# 16º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2025

BEATRIZ M. DA SILVA OLIVEIRA[1], FELIPE R. MARTINEZ BASILE[2]

[1] Cursando técnico de Redes de Computadores, voluntária PIVICT, IFSP, Campus Pirituba, beatriz.mota@aluno.edu.br.
[2] Docente e pesquisador do curso técnico de Redes de Computadores, Arquitetura de Computadores e Redes, Campus Pirituba, felipe.basile@ifsp.edu.br
Área de conhecimento (Tabela CNPq): 1.03.03.04-9 Sistemas de Informação

## Implementação do Protocolo NOSTR como Ferramenta de Comunicação Descentralizada sob a perspectiva da Cibersegurança

RESUMO: Este trabalho propõe a investigação do protocolo de comunicação Notes and Other Stuff Transmitted by Relays (NOSTR) — "Notas e Outras Informações Transmitidas por Servidores Retransmissores" — à luz dos aspectos de cibersegurança do modelo de referência de McCumber. O protocolo NOSTR, proposto em 2021 por fiatjaf, viabiliza a criação de redes sociais descentralizadas, que reduzem a dependência de entidades centralizadoras e fomentam a preservação da liberdade de comunicação. Para avaliar o funcionamento do protocolo, foi configurado um perfil no aplicativo Amethyst e explorou-se sua operacionalidade. A análise foi articulada ao modelo de referência de McCumber, evidenciando pontos fortes e fragilidades do NOSTR com base nos fundamentos da segurança da informação. Os resultados evidenciaram que o sistema oferece confidencialidade, integridade e disponibilidade, por meio do uso de criptografia assimétrica e da infraestrutura distribuída. No entanto, ameaças à segurança digital são inerentes ao NOSTR, dado que não possui mecanismos centrais para moderação de conteúdo malicioso. Conclui-se que o protocolo é uma alternativa promissora a sistemas centralizados e viável socialmente, embora requeira estudos sobre ética, segurança, escalabilidade e conscientização digital.

**PALAVRAS-CHAVE**: NOSTR; McCumber; cibersegurança; redes sociais descentralizadas; liberdade de comunicação; criptografia.

## Implementation of the NOSTR Protocol as a Decentralized Communication Tool from a Cybersecurity perspective

**ABSTRACT:** This study investigates the communication protocol *Notes and Other Stuff Transmitted by Relays* (NOSTR) through the lens of McCumber's cybersecurity reference model. Introduced in 2021 by fiatjaf, NOSTR enables the development of fully decentralized social networks. These networks reduce reliance on centralized entities and mitigate censorship, thus fostering freedom of communication. To assess its functioning, a profile was configured in the Amethyst application, a NOSTR-based client, and its main features were explored. The analysis, framed by McCumber's model, revealed both strengths and vulnerabilities of NOSTR regarding core cybersecurity principles. Results indicate that the system provides confidentiality, integrity, and availability, supported by asymmetric cryptography and distributed infrastructure. Nevertheless, security risks are inherent to NOSTR, as the protocol lacks centralized mechanisms to moderate malicious content. Overall, NOSTR emerges as a socially viable alternative to centralized platforms, though further research is needed on ethics, security, scalability, and digital awareness.

**KEYWORDS:** NOSTR; McCumber; cybersecurity; decentralized social networks; freedom of communication; cryptography.

## INTRODUÇÃO

O avanço das redes sociais e da comunicação digital trouxe à tona debates sobre centralização, censura e controle de dados por grandes corporações. Episódios recentes, como a interrupção

temporária da rede social X no Brasil, evidenciaram a fragilidade do acesso público à informação em redes centralizadas (G1, 2024). Nesse contexto, surge o NOSTR, um protocolo de comunicação digital criado em 2021 pelo brasiliero anônimo conhecido como fiatjaf, que tem como objetivo permitir a criação de aplicativos de redes sociais descentralizadas, autogerenciadas pelos usuários (NOSTR, 2024). Sua arquitetura é baseada em clientes e *relays*, permitindo a transmissão de mensagens sem a necessidade de servidores monopolizados por *BigTechs*. Este projeto estudou aspectos técnicos do NOSTR, bem como as consequências de sua estrutura na cibersegurança.

A análise do NOSTR vai além de sua configuração técnica, contemplando também os impactos de um modelo descentralizado sobre os princípios básicos e fundamentais da cibersegurança. Para isso, foi explorado o Cubo de McCumber, modelo de referência em cibersegurança que organiza os princípios de proteção da informação em uma estrutura tridimensional, facilitando a análise de riscos e a implementação de controles. Diante disso, a hipótese deste trabalho é que o NOSTR é uma alternativa viável às redes centralizadas, mas com limitações em escalabilidade e segurança. O objetivo é avaliar seu funcionamento prático e discutir seus impactos técnicos e sociais, fornecendo subsídios para pesquisas futuras sobre protocolos descentralizados e sua aplicação em ambientes digitais (SILVA, 2020).

## MATERIAL E MÉTODOS

A pesquisa foi conduzida por meio de um estudo exploratório com base em pesquisa técnica e experimentação do NOSTR. Inicialmente, foram analisados seus fundamentos, incluindo requisitos de funcionamento, formato de eventos em *JavaScript Object Notation* (JSON) e o papel de *relays* e clientes na comunicação descentralizada.

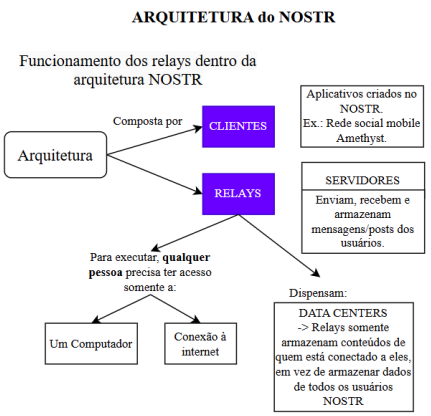
Em seguida, configurou-se um perfil no aplicativo Amethyst, cliente NOSTR compatível com Android, gerando no cadastro chaves pública e privada para autenticação. Após a configuração, foram exploradas utilidades do aplicativo, como a publicação de eventos e o acesso a relays (servidores NOSTR) públicos, possibilitando compreender o fluxo de comunicação descentralizada.

Para análise de cibersegurança, foi utilizado o modelo do Cubo de McCumber como ferramenta conceitual (SILVA, 2020), adaptando suas dimensões para avaliar aspectos técnicos e sociais. O cubo de McCumber é um modelo de referência de cibersegurança constituído por três dimensões: (1) Princípios da Cibersegurança, (2) Estados da Informação e (3) Medidas da Cibersegurança. Cada uma delas indica três aspectos essenciais da comunicação digital. Por meio de tabelas construídas pelo pesquisador, identificaram-se pontos fortes, como criptografia e resistência à censura, e fragilidades, como a dependência do comportamento ético dos usuários.

## RESULTADOS E DISCUSSÃO

Na Figura 1, é apresentado o funcionamento do protocolo NOSTR, que ilustra sua arquitetura descentralizada composta por clientes e relays. Essa estrutura evidencia como a comunicação ocorre independentemente de servidores centrais, reforçando o princípio de disponibilidade da informação e a resistência à censura.

FIGURA 1. Funcionamento do protocolo NOSTR, responsável pela criação de todo o ecossistema de redes sociais descentralizadas. *Fonte: elaboração própria (2025).*



A análise do NOSTR com base na primeira dimensão do Cubo de McCumber, que contempla os princípios de cibersegurança, evidenciou pontos relevantes. Na Tabela 1, são apresentados os resultados dessa análise, relacionando o protocolo NOSTR aos princípios de confidencialidade, integridade e disponibilidade. Observa-se que, embora o sistema ofereça resistência a manipulações da informação e falhas, a segurança completa depende da atuação consciente dos usuários.

TABELA 1. Relação entre o protocolo NOSTR e os Princípios da Cibersegurança consoantes à primeira dimensão do cubo de McCumber.

| Princípio | NOSTR | Observações |
|---|---|---|
| Confidencialidade | Eventos (ações e interações na plataforma) não são privados, apenas assinados digitalmente. O controle de envios privados e públicos depende dos servidores retransmissores. | Não há criptografia ponta a ponta por padrão. Ao publicar um evento em um *relay*, as mensagens não são cifradas, isto é, não ficam protegidas contra leitura. |
| Integridade | A assinatura digital garante que os conteúdos publicados pelos usuários não sejam alterados. | Se um evento é modificado por terceiros, a assinatura digital deixa de ser válida. A integridade depende apenas da segurança da chave privada, gerenciada pelo próprio usuário. |
| Disponibilidade | Relays múltiplos aos quais o usuário se conecta evitam ponto de falha único, permitindo redundância na disponibilidade dos dados e dificultando a censura. | Caso um conteúdo tenha sido publicado em múltiplos relays, a indisponibilidade de um relay não impede o acesso dos eventos por meio dos demais. |

Na Tabela 2, é possível visualizar os resultados obtidos na segunda dimensão do Cubo, que evidenciam como os estados de transmissão, armazenamento e processamento se relacionam à cibersegurança do NOSTR. O resultado expõe que a transmissão e o armazenamento de eventos nos relays demonstraram eficiência, com propagação rápida e preservação dos dados, enquanto o processamento é condicionado à infraestrutura dos clientes, como o aplicativo Amethyst.

TABELA 2. Relação entre o protocolo NOSTR e a segurança nos Estados de Armazenamento dos dados consoante à segunda dimensão do cubo de McCumber.

| Estado da Informação | NOSTR | Observações |
|---|---|---|
| Transmissão | Eventos podem ser interceptados, mas não podem ser alterados (integridade garantida), graças à assinatura digital de cada um. | Eventos passam por relays públicos. Um evento publicado em um cliente é propagado quase instantaneamente para outros usuários conectados a relays. |
| Armazenamento | Os dados do usuário ficam armazenados em relays (servidores simples). Mesmo após semanas, os dados permanecem | A preservação da segurança dos dados durante o armazenamento é atribuída ao próprio usuário, visto |

| | | |
|---|---|---|
| | acessíveis, desde que o relay continue ativo e seguro. | que ele escolhe os relays aos quais se conecta. |
| Processamento | Clientes (aplicativos) leem e exibem os eventos. Portanto, o risco durante o processamento depende da infraestrutura processual do aplicativo escolhido para a comunicação. | Um exemplo é o aplicativo (cliente) Amethyst, que interpreta o evento recebido e o apresenta em formato de postagem. |

Em termos de escalabilidade, o protocolo demonstrou limitações na gestão de grandes volumes de dados e interações. A manutenção de múltiplos relays e a autenticação de mensagens entre um número crescente de usuários exigem soluções eficientes de armazenamento e processamento. Comparações com sistemas centralizados mostram que, embora a descentralização ofereça maior resiliência contra falhas de infraestrutura, ela também requer planejamento cuidadoso para suportar crescimento sem comprometer segurança ou desempenho (AKKERMANS, 2011).

Por fim, a Tabela 3 apresenta os resultados referentes à terceira dimensão do Cubo de McCumber, que trata das contramedidas de segurança. Nela, observa-se que a tecnologia (criptografia assimétrica) garante autenticidade e as políticas flexíveis dos relays permitem autonomia, mas também implicam riscos de abuso, o que reforça a importância da conscientização e da responsabilidade individual e ética dos usuários. Já a dimensão humana evidencia a necessidade de conscientização dos usuários quanto à proteção das chaves privadas, dentre outros aspectos importantes para a segurança digital.

TABELA 3. Relação entre o protocolo NOSTR e as Contramedidas de cibersegurança segundo à terceira dimensão do cubo de McCumber.

| Contramedida | NOSTR | Observações |
|---|---|---|
| Tecnologia | O uso de criptografia assimétrica é funcional para a autenticação, porém não garante privacidade total. | Um evento só pode ser publicado com a chave privada correspondente, validada por meio da chave pública. |
| Políticas | Não existe um regulamento moderador central. Há alta liberdade, concomitante ao risco de abuso. | Relays podem hospedar conteúdos abusivos, pois cabe aos proprietários dos relays definir seus regulamentos e políticas; e aos usuários decidirem permanecer ou migrar para outros relays. |
| Pessoas (conscientizaçã o e treinamento) | No sistema NOSTR, as discussões acerca da importância de comunidades eticamente conscientes ainda são baixas. | Além disso, as pessoas devem ser instruídas a proteger suas chaves corretamente, visto que a perda da chave privada implica perda irreversível da identidade digital na rede.. |

Assim, observa-se que cada dimensão do Cubo de McCumber se reflete diretamente nos resultados obtidos. A primeira dimensão, referente aos princípios da cibersegurança, evidencia a integridade e a disponibilidade no protocolo, conforme demonstrado na Tabela 1. A segunda dimensão, que aborda os estados da informação, revela o nível de eficiência na transmissão, no armazenamento e no processamento dos dados, conforme apresentado na Tabela 2. Por fim, a terceira dimensão, correspondente às contramedidas de segurança, ressalta a importância da tecnologia, das

políticas e do comportamento humano na proteção do NOSTR, conforme exposto na Tabela 3, evidenciando que a segurança do sistema depende tanto da estrutura técnica quanto da atuação ética e consciente dos participantes da rede.

Ao relacionar o NOSTR com projetos de segurança de ativos digitais, como carteiras de Bitcoin (ROCHA; BASILE; LÓPEZ, 2025), e análises forenses em telemedicina (MACHADO *et al*., 2021), é possível perceber convergências importantes: todos os sistemas dependem da aplicação rigorosa de protocolos de segurança e ferramentas técnicas para proteger dados, manter confiabilidade e garantir a integridade das informações. O estudo do NOSTR reforça que, para redes descentralizadas, o domínio desses princípios é essencial não apenas para a proteção técnica, mas também para assegurar aspectos éticos e sociais, contribuindo para ambientes digitais mais seguros e confiáveis.

Do ponto de vista ético, a descentralização traz desafios importantes. Diferentemente de redes centralizadas, em que há níveis de controle e filtragem, no NOSTR a responsabilidade pela moderação recai sobre aqueles usuários que decidirem gerir os relays. Esse aspecto destaca a necessidade de conscientização sobre o uso responsável e a aplicação de princípios de segurança, uma vez que a liberdade de comunicação deve ser equilibrada com a prevenção de abusos, golpes e desinformação. A comparação com projetos educativos em defesa digital evidencia que capacitar usuários para reconhecer ameaças e atuar de forma ética é fundamental para a sustentabilidade de redes descentralizadas (BASILE; RAMÍREZ LÓPEZ, 2020).

## CONCLUSÕES

O estudo demonstrou que o protocolo NOSTR apresenta um modelo de comunicação descentralizada viável. A análise com base no Cubo de McCumber evidenciou que a integridade e autenticidade dos eventos são garantidas pela assinatura digital, a confidencialidade depende da gestão adequada das chaves privadas pelos usuários, e a disponibilidade é fortalecida pela redundância de múltiplos relays. A avaliação das contramedidas de segurança indicou que, embora a tecnologia e a infraestrutura sejam robustas, fatores humanos e éticos permanecem críticos, uma vez que a moderação e o comportamento seguro recaem sobre os próprios usuários.

Ao comparar o NOSTR com outros projetos de segurança de ativos digitais, como carteiras de Bitcoin (ROCHA; BASILE; LÓPEZ, 2025) e sistemas de telemedicina (MACHADO *et al.*, 2021), também observou-se convergências na necessidade de protocolos e conscientização de usuários. Conclui-se que o NOSTR, embora ofereça maior resiliência e resistência à censura, exige educação digital para prevenção de abusos e desinformação (BASILE; RAMÍREZ LÓPEZ, 2020), boas práticas dos usuários e soluções técnicas escaláveis para ambientes digitais amplos.

## CONTRIBUIÇÕES DOS AUTORES

B.M.S.O. realizou a pesquisa, experimentação e redação do trabalho. F.R.M.B. orientou o estudo, contribuiu com a metodologia e revisou o manuscrito. Ambos os autores revisaram e aprovaram a versão final.

## AGRADECIMENTOS

Agradecemos ao Instituto Federal de São Paulo – Campus Pirituba e ao PIVICT pelo apoio na pesquisa. E também a colegas e professores que contribuíram com suas visões sobre a importância do trabalho.

## REFERÊNCIAS

AKKERMANS, H.; YGGE, F. Decentralized Markets versus Central Control: A Comparative Study. 2011. Disponível em: https://arxiv.org/abs/1106.0223. Acesso em: 25 ago. 2025.

BASILE, Felipe Rodrigues Martinez; RAMÍREZ LÓPEZ, Leonardo Juan. *Estrategia formativa en defensa digital para adolescentes: experiencia en el Instituto Federal de São Paulo*. Revista Científica General José María Córdova, Bogotá, v. 18, n. 30, p. 271–287, abr./jun. 2020. DOI: 10.21830/19006586.579. Disponível em: Redalyc.

G1. **Bloqueio da rede social X no Brasil repercute na imprensa internacional**. Jornal Nacional, 31 ago. 2024. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2024/08/31/bloqueio-da-rede-social-x-no-brasil-repercute-na-imprensa-internacional.ghtml. Acesso em: 20 maio 2025.

MACHADO, Nadjila Tejo et al. *Investigação de splicing e cloning em imagens nos cenários da telemedicina por meio da forense computacional*. In: CONGRESSO DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA DO IFSP, 12. Anais... São Paulo, 2021. (Título do artigo).

NOSTR. **Decentralized publishing for the web**. Disponível em: https://nostr.how/en/what-is-nostr. Acesso em: 11 jun. 2024.

ROCHA, Rafael; BASILE, Felipe Rodrigues Martinez; LÓPEZ, Leonardo J. R. *Uma análise da cibersegurança na implementação de uma carteira cold wallet para transações com criptomoedas*. In: CONGRESSO DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA DO IFSP, 15., 2024. Anais... São Paulo: IFSP, 2025.

SILVA, Rafael et al. **Da segurança da informação à proteção dos dados: proposta de um modelo de referência**. In: Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2020), 20., 2020. Disponível em: https://www.researchgate.net/publication/348186384. Acesso em: 17 jul. 2025.