BANCO CENTRAL DO BRASIL

EDITAL DE CONSULTA PÚBLICA 57/2017, DE 19 DE SETEMBRO DE 2017

Divulga proposta de resolução que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem, a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A Diretoria Colegiada do Banco Central do Brasil decidiu colocar em consulta pública minuta de resolução dispondo sobre a implementação, por parte das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, de política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

2. A proposta de resolução prevê a obrigatoriedade de as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil implementarem política de segurança cibernética e estabelece o conteúdo mínimo dessa política, bem como os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo exigências contratuais mínimas. A proposta traz, ainda, exigências quanto ao tratamento dos incidentes relacionados ao ambiente cibernético e prevê que as instituições devem desenvolver ações para o compartilhamento de informações sobre esses incidentes.

3. Essa iniciativa de regulação considera a crescente utilização de meios eletrônicos e de inovações tecnológicas no setor financeiro, o que requer que as instituições tenham controles e sistemas de segurança cibernética cada vez mais robustos, especialmente quanto à resiliência a ataques cibernéticos.

4. Dessa forma, a proposta apresenta regras específicas sobre o tema, que buscam fortalecer as estruturas de prevenção e de tratamento aos incidentes relacionados ao ambiente cibernético.

5. Destaca-se que a proposta prevê a vedação da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem no exterior. Especialmente sobre esse ponto, registra-se que a avaliação da proposta compreenderá, inclusive, argumentos e condições para eventual revisão ou ajuste de referida vedação.

6. A minuta está disponível no endereço do Banco Central do Brasil na internet, "www.bcb.gov.br", no *menu* do perfil geral "Legislação e normas", "Consultas Públicas", "Consultas Ativas"; e nas centrais de atendimento ao público, de 10 às 16 horas, nos seguintes endereços:

I - SBS, Quadra 3, Bloco "B" – Edifício-Sede – Segundo subsolo, Brasília (DF);

II - Boulevard Castilhos Franca, 708, Campina, Belém (PA);

III - Av. Álvares Cabral, 1.605, Santo Agostinho, Belo Horizonte (MG);

IV - Av. Cândido de Abreu, 344, Centro Cívico, Curitiba (PR);

V - Av. Heráclito Graça, 273, Centro, Fortaleza (CE);

VI - Rua 7 de setembro, 586, Centro, Porto Alegre (RS);

VII - Rua da Aurora, 1.259, Santo Amaro, Recife (PE);

VIII - Av. Presidente Vargas, 730, Centro, Rio de Janeiro (RJ);

IX - 1ª Avenida, 160, Centro Administrativo da Bahia, Salvador (BA); e

X - Av. Paulista, 1.804, Bela Vista, São Paulo (SP).

7. Os interessados poderão encaminhar sugestões e comentários até 21 de novembro de 2017, por meio:

I - do *link* contido no edital publicado no endereço eletrônico do Banco Central do Brasil;

II - do *e-mail* denor@bcb.gov.br; ou

III - de correspondência dirigida ao Departamento de Regulação do Sistema Financeiro (Denor), SBS, Quadra 3, Bloco "B", 9º andar, Edifício-Sede, Brasília (DF), CEP 70074-900.

8. Conforme o Comunicado nº 9.187, de 16 de janeiro de 2002, os comentários e sugestões enviados ficarão à disposição do público em geral na página do Banco Central do Brasil na internet.

Otávio Ribeiro Damaso
Diretor de Regulação

Anexo: 1.

BANCO CENTRAL DO BRASIL

RESOLUÇÃO Nº , DE DE DE 2017

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 e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro de 1964, torna público que o Conselho Monetário Nacional, em sessão realizada em de de 2017, com base nos arts. 4º, inciso VIII, da referida Lei, 9º da Lei nº 4.728, de 14 de julho de 1965, 7º e 23, alínea "a", da Lei nº 6.099, de 12 de setembro de 1974, 1º, inciso II, da Lei nº 10.194, de 14 de fevereiro de 2001, e 1º, § 1º, da Lei Complementar nº 130, de 17 de abril de 2009,

R E S O L V E U :

CAPÍTULO I
DO OBJETO E DO ÂMBITO DE APLICAÇÃO

Art. 1º Esta Resolução 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 e demais instituições 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 referidas no art. 1º 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 operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

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

§ 2º Admite-se a adoção de política de segurança cibernética única por:

I - conglomerado; e

II - sistema cooperativo de crédito.

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

I - descrever os objetivos de segurança cibernética da instituição;

II - prever os controles e as tecnologias adotados pela instituição para reduzir a sua vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética estipulados;

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

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

V - estabelecer diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

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;

c) a classificação dos dados e das informações quanto à relevância, sob a responsabilidade da instituição; e

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

VI - prever mecanismos para disseminação da cultura de segurança cibernética, incluindo a implementação de programas de capacitação de pessoal e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados ao tema; e

VII - prever as iniciativas para compartilhamento de informações com as demais instituições sobre os incidentes relevantes mencionados no inciso IV.

§ 1º Os objetivos de segurança cibernética referidos no inciso I devem contemplar a capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

§ 2º Os controles e as tecnologias de que trata o inciso II devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, o controle de atualizações de **hardware** e de **software**, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra **softwares** maliciosos e os controles de acesso e de segmentação da rede de computadores.

§ 3º Os controles citados no inciso II devem ser utilizados, inclusive, na adoção de novas tecnologias empregadas nas atividades da instituição.

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

§ 5º As diretrizes de que trata o inciso V, alínea "b", devem contemplar procedimentos e controles em níveis de complexidade, abrangência e acurácia semelhantes aos utilizados pela própria instituição.

§ 6º A política de segurança cibernética deve ser divulgada por meio de linguagem compatível com a complexidade das funções desempenhadas:

I - aos funcionários da instituição em seus diversos níveis;

II - às empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para condução das atividades operacionais da instituição; e

III - aos demais interessados, quando for o caso.

Seção II
Do Plano de Ação e de Resposta a Incidentes

Art. 4º As instituições referidas no art. 1º 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 definir, no mínimo:

I - as ações a serem desenvolvidas pela instituição para adequar sua estrutura 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, segundo cronograma especificado pela instituição, 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. 5º As instituições referidas no art. 1º devem designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes referido no art. 4º.

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

Art. 6º As instituições referidas no art. 1º devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, citado no art. 4º, com data-base de 31 de dezembro.

§ 1º O relatório referido no **caput** deve ser finalizado até 31 de março do ano seguinte ao da data-base.

§ 2º O relatório de que trata o **caput** deve abordar, no mínimo:

I - a efetividade da implementação do plano de ação e de resposta a incidentes;

II - os incidentes relacionados com o ambiente cibernético relevantes para a instituição ocorridos no período; e

III - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

§ 3º O relatório mencionado no **caput** deve ser submetido ao comitê de risco, quando existente.

Art. 7º A política de segurança cibernética, o respectivo plano de ação e de resposta a incidentes, mencionado no art. 4º, e o relatório de que trata o art. 6º devem ser aprovados pelo conselho de administração da instituição.

Parágrafo único. No caso de inexistência do conselho de administração, as responsabilidades mencionadas no **caput** devem ser atribuídas à diretoria ou aos administradores da instituição.

Art. 8º A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados, reavaliados, no mínimo, anualmente, revisados sempre que necessário e estar em harmonia com as exigências legais e regulamentares sobre o tema.

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

Art. 9º As instituições mencionadas no art. 1º, na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem:

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

II - exigir que o contratado assegure:

a) o acesso da instituição contratante aos dados e às informações processados ou armazenados pela empresa contratada;

b) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pela empresa contratada;

c) a auditoria dos serviços prestados e sua conformidade com a regulamentação; e

d) o acesso da instituição contratante aos instrumentos de monitoramento e de gestão dos controles providos pela empresa contratada na prestação dos serviços;

III - assegurar a capacidade de o contratado identificar e segregar dados dos clientes da instituição contratante usando controles físicos ou lógicos;

IV - assegurar a qualidade dos controles de acesso adotados pela empresa contratada, voltados à proteção dos dados e das informações dos clientes da instituição contratante; e

V - dispor de recursos e competências necessários para a adequada gestão dos serviços contratados, inclusive para auditoria de ambientes compartilhados.

§ 1º Para os fins do disposto nesta Resolução, os serviços de computação em nuvem abrangem a disponibilidade, à instituição 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, 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.

§ 2º 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 da alínea "c" do inciso V do art. 3º.

§ 3º No caso da execução de aplicativos por meio da internet, referidos no inciso III do § 1º, a instituição deve assegurar que o contratado adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

Art. 10. A instituição contratante dos serviços mencionados no art. 9º 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. 11. É vedada a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior.

Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever:

I - a indicação do local das instalações onde os serviços serão prestados e os dados serão armazenados, processados e gerenciados;

II - a adoção de medidas de segurança específicas 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 clientes;

IV - a possibilidade, em caso de substituição da empresa contratada, de:

a) transferência dos dados citados no inciso I ao novo prestador de serviços; e

b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a confirmação de recebimento dos dados pelo novo contratado;

V - o acesso da instituição contratante às instalações da empresa contratada e às informações para a realização de verificações no tocante aos incisos I a III;

VI - a necessidade de anuência da instituição contratante para subcontratação de serviços por parte da empresa contratada;

VII - a permissão de acesso do Banco Central do Brasil aos contratos e acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às respectivas informações sobre seus processamentos, bem como às instalações citadas no inciso I;

VIII - a manutenção, no País, das cópias de segurança dos dados e das informações armazenados pela empresa contratada, bem como das informações sobre os seus processamentos;

IX - a possibilidade de acesso, pelo Banco Central do Brasil, aos dados e às informações de que trata o inciso VIII; e

X - a possibilidade da adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil.

§ 1º O contrato mencionado no **caput** deve prever que a empresa contratada deve manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

§ 2º O contrato mencionado no **caput** deve prever, para o caso da decretação de regime de resolução da instituição 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 mencionadas no inciso VII, bem como às cópias dos dados e das informações citados no inciso VIII, inclusive às chaves de criptografia e aos sistemas necessários ao seu processamento; e

II - a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada de 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 do contratante.

CAPÍTULO IV
DISPOSIÇÕES GERAIS

Art. 13. As instituições referidas no art. 1º devem assegurar que suas políticas para gerenciamento de riscos previstas na regulamentação em vigor disponham, no tocante à continuidade de negócios, sobre:

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

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 no País; e

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

Art. 14. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios:

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

II - o prazo estimado 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 gerem decretação de situação de crise pela instituição financeira, bem como as providências para o reinício das suas atividades.

Art. 15. As instituições de que trata o art. 1º 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.

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

Art. 16. Sem prejuízo do dever de sigilo e da livre concorrência, as instituições mencionadas no art. 1º devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes de que trata o inciso IV do art. 3º.

§ 1º O compartilhamento de que trata o **caput** deve abranger informações recebidas de empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades da instituição.

§ 2º Deve ser assegurado o acesso do Banco Central do Brasil às informações compartilhadas.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 17. 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 - o documento relativo ao plano de ação e de resposta a incidentes, de que trata o art. 4º;

III - o relatório anual, de que trata o art. 6º;

IV - o contrato de que trata o art. 12, contado o prazo a partir da extinção do contrato; e

V - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 15.

Art. 18. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer:

I - a forma de compartilhamento e as informações que devem ser compartilhadas, tendo em vista o disposto no art. 16;

II - a exigência de certificações e outros requisitos técnicos a serem requeridos das empresas contratadas, pela instituição financeira contratante, na prestação dos serviços de que trata o art. 9º;

III - os prazos máximos, de que trata o art. 14, inciso II, para reinício ou normalização das atividades ou dos serviços relevantes interrompidos; e

IV - os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para o cumprimento desta Resolução.

Art. 19. As instituições que já contrataram a prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem no exterior devem apresentar ao Banco Central do Brasil, no prazo máximo de noventa dias, contados da data de entrada em vigor desta Resolução, cronograma para o retorno da execução desses serviços no País.

Parágrafo único. O prazo máximo para a execução plena, no País, dos serviços de que trata o **caput** é 31 de dezembro de 2021.

Art. 20. O Banco Central do Brasil poderá impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inadequação do serviço aos termos desta Resolução, estabelecendo prazo para a adequação dos referidos serviços.

Art. 21. Esta Resolução entra em vigor 180 (cento e oitenta) dias após a data de sua publicação.

Ilan Goldfajn
Presidente do Banco Central do Brasil