RESOLUÇÃO CMN Nº 4.892, DE 26 DE FEVEREIRO DE 2021

Altera a Resolução nº 3.631, de 30 de outubro de 2008, que dispõe sobre a realização de contrato de swap de moedas entre o Banco Central do Brasil e o Federal Reserve Bank of New York.

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 25 de fevereiro de 2021, com fundamento no art. 6º da Lei nº 11.908, de 3 de março de 2009, e no art. 4º, inciso V, da Lei nº 4.595, de 1964, resolve:

Art. 1º A Resolução nº 3.631, de 30 de outubro de 2008, passa a vigorar com a seguinte alteração:

"Art. 2º O valor em aberto das operações decorrentes do contrato referido no art. 1º não ultrapassará o montante agregado de US$60 bilhões, admitindo-se a realização de operações até 30 de setembro de 2021." (NR)

Art. 2º Fica revogada a Resolução CMN nº 4.850, de 27 de agosto de 2020.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

ROBERTO DE OLIVEIRA CAMPOS NETO
Presidente do Banco Central do Brasil

RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021

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 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 25 de fevereiro de 2021, 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, resolve:

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 autorizadas a funcionar pelo Banco Central do Brasil.

Parágrafo único. O disposto nesta Resolução não se aplica às instituições de pagamento, que devem observar a regulamentação emanada do Banco Central do Brasil, no exercício de suas atribuições legais.

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 prudencial; e

II - sistema cooperativo de crédito.

§ 3º As instituições 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;

II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição 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;

V - as 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; 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, incluindo:

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

b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; 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 as demais instituições referidas no art. 1º.

§ 1º Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade da instituição 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, no mínimo, 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.

§ 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.

Seção II

Da Divulgação da Política de Segurança Cibernética

Art. 4º A política de segurança cibernética deve ser divulgada aos funcionários da instituição 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 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 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 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 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.

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

Art. 8º As instituições referidas no art. 1º 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 de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

§ 2º O relatório mencionado no caput deve ser:

I - submetido ao comitê de risco, quando existente; e

II - 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.

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 referidas no art. 1º 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 mencionadas no art. 1º, 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 clientes 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 clientes 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 inciso III do art. 13, 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 de recursos providos nos termos da alínea "f" do inciso II do caput.

Art. 13. 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 contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

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

Art. 14. A instituição 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 comunicada pelas instituições referidas no art. 1º ao Banco Central do Brasil.

§ 1º A comunicação mencionada no caput deve conter as seguintes informações:

I - a denominação da empresa contratada;

II - os serviços relevantes contratados; e