pelo processo de fabricação, até o momento em que tais tecnologias serão descartadas.

Tabela 3 - Problemas Ambientais relacionados aos Cartões Físicos de Pagamento

Problemas Ambientais	Como acontece	Afeta quais Tecnologias?	Impactos Resultantes
Processo de Fabricação	Cartões de PVC não recicláveis, com *chips* e pedaços de metal	Somente os Cartões Físicos de Pagamento	Emissão excessiva de poluentes
Poluição na natureza	Descarte inadequado de cartões	Somente os Cartões Físicos de Pagamento	Acúmulo de resíduos
Processo de descarte	Resíduos plásticos são descartados em aterros sanitários e oceanos	Somente os Cartões Físicos de Pagamento	Aumento de poluição e efeito estufa
Processo de Fabricação	Produção de *smartphones* gera 80% de pegada de carbono	Somente a tecnologia NFC	Aumento da Pegada de Carbono
Minérios	Seus componentes são feitos de minérios	Somente a tecnologia NFC	Uso demasiado do óleo combustível

Fonte: Elaborada pelos autores (2024) com base em Science News Explores (2022), Payment Dives (2021), Thales Group (2020), ONU News (2019)

Ou seja, numa primeira análise, poderá ser observado que a tecnologia NFC, num quesito ambiental, é superior aos cartões de plástico. Pois com essa tecnologia em um dispositivo móvel, eliminaria a necessidade de cartões físicos de pagamento, diminuindo a produção de resíduos plásticos usados para a fabricação de cartões, que tem impacto direto na saúde ambiental e contribui para a emissão de gases causadores do efeito estufa.

5. CONSIDERAÇÕES FINAIS

Este estudo abordou aspectos relacionados à Segurança da Informação e Sustentabilidade de cartões físicos de pagamento e NFC. A análise realizada indica que o NFC possui potencial superior tanto em termos de Segurança da Informação quanto de Sustentabilidade quando comparado aos cartões físicos de pagamento.

A tecnologia NFC, embora não ofereça intrinsecamente proteção contra a espionagem de dados, requer a implementação de um canal seguro entre os dispositivos NFC. Isso implica a adoção de protocolos de criptografia e segurança para assegurar a confidencialidade, integridade e autenticidade dos dados transmitidos. O protocolo Diffie-Hellman é empregado em sistemas de segurança para estabelecer uma chave de sessão segura entre duas partes, facilitando a comunicação segura em sistemas NFC por meio de cálculos modulares. Devido à

sua complexidade computacional, o protocolo Diffie-Hellman é resistente a ataques de escuta passiva, tornando desafiador para um invasor determinar a chave de sessão sem acesso à chave privada das partes envolvidas na comunicação NFC.

Além de analisar as capacidades de Segurança da Informação do NFC, este estudo também avaliou sua sustentabilidade em comparação com os cartões de plástico convencionais. Empresas de tecnologia, ao longo dos anos, têm investido significativamente em práticas sustentáveis. A crescente conscientização ambiental torna evidente que, enquanto os cartões físicos de pagamento são amplamente utilizados e seguros, sua produção e descarte têm um impacto negativo significativo no meio ambiente devido ao plástico utilizado. Por outro lado, a tecnologia NFC não apresenta esse problema ambiental, embora exija dispositivos habilitados com essa tecnologia, como *smartphones*, os quais não são necessariamente sustentáveis.

Apesar da necessidade de dispositivos específicos para NFC, como *smartphones*, é importante ressaltar que o uso generalizado desses dispositivos móveis é uma realidade atual e possivelmente futura. Portanto, se a tecnologia NFC for adotada como meio de pagamento em substituição aos cartões físicos, isso poderia resultar em uma redução significativa na poluição causada pelo descarte de resíduos plásticos.

Referências

BARBOSA, P.; FERREIRA, M.; NEVES, J. E. D. **Abordagem de Segurança no Desenvolvimento de Aplicações Web**. III FatecSeg. 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/107. Acesso em 5 maio 2024.

CHARGEFLOW. **EMV Bypass Cloning: Are Chip Cards Safe for Ecom Merchants?**. Disponível em: EMV Bypass Cloning: Revelando a segurança dos cartões com chip em 2023 (chargeflow.io). Acesso em 11 de maio 2024.

CHAVES, M; MATSUNO, R. B. **Segurança em cartões Smartcard EMV**. Disponível em: https://www.ic.unicamp.br/~rdahab/cursos/mp202/Welcome_files/trabalhos/SmartCardsEMV/texto/. Acesso em 19 de maio 2024.

DESMADIREGA, L. A.; HERMANA, B. **The Comparison of ATM/Debit Card, Credit Card, and E-Money Transactions in Indonesia Before and After the Covid-19 Pandemic Period January 2018 - August 2023**. Disponível em: https://www.researchgate.net/publication/376330901_The_Comparison_of_ATMDebit_Card_Credit_Card_and_E-Money_Transactions_in_Indonesia_Before_and_After_the_Covid-19_Pandemic_Period_January_2018_-_August_2023. Acesso em 06 maio de 2024.

IBM. **Funções de hashing**. 2021. Disponível em: https://www.ibm.com/docs/pt-br/psfa/7.1.0?topic=toolkit-hashing-functions. Acesso em 02 de nov. 2024

MOURA, T. M.; D' ALKMIN NEVES, J. E. **Análise de Segurança em Dispositivos Internet das Coisas**. Revista Interface Tecnológica, [S. l.], v. 18, n. 2, p. 15–27, 2021. Disponível em: https://doi.org/10.31510/infa.v18i2.1174. Acesso em: 5 maio 2024.

NEVES, J. E. D. **Estudo dos parâmetros do modelo de Mason para cerâmicas piezelétricas utilizando algoritmos genéticos**. Dissertação (Mestrado em Tecnologia) – Faculdade de Tecnologia, Universidade Estadual de Campinas. Limeira, 129 p. 2018. Disponível em: https://doi.org/10.47749/T/UNICAMP.2018.995710. Acesso em 10 maio 2024.

NEVES, J. E. D.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A. **Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping**. Smart Innovation, Systems and Technologies. 1ed.: Springer International Publishing, 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em 10 maio 2024.

NFC FORUM. **What NFC does**. 2024. Disponível em: https://nfc-forum.org/. Acesso em 05 dez. 2024.

NUBANK. **Cartão com tarja magnética: como funciona essa tecnologia**. 2021. Diponível em: https://blog.nubank.com.br/cartao-com-tarja-magnetica-como-funciona-a-tecnologia/. Acesso em 24 nov. 2023.

ONU NEWS. **Agência da ONU alerta sobre impacto dos smartphones no meio ambiente**. 2019. Disponível em: https://news.un.org/pt/story/2019/01/1657472. Acesso em 07 jun. 2024.

PAYMENTS DIVE. **Card companies go green, but hurdles remain**. 2021. Disponível em: https://www.paymentsdive.com/news/payments-companies-look-towards-greener-future-roadblocks-lie-ahead/602847/. Acesso em 06 dez. 2023.

PEDRO, A. M.; TURCI JUNIOR, M.; MONTEIRO, A. S.; ESPERANDIO, A. A. M.; BASTOS, C. V.; NEVES, J. E. D. **Blockchain como Fator de Transparência**. Revista Brasileira em Tecnologia da Informação, v. 5, 79-95 p., 2024. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/104. Acesso em 10 maio 2024.

PENSAMENTO VERDE. **A relação de consumo e descarte de celulares velhos no Brasil.** 2018. Disponível: https://www.pensamentoverde.com.br/meio-ambiente/relacao-de-consumo-e-descarte-de-celulares-velhos-no-brasil/. Acesso em 07 jun. 2024.

PIRES, E. F. M.; NEVES, J. E. D. **Os Benefícios do ChatGPT**: Uma Abordagem para Potencializar Técnicas de Hardening. 13º CONCISTEC - Congresso Científico da Semana Nacional de Ciência e Tecnologia do IFSP. Artigo 41. 2023. Disponível em: https://drive.ifsp.edu.br/s/e4nk2YzbHtCHaq6/download?path=%2F&files=41_OS%20BENEFICIOS%20DO%20CHAT%20GPT_%20UMA%20ABORDAGEM%20PARA%20POTENCIALIZAR%20T%C3%89CNICAS%20DE%20HARDENING.pdf. Acesso em 5 maio 2024.

SANTOS, A. M.; NEVES, J. E. D. **Exploração Maliciosa do ChatGPT para Ataques Cibernéticos**. III FatecSeg. 2023. Disponível em:

https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/108. Acesso em 5 maio 2024.

SCAIFE, N.; PEETERS, C.; VELEZ, C.; ZHAO, H.; TRAYNOR, P.; ARNOLD, D. **The cards aren't alright: Detecting counterfeit gift cards using encoding jitter**. In: 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018. p. 1063-1076. Disponível em: https://ieeexplore.ieee.org/abstract/document/8418654. Acesso em 02 nov. 2024.

SCIENCE NEWS EXPLORES. **How we choose to pay has hidden costs for the planet**. Disponível em: https://www.snexplores.org/article/money-currency-plastic-paper-cash-credit-environmental-cost. Acesso em 06 dez. 2023.

SINGH, M. M.; ADZMAN, K. A. A. K.; HASSAN, R. **Near Field Communication (NFC) technology security vulnerabilities and countermeasures**. International Journal of Engineering & Technology, v. 7, n. 4.31, p. 298-305, 2018. Disponível em: https://www.researchgate.net/publication/329642316_Near_Field_Communication_NFC_Technology_Security_Vulnerabilities_and_Countermeasures. Acesso em 02 nov. 2024.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. **Cibersegurança na Agricultura de Precisão:** Exploração à Aplicação de Medidas Preventivas. Advances in Global Innovation & Technology, v. 2, 61-73 p., 2024. Disponível em: https://doi.org/10.29327/2384439.2.2-5. Acesso em 10 maio 2024.

STRIPE. **What are EMV chip cards? How EMV works and why it's so secure**. 2023. Disponível em: https://stripe.com/br/resources/more/what-are-emv-chip-cards. Acesso em 26 nov. 2023.

THALES GROUP. **O substituto ecológico dos cartões de crédito de plástico**: a alternativa de origem biológica. 2020. Disponível em: Alternative to PVC cards (an illustrated Q&A) (thalesgroup.com). Acesso em 22 maio 2024.

WONG, W. T. **Security of NFC payment on mobile payment application**. 2018. Tese de Doutorado. UTAR. Disponível em: http://eprints.utar.edu.my/3050/. Acesso em 02 nov. 2024.

YUNUSOV, T. **First contact. Attacks on chip-based cards**. 2024. Disponível em: https://hackmag.com/security/smartcard-attacks/. Acesso em 11 maio 2024.