Informe SPI - 003/2026, de 10/02/2026

O Banco Central do Brasil comunica:

Reproduzimos o Comunicado aos Participantes do Pix 7/2026, desta data.

DEBAN - Departamento de Operações Bancárias e de Sistema de Pagamentos
Email: **spi@bcb.gov.br**

De: Pix- Seguranca (caixa Corporativa) <pix-seguranca@bcb.gov.br>
Assunto: [Comunicado aos Participantes do Pix 7/2026] - Gestão de certificados utilizados na comunicação com o SPI e o DICT

Gestão de certificados utilizados na comunicação com o SPI e o DICT

Os certificados utilizados pelos **participantes diretos** para estabelecimento do canal de comunicação com a **ICOM/SPI** e com o **DICT (CERTPIC)**, bem como aqueles utilizados para a **assinatura de mensagens e requisições (CERTPIA)** constituem o mecanismo de identificação e autenticação das informações enviadas ao Banco Central. Nesse sentido, **a proteção e a guarda das chaves privadas** desses certificados é um dos processos de **cibersegurança** mais críticos para o bom funcionamento do **ecossistema Pix.**

Em razão dessa criticidade, **é indispensável que os participantes adotem, de forma sistemática e rigorosa**, os procedimentos de **emissão, substituição, desativação e revogação de certificados**, de modo a evitar o uso indevido de credenciais que já não devam mais ser consideradas válidas. Assim, sempre que ocorrer qualquer situação que envolva alteração **no ambiente tecnológico, no modelo de conexão** ou **nos fornecedores** que tenham acesso aos certificados, o participante deve adotar conjuntamente os seguintes procedimentos obrigatórios:

a. emissão de novos certificados **CERTPIC** e **CERTPIA**, conforme o caso;

b. desativação, **junto ao Banco Central do Brasil**, dos certificados anteriormente utilizados, nos termos da **seção 5.5 do Manual de Segurança do Pix**, o que inclui o

envio de mensagem por meio do **BC Correio** e o contato subsequente com a **Central de Atendimento do Pix**; e

c. revogação dos certificados antigos junto à respectiva **autoridade certificadora (AC).**

Os procedimentos "a", "b" e "c", acima, **devem ser todos observados, entre outras, nas seguintes situações:**

1. descontinuidade de uso de determinado certificado, por qualquer motivo;
2. mudança de Provedor de Serviços de Tecnologia da Informação (PSTI);
3. migração do modelo de conexão via PSTI para conexão direta;
4. mudança de fornecedor que, em razão dos serviços prestados, detenha ou tenha acesso aos certificados do participante, sejam eles **CERTPIC** ou **CERTPIA**; e
5. confirmação ou forte suspeita de fraude/ataque. Nessa hipótese, o PSP deve adotar **medidas imediatas de contenção**, incluindo a **substituição conjunta dos certificados CERTPIC e CERTPIA** e, quando aplicável, **o bloqueio imediato no módulo SPI do SPB-Web**, como forma de interromper a continuidade do ataque.

Ressalte-se que, em caso de confirmação ou forte suspeita de fraude ou ataque cibernético, é recomendada a substituição conjunta dos certificados CERTPIC e CERTPIA, **independentemente de a exposição ter sido identificada em apenas um deles**, como medida preventiva de mitigação de risco.

A ausência de observância dos procedimentos acima pelo PSP pode resultar na **continuidade da aceitação, pelo Banco Central, de mensagens enviadas ou assinadas com certificados anteriormente utilizados**, ampliando de forma indevida a superfície de ataque dos participantes.

Ressalte-se, ainda, que o procedimento de desativação **não se aplica a certificados já vencidos**, uma vez que, nesses casos, mensagens e conexões associadas a tais certificados são automaticamente rejeitadas pelos sistemas do Banco Central.

Por fim, destaca-se que os requisitos e procedimentos de segurança previstos na regulamentação aplicável ao Pix, bem como nos **Manuais de Segurança do Pix** e de **Segurança do SFN**, são de **observância obrigatória** por **todos os participantes**.

Em caso de dúvidas, entrar em contato com a Central de Atendimento de TI do Pix, pelo e-mail suporte.pix@bcb.gov.br.

Por favor, não responder a esse e-mail.