BANCO CENTRAL DO BRASIL

CIRCULAR Nº 3.909, DE 16 DE AGOSTO 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

A Diretoria Colegiada do Banco Central do Brasil, em sessão realizada em 15 de agosto de 2018, com base nos arts. 9º, 10 e 15 da Lei nº 12.865, de 9 de outubro de 2013, e tendo em vista o art. 14 da Resolução nº 4.282, de 4 de novembro de 2013,

R E S O L V E :

CAPÍTULO I
DO OBJETO E DO ÂMBITO DE APLICAÇÃO

Art. 1º Esta Circular 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

CAPÍTULO II
DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Seção I
Da Implementação da Política de Segurança Cibernética

Art. 2º As instituições de pagamento devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

§ 1º A política mencionada no **caput** deve ser compatível com:

I - o porte, o perfil de risco e o modelo de negócio da instituição;

II - a natureza das atividades da instituição e a complexidade dos produtos e serviços oferecidos; e

III - a sensibilidade dos dados e das informações sob responsabilidade da instituição.

§ 2º Admite-se que as instituições de pagamento integrantes de conglomerado prudencial adotem política de segurança cibernética única do conglomerado prudencial, nos termos da regulamentação em vigor, desde que compatível com o disposto neste Capítulo.

§ 3º As instituições de pagamento que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2º devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição.

Art. 3º A política de segurança cibernética deve contemplar, no mínimo:

I - os objetivos de segurança cibernética da instituição de pagamento;

II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição de pagamento a incidentes e atender aos demais objetivos de segurança cibernética;

III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição de pagamento;

V - as diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição de pagamento;

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição de pagamento, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com instituições de pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

§ 1º Na definição dos objetivos de segurança cibernética referidos no inciso I do **caput**, deve ser contemplada a capacidade da instituição de pagamento para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

§ 2º Os procedimentos e os controles de que trata o inciso II do **caput** devem abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra **softwares** maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

§ 3º Os procedimentos e os controles citados no inciso II do **caput** devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição de pagamento.

§ 4º O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do **caput**, devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

§ 5º As diretrizes de que trata o inciso V, alínea "b", do **caput** devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição de pagamento.

Seção II
Da Divulgação da Política de Segurança Cibernética

Art. 4º A política de segurança cibernética deve ser divulgada aos funcionários da instituição de pagamento e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

Art. 5º As instituições de pagamento devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

Seção III
Do Plano de Ação e de Resposta a Incidentes

Art. 6º As instituições de pagamento devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética.

Parágrafo único. O plano mencionado no **caput** deve abranger, no mínimo:

I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Art. 7º As instituições de pagamento devem designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

Parágrafo único. O diretor mencionado no **caput** pode desempenhar outras funções na instituição, desde que não haja conflito de interesses.

Art. 8º As instituições de pagamento devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6º, com data-base de 31 de dezembro.

§ 1º O relatório de que trata o **caput** deve abordar, no mínimo:

I - a efetividade da implementação das ações descritas no art. 6º, parágrafo único, inciso I;

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos no art. 6º, parágrafo único, inciso II;

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV - os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

§ 2º O relatório mencionado no **caput** deve ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base.

Art. 9º A política de segurança cibernética referida no art. 2º e o plano de ação e de resposta a incidentes mencionado no art. 6º devem ser aprovados pelo conselho de administração ou, na sua inexistência, pela diretoria da instituição de pagamento.

Art. 10. A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

CAPÍTULO III
DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Art. 11. As instituições de pagamento devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior.

Art. 12. As instituições de pagamento, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II - a verificação da capacidade do potencial prestador de serviço de assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos usuários finais da instituição por meio de controles físicos ou lógicos; e

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição.

§ 1º Na avaliação da relevância do serviço a ser contratado, mencionada no inciso I do **caput**, a instituição contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação realizada nos termos do art. 3º, inciso V, alínea "c".

§ 2º Os procedimentos de que trata o **caput**, inclusive as informações relativas à verificação mencionada no inciso II, devem ser documentados.

§ 3º No caso da execução de aplicativos por meio da internet, referidos no art. 13, inciso III, a instituição deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

§ 4º A instituição deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos nos termos da alínea "f" do inciso II do **caput**.

Art. 13. Para os fins do disposto nesta Circular, os serviços de computação em nuvem abrangem a disponibilidade à instituição de pagamento contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar **softwares**, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

Art. 14. A instituição de pagamento contratante dos serviços mencionados no art. 12 é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

~~Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada pelas instituições de pagamento ao Banco Central do Brasil.~~

Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições de pagamento ao Banco Central do Brasil. (Redação dada pela Circular nº 3.969, de 13/11/2019.)

§ 1º A comunicação de que trata o **caput** deve conter as seguintes informações:

I - a denominação da empresa a ser contratada;

II - os serviços relevantes a serem contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

~~§ 2º A comunicação de que trata o **caput** deve ser realizada, no mínimo, sessenta dias antes da contratação dos serviços.~~

§ 2º A comunicação de que trata o **caput** deve ser realizada até dez dias após a contratação dos serviços. (Redação dada pela Circular nº 3.969, de 13/11/2019.)

~~§ 3º As alterações contratuais que impliquem modificação das informações de que trata o § 1º devem ser comunicadas ao Banco Central do Brasil, no mínimo, sessenta dias antes da alteração contratual.~~

§ 3º As alterações contratuais que impliquem modificação das informações de que trata o § 1º devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual. (Redação dada pela Circular nº 3.969, de 13/11/2019.)

~~§ 4º A comunicação de que trata o **caput** poderá ser realizada em prazo inferior ao disposto nos §§ 2º e 3º em casos excepcionais, para garantir o regular funcionamento da instituição de pagamento e desde que acompanhada de justificativa fundamentada.~~

§ 4º (Revogado pela Circular nº 3.969, de 13/11/2019.)

Art. 16. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos:

I - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

II - a instituição de pagamento contratante deve assegurar que a prestação dos serviços referidos no **caput** não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

III - a instituição de pagamento contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

IV - a instituição de pagamento contratante deve prever alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

~~§ 1º No caso de inexistência de convênio nos termos do inciso I do **caput**, a instituição de pagamento contratante deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações requeridas nos termos do art. 15 desta Circular.~~

§ 1º No caso de inexistência de convênio nos termos do inciso I do **caput**, a instituição de pagamento contratante deverá solicitar autorização do Banco Central do Brasil para: (Redação dada pela Circular nº 3.969, de 13/11/2019.)

I - a contratação do serviço, no prazo mínimo de sessenta dias antes da contratação, observado o disposto no art. 15, § 1º, desta Circular; e (Incluído pela Circular nº 3.969, de 13/11/2019.)

II - as alterações contratuais que impliquem modificação das informações de que trata o art. 15, § 1º, observando o prazo mínimo de sessenta dias antes da alteração contratual. (Incluído pela Circular nº 3.969, de 13/11/2019.)

§ 2º Para atendimento aos incisos II e III do **caput**, as instituições deverão assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições de pagamento contratantes e do Banco Central do Brasil aos dados e às informações.

§ 3º A comprovação do atendimento aos requisitos de que tratam os incisos I a IV do **caput** e o cumprimento da exigência de que trata o § 2º devem ser documentados.

Art. 17. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

I - a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I;

III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;

IV - a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição de pagamento contratante; e

b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

V - o acesso da instituição de pagamento contratante a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III;

b) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas "d" e "e"; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12, inciso II, alínea "f";

VI - a obrigação de a empresa contratada notificar a instituição de pagamento contratante sobre a subcontratação de serviços relevantes para a instituição;

VII - a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

VIII - a adoção de medidas pela instituição de pagamento contratante, em decorrência de determinação do Banco Central do Brasil; e

IX - a obrigação de a empresa contratada manter a instituição de pagamento contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Parágrafo único. O contrato mencionado no **caput** deve prever, para o caso da decretação de regime de resolução da instituição de pagamento contratante pelo Banco Central do Brasil:

I - a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do **caput**, que estejam em poder da empresa contratada; e

II - a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da instituição de pagamento contratante.

Art. 18. O disposto nos arts. 11 a 17 não se aplica à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado.

CAPÍTULO IV
DISPOSIÇÕES GERAIS

Art. 19. As instituições de pagamento devem assegurar que suas políticas previstas na estrutura de gerenciamento de riscos, nos termos da regulamentação em vigor, disponham, no tocante à continuidade dos serviços de pagamento prestados, sobre:

I - o tratamento dos incidentes relevantes relacionados com o ambiente cibernético de que trata o art. 3º, inciso IV;

II - os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição; e

III - os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados de que trata o art. 3º, inciso V, alínea "a".

Art. 20. Os procedimentos adotados pelas instituições de pagamento para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade dos serviços de pagamento prestados:

I - o tratamento previsto para mitigar os efeitos dos incidentes relevantes de que trata o art. 3º, inciso IV, e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

II - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, citados no inciso I; e

III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, que configurem uma situação de crise pela instituição de pagamento, bem como das providências para o reinício das suas atividades.

Art. 21. As instituições de pagamento devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

I - a definição de processos, testes e trilhas de auditoria;

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

§ 1º As notificações recebidas sobre a subcontratação de serviços relevantes descritas no art. 17, inciso VI, devem ser consideradas na definição dos mecanismos de que trata o **caput**.

§ 2º Os mecanismos de que trata o **caput** devem ser submetidos a testes periódicos pela auditoria interna compatíveis com os controles internos da instituição.

Art. 22. Sem prejuízo do dever de sigilo e da livre concorrência, as instituições de pagamento devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes de que trata o art. 3º, inciso IV.

§ 1º O compartilhamento de que trata o **caput** deve abranger informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros.

§ 2º As informações compartilhadas devem estar disponíveis ao Banco Central do Brasil.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 23. Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I - o documento relativo à política de segurança cibernética, de que trata o art. 2º;

II - a ata de reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição, no caso de ser formalizada a opção de que trata o art. 2º, § 2º;

III - o documento relativo ao plano de ação e de resposta a incidentes, de que trata o art. 6º;

IV - o relatório anual, de que trata o art. 8º;

V - a documentação sobre os procedimentos de que trata o art. 12, § 2º;

VI - a documentação de que trata o art. 16, § 3º, no caso de serviços prestados no exterior;

VII - os contratos de que trata o art. 17, contado o prazo referido no **caput** a partir da extinção do contrato; e

VIII - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 21, contado o prazo referido no **caput** a partir da implementação dos citados mecanismos.

Art. 24. As instituições de pagamento que, na data de entrada em vigor desta Circular, já tiverem contratado a prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem apresentar ao Banco Central do Brasil, no prazo máximo de noventa dias, contados a partir da data de entrada em vigor desta Circular, cronograma para adequação:

I - ao cumprimento do disposto no art. 16, incisos I, II, IV e § 2º, no caso de serviços prestados no exterior; e

II - ao disposto nos arts. 15, § 1º, e 17.

Parágrafo único. O prazo previsto no cronograma para adequação mencionado no **caput** não pode ultrapassar 31 de dezembro de 2021.

Art. 25. A aprovação da política de segurança cibernética e do plano de ação e de resposta a incidentes, referida no art. 9º, deve ser realizada até noventa dias contados da data de entrada em vigor desta Circular.

Art. 26. O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto nesta Circular, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços e dos contratos correspondentes.

Art. 27. A Circular nº 3.681, de 4 de novembro de 2013, passa a vigorar com as seguintes alterações:

"Art. 2º .....

I - .....

.....

j) falhas em sistemas, processos ou infraestrutura de tecnologia da informação; e

....." (NR)

"Art. 3º .....

§ 1º A estrutura de gerenciamento de riscos mencionada no **caput** deve:

I - ser compatível com a natureza das atividades da instituição e a complexidade dos produtos e serviços oferecidos e proporcional à dimensão das exposições aos mencionados riscos;

II - ser segregada da unidade executora da atividade de auditoria interna;

III - permitir a identificação, a mensuração, o monitoramento, o controle, a mitigação e o gerenciamento contínuo e integrado dos riscos operacional, de liquidez e de crédito;

IV - prever políticas e estratégias aprovadas e revisadas, no mínimo anualmente, pela diretoria e pelo conselho de administração, se houver, a fim de determinar sua compatibilidade com os objetivos da instituição e com as condições de mercado; e

V - manter documentação acerca de suas políticas, estratégias de gerenciamento de riscos e governança à disposição do Banco Central do Brasil.

§ 2º As políticas e as estratégias previstas no inciso IV do § 1º devem contemplar os seguintes assuntos:

I - critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional; e

II - continuidade dos serviços de pagamento prestados." (NR)

"Art. 4º .....

.....

XV - notificação ao usuário final acerca de eventual não execução de uma transação;

XVI - mecanismos que permitam ao usuário final verificar se a transação foi executada corretamente;

XVII - critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores; e

XVIII - avaliação, gerenciamento e monitoramento do risco operacional decorrente de serviços terceirizados relevantes para o funcionamento regular da instituição de pagamento.

Parágrafo único. Caso as instituições de pagamento terceirizem funções relacionadas com a segurança dos serviços oferecidos, o respectivo contrato de prestação de serviços deve estipular que o contratado deverá:

I - atender ao disposto neste artigo; e

II - permitir o acesso da instituição de pagamento aos dados e às informações sobre os serviços prestados." (NR)

Art. 28. Fica revogado o parágrafo único do art. 3º da Circular nº 3.681, de 2013.

Art. 29. Esta Circular entra em vigor em 1º de setembro de 2019.

Otávio Ribeiro Damaso
Diretor de Regulação