**CIBERATAQUES NA CADEIA DE SUPRIMENTOS E OS RISCOS SISTÊMICOS AO SISTEMA FINANCEIRO BRASILEIRO: ANÁLISE DO CASO C&M SOFTWARE**

*Alexsand Farias de Souza***[[1]](#footnote-1)**

**Resumo**

Este artigo analisa criticamente o ataque cibernético ocorrido no dia 03 julho de 2025, que atingiu instituições financeiras brasileiras por meio da C&M Software, empresa responsável pela intermediação entre bancos menores e o Banco Central. O objetivo é compreender de que forma falhas na governança de acessos privilegiados na cadeia de suprimentos permitiram a invasão, gerando riscos sistêmicos ao ecossistema financeiro nacional. Como metodologia, utilizou-se uma abordagem qualitativa, baseada em análise documental de notícias, relatórios técnicos e literatura acadêmica recente sobre segurança da informação e ataques à cadeia de suprimentos. A pesquisa identificou que o ataque ocorreu em múltiplas fases, envolvendo engenharia social, comprometimento inicial, escalonamento de privilégios e execução rápida das transações financeiras, que teriam sido convertidas em criptoativos. Entre os principais resultados, destaca-se a constatação de que, mesmo com investimentos robustos em segurança por parte dos bancos, a fragilidade de fornecedores terceirizados representa uma ameaça relevante. Conclui-se que é urgente aprimorar auditorias, políticas de gestão de acessos e fiscalização regulatória, ampliando a proteção não apenas das instituições financeiras, mas de toda a infraestrutura tecnológica que sustenta o sistema. O estudo contribui ao evidenciar a necessidade de estratégias integradas de prevenção e resposta para reduzir riscos futuros e proteger a confiança no mercado financeiro brasileiro.

**Palavras-chave:** Segurança da informação. Cadeia de suprimentos. Ataque cibernético. Sistema financeiro. Governança.

**Abstract**

This article critically analyzes the cyberattack that affected Brazilian financial institutions in July 2025 through C&M Software, a company responsible for connecting smaller banks to the Central Bank. The objective is to understand how failures in privileged access governance within the technological supply chain enabled the invasion, generating systemic risks to the national financial ecosystem. The methodology adopted was qualitative, based on document analysis of journalistic sources, technical reports and recent academic literature on information security and supply chain attacks. The study identified that the attack occurred in multiple phases, involving social engineering, initial compromise, privilege escalation and rapid execution of financial transactions, which were likely converted into cryptoassets. Among the main results, it stands out that, despite robust investments in security by banks, the fragility of third-party providers represents a significant threat. It is concluded that it is urgent to improve audits, access management policies and regulatory oversight, expanding protection not only for financial institutions but also for the entire technological infrastructure that supports the system. The study contributes by highlighting the need for integrated prevention and response strategies to reduce future risks and protect trust in the Brazilian financial market.

**Keywords:** Information security. Supply chain. Cyberattack. Financial system. Governance.

**Introdução**

A transformação digital do sistema financeiro brasileiro, impulsionada pelo avanço do PIX e pela crescente digitalização de serviços bancários, trouxe benefícios significativos como agilidade, inclusão e redução de custos operacionais. Contudo, essa modernização também ampliou consideravelmente a superfície de exposição a riscos cibernéticos, especialmente no que diz respeito a prestadores de serviços terceirizados que integram a cadeia de suprimentos tecnológica das instituições financeiras.

O presente estudo investiga o ataque cibernético ocorrido no dia 03 julho de 2025, no qual criminosos exploraram vulnerabilidades na C&M Software - empresa homologada pelo Banco Central para conectar bancos menores aos sistemas de pagamentos. O objetivo central é compreender como falhas na governança de acessos privilegiados nessa cadeia de suprimentos permitiram a invasão e analisar os riscos sistêmicos que ameaças desse tipo representam para todo o ecossistema financeiro nacional.

Como metodologia, foi adotada uma abordagem qualitativa, fundamentada em análise documental de relatórios técnicos, notícias e estudos acadêmicos sobre segurança da informação, ataques à cadeia de suprimentos e governança de TI. Essa análise busca responder à seguinte questão de pesquisa: de que forma a fragilidade em controles de segurança de fornecedores críticos pode comprometer a estabilidade e a confiança no sistema financeiro?

Justifica-se este estudo pela relevância do tema para a área de segurança da informação e pelo impacto econômico e reputacional gerado por ataques cibernéticos que ultrapassam as barreiras tradicionais de proteção bancária. Ao final, pretende-se contribuir com reflexões e recomendações para aprimorar políticas de prevenção, auditoria e fiscalização, reforçando a resiliência do sistema financeiro frente a ameaças cada vez mais complexas.

**Ciberataques na cadeia de suprimentos: fundamentos,**

**contexto e análise crítica.**

O fenômeno dos ciberataques à cadeia de suprimentos (supply chain attacks) representa uma evolução nas ameaças à segurança da informação, pois atinge organizações por meio de fornecedores estratégicos. De acordo com Kim, Park e Choi (2022, p. 4), “esses ataques exploram relações de confiança estabelecidas entre organizações e seus parceiros tecnológicos, permitindo acesso indireto a sistemas críticos”. Tal estratégia criminosa contorna defesas robustas ao focar em elos mais frágeis da cadeia, muitas vezes desprotegidos ou com controles menos rigorosos.

No Brasil, o crescimento exponencial de plataformas digitais de pagamento, como o PIX, ampliou a dependência de provedores homologados para garantir conectividade entre bancos menores e o Banco Central (COSTA; LIMA, 2023). A C&M Software, por exemplo, atua como elo essencial entre instituições financeiras e o Sistema de Pagamentos Brasileiro. Essa interdependência, embora positiva para democratizar o acesso ao mercado, cria novas superfícies de exposição a ataques.

Segundo Sousa e Almeida (2021), a governança de Tecnologia da Informação deve abranger todo o ecossistema, incluindo terceiros que possuem acessos privilegiados. No entanto, como destaca a Resolução nº 4.658/2018 do Conselho Monetário Nacional, embora haja exigências normativas, nem sempre são implementadas auditorias constantes e mecanismos de fiscalização eficazes para prestadores de serviços terceirizados.

O ataque hacker ocorrido em julho de 2025 contra a C&M Software evidenciou essa lacuna. De acordo com as informações divulgadas, criminosos utilizaram técnicas de engenharia social para obter credenciais privilegiadas e executar transações fraudulentas estimadas em até R$ 800 milhões. Essa ação ocorreu em múltiplas fases, iniciando com comprometimento inicial, seguido de reconhecimento interno, escalonamento de privilégios e execução rápida das transações, convertidas em criptoativos para dificultar rastreamento.

Como observa Micaella Ribeiro, especialista em identidades digitais, o ataque demonstrou “um ecossistema criminoso estruturado, capaz de agir de forma coordenada e silenciosa” (apud g1, 2025). Tal complexidade reforça a necessidade de abordagens preventivas integradas, indo além de ferramentas tecnológicas para incluir cultura organizacional de segurança, treinamento contra engenharia social e processos contínuos de auditoria.

A literatura também aponta que os impactos vão além do aspecto financeiro. Costa e Lima (2023) identificam efeitos reputacionais, sistêmicos e operacionais decorrentes de falhas na segurança da cadeia de suprimentos. Como citado pelos autores:

“O impacto sistêmico atinge não apenas a instituição vítima direta, mas compromete a confiança de todo o ecossistema financeiro, exigindo resposta coordenada de reguladores, empresas e sociedade” (COSTA; LIMA, 2023, p. 53).

Além disso, destaca-se que ataques dessa natureza são cada vez mais frequentes. Hiago Kin, presidente do Instituto Brasileiro de Resposta a Incidentes Cibernéticos, aponta que ocorrem “duas ou três vezes por ano, mas costumam ser abafados pelas instituições” (apud g1, 2025). Esse dado demonstra que a dimensão do problema tende a ser maior do que a divulgada publicamente.

Do ponto de vista regulatório, a Resolução nº 4.658/2018 prevê políticas de segurança cibernética e controles de acesso, mas não detalha exigências para certificação periódica de fornecedores. Essa lacuna precisa ser revista para assegurar que prestadores de serviços, como a C&M Software, cumpram padrões equivalentes aos exigidos das instituições financeiras.

Em síntese, o estudo evidencia que ataques à cadeia de suprimentos são favorecidos pela combinação de dependência tecnológica crescente, confiança excessiva em fornecedores e fragilidades na governança de acessos privilegiados. Esses fatores, articulados, representam risco sistêmico real ao sistema financeiro, justificando medidas de prevenção mais abrangentes e fiscalização constante.

**Considerações Finais**

O presente artigo teve como objetivo analisar criticamente o ataque cibernético ocorrido em julho de 2025, que impactou instituições financeiras brasileiras por meio da exploração de vulnerabilidades na cadeia de suprimentos da C&M Software. A investigação partiu da hipótese de que falhas na governança de acessos privilegiados e na fiscalização de fornecedores críticos representam riscos sistêmicos relevantes ao sistema financeiro nacional.

Com base na análise documental de fontes jornalísticas, relatórios técnicos e estudos acadêmicos, constatou-se que o ataque seguiu um padrão sofisticado: engenharia social para obtenção de credenciais privilegiadas, escalonamento de acessos e execução rápida de transações financeiras, convertidas em criptoativos para dificultar o rastreamento. Entre os principais resultados da pesquisa, destaca-se que, mesmo com investimentos robustos em segurança da informação por parte das instituições financeiras, a fragilidade de prestadores de serviços terceirizados ainda representa uma ameaça significativa à estabilidade e à reputação do ecossistema financeiro.

Além do impacto financeiro estimado, o estudo evidenciou efeitos reputacionais, operacionais e sistêmicos que comprometem a confiança nas operações digitais. Reforçou-se, também, que ataques dessa natureza não são casos isolados, mas parte de um fenômeno mais amplo e recorrente que exige maior atenção.

Conclui-se, assim, que medidas como auditorias constantes, fortalecimento da governança de acessos, treinamento contra engenharia social e fiscalização regulatória mais rigorosa são fundamentais para mitigar riscos semelhantes. A pesquisa contribui ao destacar a necessidade de estratégias integradas de prevenção e resposta, reforçando que a proteção do sistema financeiro depende não apenas de tecnologia avançada, mas também de uma cultura organizacional orientada à segurança e responsabilidade compartilhada entre instituições, fornecedores e reguladores.

**Referências**

COSTA, João Ferreira; LIMA, Rafael da Silva. Riscos cibernéticos na cadeia de suprimentos financeira: desafios e perspectivas no Brasil. Revista Brasileira de Segurança da Informação, v. 12, n. 3, p. 45–61, 2023.

KIM, Seung; PARK, Jihoon; CHOI, Young. Supply Chain Attacks and Financial Systems: A Systematic Review. Journal of Cybersecurity, v. 8, n. 1, p. 1–15, 2022.

SOUSA, Marcelo Lopes; ALMEIDA, Thiago Pereira. Governança de TI e risco cibernético: análise das instituições financeiras brasileiras. Revista de Gestão e Tecnologia, v. 17, n. 2, p. 23–40, 2021.

CONSELHO MONETÁRIO NACIONAL. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=4658. Acesso em: 03 jul. 2025.

BOLZANI, Isabela; HELDER, Darlan. Ataque hacker ao sistema financeiro: o que se sabe sobre o golpe e quais os próximos passos. In.: G1 Economia. 03 jul. 2025. Disponível em: https://g1.globo.com/economia/noticia/2025/07/03/ataque-hacker-sistema-financeiro.ghtml. Acesso em: 03 jul. 2025.

1. Graduado em Análise e Desenvolvimento de Sistemas, Especialista em Inteligência Artificial pela FACUMINAS, Instrutor da Cisco Networking Academy, Líder regional da ANETI-AM e Docente dos cursos: Sistemas de Informação, Engenharia de Software, Engenharia da Computação, Ciência da Computação do Centro Universitário Fametro, e-mail: alexsand.souza@fametro.edu.br. [↑](#footnote-ref-1)