



BANCO CENTRAL DO BRASIL

DECISÃO 1593/2025-BCB/DERAD, DE 17 DE DEZEMBRO DE 2025

Processo de Apuração de Descumprimento do
Regulamento do Pix – Sumup Sociedade de
Crédito Direto S.A. – PE 269778

1. A Sumup Sociedade de Crédito Direto S.A. (Sumup), CNPJ 37.241.230/0001-52, foi notificada para apresentar defesa no presente processo de apuração de descumprimento do Regulamento do Pix, em razão do descumprimento a seguir descrito:

1.1 Descumprimento do Regulamento do Pix: deixar de atender requisitos técnicos de segurança do Pix, tendo como consequência incidente de segurança com comprometimento da confidencialidade de informações vinculadas a chaves Pix.

1.1.1 Capitulação:

- art. 84-B, incisos I e II, do Regulamento Anexo à Resolução BCB nº 1, de 12 de agosto de 2020 (Regulamento do Pix);
- Manual Operacional do Diretório de Identificadores de Contas Transacionais – DICT, versão 7.1, seção 13, itens 13.2.2 e 13.2.3;
- Manual de Segurança do Pix, versão 3.6, seção 6, item 5.

1.1.2 Descrição das ocorrências:

- no período de 28.9.2023 a 16.3.2024, houve quantidade elevada de consultas de chaves Pix por um conjunto de clientes da Sumup;
- no curso da apuração iniciada pelo Banco Central do Brasil – BCB, a participante informou:
 - ter feito avaliação minuciosa do comportamento dos usuários reportados e encerrado o relacionamento com esses usuários, além de atuar para implementar solução de monitoramento que considerasse não apenas a quantidade de consultas de chaves Pix, mas também se a consulta havia resultado em liquidação;
 - o conjunto de informações que era exibido aos usuários solicitantes das consultas de chaves Pix era: (i) nome do detentor da chave Pix; (ii) número da agência e da conta vinculada à chave Pix; (iii) instituição recebedora vinculada à chave Pix; e (iv) número de CPF mascarado, se usuário final pessoa natural;
 - chegou-se à identificação de 34 usuários com comportamento atípico de consultas de chaves Pix no período de 28.9.2023 a 16.3.2024, os quais teriam realizado requisições de consultas de chaves Pix não existentes e 140.943 consultas ao DICT de chaves Pix válidas;
- em que pese a Sumup ter, emergencialmente, bloqueado os usuários suspeitos e ter iniciado a identificação e correção de falhas, as informações disponíveis apontaram, no período do evento, para desconformidades em relação ao Manual de Segurança do Pix, ao Manual Operacional do DICT e ao Regulamento do Pix, o que ensejou notificação à



BANCO CENTRAL DO BRASIL

participante para que adotasse práticas a fim de sanar as deficiências identificadas e garantir a manutenção da aderência de sua atuação aos normativos pertinentes;

- as análises da resposta à notificação e dos esclarecimentos adicionais encaminhados pela Sumup levaram à conclusão de que a participante se adequou às disposições regulamentares do Pix das quais havia indicação de descumprimento.

2. Em 12.11.2025, foi proferida a Decisão 1415/2025-BCB/Derad (doc. 36), que aplicou a pena de multa de R\$252.000,00 a Sumup Sociedade de Crédito Direto S.A., tendo em vista a caracterização do descumprimento do regulamento do Pix de deixar de atender requisitos técnicos de segurança do Pix, tendo como consequência incidente de segurança com comprometimento da confidencialidade de informações vinculadas a chaves Pix.

3. Entretanto, à época da comunicação da referida decisão, os procuradores da participante encaminharam *e-mail* consignando a não consideração, na Decisão, da defesa protocolada em 14.6.2024 (doc. 44), que teria sido, então, apresentada tempestivamente e não se encontrava nos autos. Dessa forma, diante do prejuízo ao exercício regular do direito ao contraditório e à ampla defesa, e após a devida juntada do documento de defesa (doc. 41), o processo será reanalisado a fim de considerar as razões defensivas.

4. Regularmente notificada (docs. 26-29), a participante apresentou defesa tempestiva (doc. 41) alegando, em síntese, que:

- adotou voluntariamente os procedimentos e mecanismos necessários para reparar as deficiências e danos decorrentes do incidente de segurança ocorrido;
- para solucionar as deficiências relacionadas ao fornecimento de informações via interface de programação de aplicações – API do Pix, revisitou, logo após o incidente, seus sistemas e tecnologias para assegurar o fornecimento de informações estritamente necessárias para o correto funcionamento dos aplicativos e garantir o uso exclusivo de sua rede interna de informações de CPF completo, dados de agência e conta de usuários recebedores e informações relacionadas à segurança da chave Pix, correções finalizadas em 25.3.2024;
- como resultado e, ainda, para evitar eventual comprometimento de informações, removeu também os dados de agência e conta dos usuários recebedores das APIs do Pix e da tela do aplicativo;
- com relação à deficiência relacionada à política interna de limitação de consultas de chaves Pix, logrou êxito em implementá-la com parâmetros e requisitos mais restritivos do que o *token bucket*, algoritmo utilizado pelo Pix para fins de mecanismo de limitação, tendo promovido uma camada de proteção maior para limitar o envio excessivo de requisições;
- quanto à deficiência relativa aos mecanismos de identificação e tratamento de casos de excessivas consultas de chaves Pix que não resultem no envio de ordem de pagamento, implementou mecanismos de controle da relação entre o volume de consultas (VCD) ao DICT e o envio de ordens ao Sistema de Pagamentos Instantâneos – SPI (EOS), em escala de uma hora e mecanismo de verificação do número de consultas de um usuário que não resultem em ordem de pagamento, no período de uma hora;
- quanto à deficiência relacionada aos mecanismos de identificação e tratamento de casos de excessivas consultas de chaves Pix não registradas no DICT, foi implementado



BANCO CENTRAL DO BRASIL

mecanismo com o objetivo de assegurar que, no caso de a relação de chaves Pix NOT FOUND e FOUND ser superior ao parâmetro definido como anômalo, os usuários pagadores e as transações realizadas sejam enviados para análise manual do time de prevenção a fraudes;

- a acusação desconsiderou a baixa lesão ou risco de lesão à imagem, à integridade, à confiabilidade e à segurança do Pix, ainda que se trate de incidente de segurança com dados pessoais, uma vez que o percentual do total de chaves Pix potencialmente comprometidas em relação ao total de chaves Pix registradas no DICT na data de cessação do incidente foi de, aproximadamente, 0,02%, parcela quase irrisória tendo em vista as operações da Sumup e, principalmente, do SPI, de modo que o incidente não foi capaz de gerar lesão relevante ao ambiente Pix;
- tampouco se verificou lesão aos usuários impactados, indícios de roubo de conta, violação ou tentativa de violação dos sistemas da participante, tentativa de utilização dos dados para qualquer outra finalidade nem indícios de comercialização e cessão dos dados afetados a terceiros;
- após o incidente, a Sumup prontamente bloqueou a conta dos usuários que realizaram consultas em alto volume, revisou e alterou limites de consultas diárias e por minuto a chaves Pix, removeu a disponibilização de informações como número de agência e conta após consulta de chaves Pix e desenvolveu mecanismos para comparar volumes de consultas de chaves Pix com o volume de liquidações das transações;
- a inexistência de risco ou dano relevante aos usuários pode ser corroborada pela análise de critérios trazidos pelo art. 5º da Resolução CD/ANPD nº 15, de 24 de abril de 2024, o qual estabelece que o incidente de segurança poderá resultar em risco ou dano relevante ao titular quando atingir, cumulativamente, dois critérios: (i) afetar significativamente interesses e direitos fundamentais dos titulares; e (ii) envolver (a) dados pessoais sensíveis, (b) dados de crianças, adolescentes e idosos, (c) dados financeiros, (d) dados de autenticação em sistemas, (e) dados protegidos por sigilo legal, judicial ou profissional ou (f) dados em larga escala;
- um incidente de segurança afetará significativamente interesses e direitos fundamentais dos titulares quando puder impedir o exercício de direitos ou a utilização de um serviço ou quando ocasionar danos materiais ou morais aos usuários afetados, hipóteses que não se confirmaram no caso concreto, visto que os dados potencialmente comprometidos foram apenas, nome, número de agência e conta, instituição recebedora vinculada à chave Pix e CPF;
- tal entendimento está inclusive em linha com a nota publicada pelo BCB em 22.3.2024, que afirmou que *“não foram expostos dados sensíveis, tais como senhas, informações de movimentações ou saldos financeiros em contas transacionais, ou quaisquer outras informações sob sigilo bancário”, mas “mesmo não sendo exigido pela legislação vigente, por conta do baixo impacto potencial para os usuários, o BC decidiu comunicar o evento à sociedade, à vista do compromisso com a transparência que rege sua atuação”;*
- requer a não aplicação do art. 6º, § 2º, do Manual de Penalidades do Pix – uma vez que, conforme demonstrado, as ocorrências não acarretaram lesão ou perigo de lesão à imagem, à integridade, à confiabilidade e à segurança do Pix, – e a aplicação do art. 7º,



BANCO CENTRAL DO BRASIL

inciso I, uma vez que as ocorrências foram tempestivamente sanadas e não houve danos causados aos clientes e usuários do Pix.

5. Nos termos do art. 84-B, os participantes devem estabelecer procedimento de identificação e de tratamento dos casos de excessivas consultas de chaves Pix, por seus clientes, que não resultem em liquidação e que não estejam registradas no DICT.
6. Por sua vez, o Manual Operacional do DICT, em seus itens 13.2.2 e 13.2.3, determina que cada participante deve estabelecer política interna própria de limitação de consultas igual ou mais restritiva do que a aplicada pelo mecanismo de *Token Bucket* do DICT, de modo a prover camada de proteção anterior, que limite o envio excessivo de requisições e evite o estouro do balde do seus usuários e do próprio participante, além de implementar e manter mecanismos de acompanhamento das requisições feitas ao DICT por solicitação de seus usuários/clientes, que considere períodos curtos (horas) e longos (dias/meses) e tenha como objetivo a identificação e o bloqueio de casos suspeitos de ataque de leitura aos dados do DICT. Já o Manual de Segurança do Pix, em sua seção 6, item 5, estabelece que os sistemas e APIs devem fornecer apenas informações estritamente necessárias para o correto funcionamento dos aplicativos do participante.
7. Os seguintes fatos evidenciam que a Sumup deixou de atender requisitos técnicos de segurança do Pix:
 - a. deficiência nos mecanismos que garantissem que as APIs relacionadas ao Pix fornecessem apenas as informações estritamente necessárias ao correto funcionamento dos aplicativos e que informações, como dados de agência e conta de destinatários de pagamento via Pix, bem como informações para fins de segurança vinculadas às chaves Pix, fossem de uso exclusivo dos sistemas internos da participante, em desacordo com o previsto na seção 6 do Manual de Segurança do Pix, haja vista a informação, posteriormente aos fatos, de plano de ação que reviu os sistemas para se adequar à determinação prevista na regulamentação aplicável (docs. 8; 10, págs. 1/2);
 - b. deficiência na implementação de política interna de limitação de consultas de chaves Pix, em desacordo com o previsto na seção 13 do Manual Operacional do DICT, haja vista a informação, posterior aos fatos, da implementação dessa política em patamar mais restritivo do que o aplicado pelo mecanismo *Token Bucket* do DICT (docs. 8; 10, pág. 2);
 - c. deficiência na implementação de mecanismos de identificação e tratamento de casos de excessivas consultas de chaves Pix que não resultem em envio de ordem de pagamento e que não estejam registradas no DICT, em desacordo com o art. 84-B do Regulamento do Pix, tendo em vista informação, posterior aos fatos, de implementação de rotinas e monitoramento para se adequar às determinações previstas na regulamentação aplicável (docs. 8; 10, págs. 2/3).
8. A insuficiência de mecanismos de proteção para prevenir ataques de leitura permitiu o acesso indevido a informações restritas vinculadas a chaves Pix por meio do uso irregular do DICT.



BANCO CENTRAL DO BRASIL

9. Não há controvérsia quanto ao incidente ocorrido, e a defesa não contesta as deficiências apuradas, reiterando as informações sobre os aprimoramentos feitos em seus sistemas para as devidas correções e argumentando pela baixa representatividade e lesividade do incidente. A esse respeito, cumpre esclarecer que a adoção de medidas saneadoras ou o atendimento às recomendações e determinações de correção, ainda que necessários e aptos a aprimorar os sistemas e mecanismos de segurança, não elidem o descumprimento já consumado. Quanto ao grau de representatividade e de lesividade, sua apreciação no âmbito a instauração do processo foi realizada com base no art. 93-A do Regulamento do Pix, que tratava das hipóteses de isenção da penalidade de multa, ocasião em que se concluiu que as infrações da Sumup não preenchem as condições para isenção da penalidade de multa (doc. 26).

10. Resta, portanto, caracterizado o descumprimento do Regulamento do Pix de deixar de atender requisitos técnicos de segurança, tendo como consequência incidente de segurança com comprometimento da confidencialidade de informações vinculadas a 140.943 chaves Pix, ocorrido entre 28.9.2023 e 16.3.2024.

11. À época dos fatos, o descumprimento sujeitava a participante às penalidades previstas no Regulamento Anexo à Resolução BCB nº 1, de 2020, com a regulamentação no Anexo I da Resolução BCB nº 177, de 22 de dezembro de 2021, alterado pela Resolução BCB nº 342, de 26 de setembro de 2023 (1º cenário). Em 1º.10.2024, entrou em vigor a Resolução BCB nº 361, de 7 de dezembro de 2023, que alterou dispositivos do Anexo I da Resolução BCB nº 177, de 2021, os quais, todavia, não guardam relação com o descumprimento tratado neste processo. Posteriormente, em 1º.10.2025, foi revogada a Resolução BCB nº 177, de 2021, passando a vigorar a Resolução BCB nº 507, de 26 de setembro de 2025, cujo Anexo I passou a regulamentar as penalidades previstas no Regulamento Anexo à Resolução BCB nº 1, de 2020, alterado, em 30.9.2025, pela Resolução BCB nº 506, de 26 de setembro de 2025 (2º cenário). Assim, em observância ao princípio constitucional da retroatividade benéfica (art. 5º, inciso XL, da Constituição Federal), é cabível a apuração da pena em cada cenário antes referido, selecionando-se aquele mais favorável à participante.

1º Cenário: Regulamento Anexo à Resolução BCB nº 1, de 2020, com regulamentação no Anexo I da Resolução BCB nº 177, de 2021, com as alterações da Resolução BCB nº 342, de 2023

12. O descumprimento enquadra-se no art. 84-B, incisos I e II, do Regulamento do Pix, nos itens 13.2.2 e 13.2.3 do Manual Operacional do DICT e na seção 6, item 5, do Manual de Segurança do Pix e sujeita a participante, de forma isolada ou cumulativa, às penalidades de multa, suspensão e exclusão, na forma do art. 93 do mesmo Regulamento, regulamentado no Anexo I à Resolução BCB nº 177, de 2021, com as alterações da Resolução BCB nº 342, de 2023 (Manual de Penalidades do Pix).

13. Para a penalidade de multa, o Manual de Penalidades do Pix fixa o valor-base de multa aplicável de R\$100.000,00 (art. 5º, inciso II, alínea “c”), multiplicado pelo fator de ponderação (FP) 3 (art. 5º, § 2º; Anexo II) – considerando FP1 = 2 (sociedade de crédito direto), FP2 = 0,5 (por representar 0,1% do total das transações Pix pagas e recebidas no Sistema de Pagamentos Instantâneos – SPI no período compreendido pelas três datas-bases anteriores à infração; doc. 35) e FP3 = 0,5 (por representar 0,0193% do total de chaves Pix potencialmente comprometidas em incidente de segurança em relação ao total de chaves Pix registradas no DICT



BANCO CENTRAL DO BRASIL

na data de cessação do evento; doc. 35) – o que resulta no valor-base final de multa de R\$300.000,00.

14. Considerando que a infração acarretou perigo de lesão à imagem, à integridade, à confiabilidade e à segurança do Pix e de terceiros (art. 6º, inciso I, alínea “a”), o que aumenta a pena em 20% (art. 6º, § 2º), aplica-se para esse cenário a multa de R\$360.000,00, que se torna a pena final na ausência de circunstâncias que reduzam a penalidade (art. 7º).

15. A aplicação do art. 7º, inciso I, para redução de penalidade, requerida pela participante, não se mostra cabível, visto que o redutor da pena é aplicado na hipótese de reparação dos danos causados, que não se confunde com o saneamento do descumprimento, que se verificou no caso concreto. Com relação à inaplicabilidade do art. 6º, inciso I, alínea “a”, reivindicada na defesa, o pedido não procede, visto que a infração acarretou perigo de lesão à imagem do Pix, situação evidenciada concretamente pela ampla e necessária divulgação da ocorrência ao público pelo BCB por ocasião do incidente, aplicando-se, portanto o referido dispositivo ao caso em exame.

16. Com relação às penalidades de suspensão e exclusão, não se vislumbra no caso concreto as hipóteses de aplicação dessas penas, conforme arts. 8º e 9º do Manual de Penalidades do Pix.

2º Cenário: Regulamento Anexo à Resolução BCB nº 1, de 2020, alterado pela Resolução BCB nº 506, de 2025, com regulamentação no Anexo I da Resolução BCB nº 507, de 2025

17. O descumprimento enquadra-se no art. 84-B, incisos I e II, do Regulamento Anexo à Resolução BCB nº 1, de 2020, alterado pela Resolução BCB nº 506, de 2025 (Regulamento do Pix), nos itens 13.2.2 e 13.2.3 do Manual Operacional do DICT e na seção 6, item 5, do Manual de Segurança do Pix e sujeita a participante, de forma isolada ou cumulativa, às penalidades de advertência, multa e exclusão, na forma do art. 93 do mesmo Regulamento, regulamentado no Anexo I à Resolução BCB nº 507, de 2025 (Manual de Penalidades do Pix).

18. Para a penalidade de multa, o Manual de Penalidades do Pix fixa o valor-base de multa de R\$100.000,00 a R\$300.000,00 (art. 18, inciso II, alínea “j”), multiplicado pelo fator de ponderação (FP) 3 (art. 18, § 2º; Anexo II), considerando que a participante possuía ativos totais de R\$409.779 mil em junho de 2025, o que resulta no valor-base de multa de R\$300.000,00 a R\$900.000,00.

19. Dessa forma, fixa-se o valor-base final em R\$300.000,00.

20. Considerando que a infração acarretou perigo de lesão à imagem do Pix (art. 20, inciso II), circunstância que aumenta a penalidade em 20% (art. 20, parágrafo único), e que houve o cumprimento total da notificação de que trata o art. 91-B do Regulamento do Pix no prazo estabelecido pelo BCB (art. 21, inciso II; doc. 25, págs. 4-6), circunstância que reduz a pena em 30%, aplica-se para esse cenário a penalidade de R\$252.000,00.

21. Com relação às penalidades de advertência e exclusão, não se vislumbra no caso concreto as hipóteses de aplicação dessas penas, conforme arts. 14, 23 e 24 do Manual de Penalidades do Pix.

22. Verifica-se, assim, que o 2º cenário é mais benéfico à participante, cabendo a retroação da regulamentação vigente.



BANCO CENTRAL DO BRASIL

23. Pelo exposto, DECIDO, com base na aplicação subsidiária do disposto no art. 53 da Lei nº 9.784, de 29 de janeiro de 1999, ANULAR a Decisão 1415/2025-BCB/Derad, de 12 de novembro de 2025, e, por consequência, seus efeitos (docs. 37/38), e aplicar a pena de MULTA de R\$252.000,00 (duzentos e cinquenta e dois mil reais) a Sumup Sociedade de Crédito Direto S.A., com fundamento no art. 93 do Regulamento Anexo à Resolução BCB nº 1, de 2020, alterado pela Resolução BCB nº 506, de 2025.

24. Comunique-se a decisão à participante, intimando-a ao recolhimento devido, no prazo de 30 (trinta) dias, contado conforme o art. 7º do Anexo I à Resolução BCB nº 507, de 2025, ressalvado o direito de recurso, nos termos do art. 11 do referido Anexo I, no mesmo período.

Climério Leite Pereira

Chefe do Departamento de Resolução e de Ação Sancionadora
(documento assinado digitalmente)