Apresentação: 08/07/2025 18:46:50.510 - Mesa
RIC n.4129/2025

Câmara dos Deputados
Gabinete do Deputado Capitão Alberto Neto

REQUERIMENTO DE INFORMAÇÃO

(Do Sr. Cap. Alberto Neto)

Requer do Excelentíssimo Ministro da Fazenda, Senhor Fernando Haddad, informações sobre o ataque cibernético ao Banco Central.

Senhor Presidente,

Com fundamento no art. 50, § 2º, da Constituição Federal, combinado com os arts. 115 e 116 do Regimento Interno da Câmara dos Deputados requeiro seja encaminhado ao Excelentíssimo Ministro da Fazenda, Senhor Fernando Haddad, solicitação de informações sobre o ataque cibernético ao Banco Central. Diante do exposto solicito resposta para os seguintes questionamentos:

1) Ministro, como o Ministério da Fazenda coordenou a resposta governamental ao maior ataque cibernético já registrado contra o sistema financeiro brasileiro, que resultou no desvio de R$ 541 milhões, e quais medidas emergenciais foram adotadas para proteger a estabilidade do sistema financeiro nacional?
2) Considerando que o ataque afetou empresas de "banking as a service" e resultou na suspensão de seis instituições do Pix, como o ministério avalia o impacto deste episódio na confiança dos usuários no sistema financeiro digital brasileiro, e que estratégias estão sendo implementadas para manter a credibilidade do Pix?
3) Diante da vulnerabilidade exposta na C&M Software, empresa que conecta múltiplas instituições ao Sistema de Pagamentos Brasileiro, que mudanças regulatórias o ministério está propondo para fortalecer a

CD259143689300
Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD259143689300
Assinado eletronicamente pelo(a) Dep. Capitão Alberto Neto

Apresentação: 08/07/2025 18:46:50.510 - Mesa
RIC n.4129/2025

supervisão de prestadores de serviços tecnológicos críticos ao sistema financeiro?

4) Ministro, este ataque evidenciou lacunas na segurança cibernética do setor financeiro. Como o ministério pretende articular com outros órgãos a criação de uma política nacional mais robusta de segurança cibernética para instituições financeiras, incluindo prestadores de serviços terceirizados?
5) Considerando que o ataque afetou principalmente instituições menores e fintechs, como o ministério pretende garantir que consumidores e pequenas instituições financeiras tenham proteção adequada contra ataques cibernéticos, sem prejudicar a inovação e competitividade do setor?
6) Qual é a estratégia do ministério para recuperar os R$ 541 milhões desviados, especialmente considerando que parte foi convertida em criptomoedas, e como o governo está fortalecendo os mecanismos de combate ao crime organizado cibernético no setor financeiro?
7) Como o ministério avalia o risco sistêmico representado por este tipo de ataque, onde um único prestador de serviços pode afetar múltiplas instituições, e que medidas preventivas estão sendo consideradas para reduzir a concentração de risco em provedores tecnológicos críticos?
8) Ministro, considerando que ataques cibernéticos são uma ameaça global, como o Brasil está cooperando com outros países na troca de informações sobre segurança cibernética financeira, e que ajustes nos marcos regulatórios nacionais estão sendo estudados com base em melhores práticas internacionais?

Justificativa

O Banco Central brasileiro implementou uma resposta firme ao maior ataque cibernético já registrado contra o sistema financeiro nacional, suspendendo cautelarmente seis instituições financeiras do sistema Pix por suspeita de envolvimento no recebimento de recursos desviados. O caso, que

CD259143689300

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD259143689300
Assinado eletronicamente pelo(a) Dep. Capitão Alberto Neto

Apresentação: 08/07/2025 18:46:50.510 - Mesa
RIC n.4129/2025

se tornou um marco na segurança cibernética financeira do país, começou na terça-feira, 1º de julho de 2025, quando hackers atacaram a infraestrutura da C&M Software, empresa especializada em "banking as a service" que conecta diversas instituições financeiras ao Sistema de Pagamentos Brasileiro.

A primeira onda de suspensões ocorreu no dia 4 de julho, atingindo a Transfeera, Soffy e Nuoro Pay. Posteriormente, na noite do mesmo dia, três novas instituições foram desconectadas do sistema: Brasil Cash, S3 Bank e Voluti Gestão Financeira. As suspensões, válidas por até 60 dias, são amparadas pelo Artigo 95-A da Resolução 30 do Banco Central, que regulamenta o Pix e permite a suspensão preventiva de participantes cuja conduta possa comprometer o funcionamento do sistema.

A C&M Software, fundada em 1999, opera como intermediária tecnológica entre bancos e o Sistema de Pagamentos Brasileiro, oferecendo serviços essenciais para o funcionamento de transações financeiras, incluindo operações via Pix. O ataque comprometeu especificamente o ambiente de mensageria da empresa, permitindo que criminosos acessassem contas de reserva que as instituições financeiras mantêm no Banco Central para cumprir exigências regulamentares.

O prejuízo total do ataque foi estimado em R$ 541 milhões pela Polícia Civil de São Paulo, embora fontes não oficiais apontem para valores próximos a R$ 1 bilhão. A BMP Money Plus, empresa que oferece soluções de conta transacional, foi a mais afetada, perdendo R$ 541 milhões. A instituição, que não atende clientes físicos e foca em soluções para empresas, informou possuir colaterais suficientes para cobrir integralmente o valor impactado, garantindo que não haveria prejuízo para sua operação ou parceiros comerciais.

O modus operandi dos criminosos envolveu a conversão dos recursos desviados em criptomoedas através de transferências Pix, aproveitando-se da rapidez e da liquidez do sistema de pagamentos instantâneos. Entre as instituições que receberam parte dos recursos desviados, destaca-se a Soffy Soluções de Pagamento, que teve uma conta

CD259143689300

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD259143689300
Assinado eletronicamente pelo(a) Dep. Capitão Alberto Neto

Apresentação: 08/07/2025 18:46:50.510 - Mesa
RIC n.4129/2025

com R$ 270 milhões bloqueada judicialmente, representando uma parcela significativa do montante total desviado.

A investigação conduziu à prisão de João Nazareno Roque, de 48 anos, ex-funcionário da C&M Software que trabalhava como técnico em informática. Roque, que possuía renda declarada de R$ 2.500 e residia em um conjunto habitacional em Pirituba, zona norte de São Paulo, confessou ter fornecido credenciais de acesso aos criminosos em troca de R$ 15 mil. Segundo o delegado responsável pela investigação, Renato Topan, o funcionário foi cooptado em março e manteve contato com pelo menos quatro pessoas diferentes, encontrando-se pessoalmente com apenas uma delas em um bar na região.

As instituições suspensas reagiram de forma variada às medidas do Banco Central. A Transfeera confirmou que suas operações continuam normais, exceto pelo Pix, enfatizando que seus clientes não foram diretamente afetados e que a empresa está colaborando com as autoridades. A Voluti Gestão Financeira informou que, ao identificar transações suspeitas, acionou seu sistema antifraude, bloqueando contas e valores suspeitos, além de ter devolvido os valores através do Mecanismo Especial de Devolução. A Brasil Cash ressaltou que não foi alvo direto do ataque e que nenhum dado de cliente foi comprometido, implementando reforços adicionais de segurança.

O caso representa um marco na história da segurança cibernética do sistema financeiro brasileiro, demonstrando tanto as vulnerabilidades quanto a capacidade de resposta das autoridades reguladoras. A Polícia Federal, a Polícia Civil de São Paulo e o Banco Central trabalham em conjunto nas investigações, que continuam em andamento para identificar outros possíveis envolvidos e rastrear o destino final dos recursos desviados.

Sendo a fiscalização uma das funções típicas do legislador, faz-se necessária a aprovação deste requerimento de informações para obtenção de dados suficientes a respeito da atuação do Poder Executivo, a fim de se assegurar a efetividade das leis ou, se assim for necessário, tomar medidas para que sejam implementadas de forma eficiente e transparente.

CD259143689300

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD259143689300
Assinado eletronicamente pelo(a) Dep. Capitão Alberto Neto

Câmara dos Deputados
Gabinete do Deputado Capitão Alberto Neto

Termos em que, pede deferimento.

Brasília, 08 de Julho de 2025.

CAPITÃO ALBERTO NETO

Deputado Federal / PL-AM

Apresentação: 08/07/2025 18:46:50.510 - Mesa
RIC n.4129/2025

CD259143689300

Para verificar a assinatura, acesse https://infoleg-autenticidade-assinatura.camara.leg.br/CD259143689300
Assinado eletronicamente pelo(a) Dep. Capitão Alberto Neto