21 de novembro de 2017

Sr. Otávio Ribeiro Damaso
Diretor
Departamento de Regulação do Sistema Financeiro
Via e-mail: denor@bcb.gov.br

Re.: Comentários Referentes ao Edital de Consulta Pública 57/2017, de 19 de Setembro de 2017

Prezado Diretor Otávio Ribeiro Damaso,

I – Introdução:

BSA | The Software Alliance[1] agradece pela oportunidade de oferecer comentários à Proposta de Resolução do Banco Central do Brasil sobre a política de segurança cibernética e requisitos para contratação de serviços de processamento, armazenamento de dados e de computação em nuvem – Consulta Pública Edital de Consulta Pública 57/2017 (doravante, a "Proposta de Resolução"). Sendo a principal defensora da indústria global de software, a BSA tem grande interesse em contribuir para iniciativas que buscam avançar a adoção da computação em nuvem mundialmente.

[1] A BSA | The Software Alliance (www.bsa.org) é a maior defensora da indústria global de software junto a governos no mercado internacional. Seu rol de membros conta com as empresas mais inovadoras do mundo, responsáveis pela criação de soluções de software que aquecem a economia e promovem a melhoria da vida moderna. Com sede em Washington, DC, e atuação em mais de 60 países, os programas de compliance pioneiros da BSA promovem o uso legal de softwares e defendem políticas públicas que promovem a inovação da tecnologia e geram crescimento na economia digital.

Os membros da BSA incluem: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Microsoft, Oracle, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro e Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Em nossa visão, um ambiente regulatório que permite que empresas, consumidores e governos aproveitem plenamente os benefícios de computação em nuvem é primordial para impulsionar a economia digital. Estes benefícios requerem políticas e regulamentos para computação em nuvem que permitam o livre movimento de dados através de fronteiras, evitem exigências de localização de dados, sejam baseados em padrões técnicos internacionais, protejam a privacidade e a propriedade intelectual e incluam mecanismos robustos para repressão e dissuasão de crimes cibernéticos.

A BSA e seus membros possuem vasta experiência no trabalho com governos e com outros stakeholders ao redor do mundo em políticas referentes à computação em nuvem. Compartilhamos os pontos de vista abaixo para auxiliar os esforços do Banco Central do Brasil para a criação de uma resolução que atenda seus objetivos regulatórios fundamentais e, ao mesmo tempo, permita que as instituições financeiras e outras instituições regulamentadas pelo Banco Central usem tecnologias em nuvem para o seu benefício e, consequentemente, para o benefício dos cidadãos brasileiros.

Parabenizamos o Banco Central por incluir referências na Proposta de Resolução que promoveriam uma abordagem baseada em risco à segurança cibernética. Estamos preocupados, porém, com a norma que proibiria o uso por instituições financeiras e outras instituições regulamentadas pelo Banco Central de serviços de computação em nuvem prestados por entidades que armazenam ou processam informações fora do Brasil. Pelos motivos expostos abaixo, tal proibição não melhoraria o acesso à informações pelo Banco Central, não melhoraria o desempenho de suas atribuições regulatórias, nem aumentaria a segurança cibernética.

Também sugerimos aperfeiçoamentos em algumas outras seções da Proposta de Resolução.

II – A Capacidade do Banco Central de desempenhar suas funções regulatórias não requer localização de Dados e Infraestrutura

Compreendemos que um dos objetivos da Proposta de Resolução é garantir que o Banco Central tenha acesso às informações necessárias para desempenhar suas funções regulatórias. Concordamos que este é um objetivo importante. A proposta de proibição do uso de serviços que armazenam ou de outra forma processam informações no exterior não iria, contudo, promover este objetivo.

As normas de localização de dados e infraestrutura previstas no Artigo 11, bem como algumas das exigências contratuais para a prestação de serviços em nuvem previstas no Artigo 12 são desnecessárias, excessivamente restritivas e dificultarão o uso por

instituições financeiras brasileiras de tecnologias de ponta. Especificamente, o Artigo 11 apenas permite que instituições financeiras contratem prestadores de serviços em nuvem se os dados da instituição financeira forem hospedados no Brasil. Certas seções do Artigo 12 estabelecem que o Banco Central terá direitos de auditar e acessar diretamente dados da instituição financeira. Nem o Artigo 11, ou as seções do Artigo 12 concedendo ao Banco Central direitos de auditoria e acesso físico direto às instalações das prestadoras de serviços em nuvem são necessários para garantir a autoridade regulatória do Banco Central do Brasil ou para promover a segurança.

O Artigo 9 da Proposta de Resolução já requer que (i) as entidades regulamentadas pelo Banco Central adotem "práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que sejam expostas"; e (ii) que as entidades regulamentadas garantam que seus contratos com provedores de computação em nuvem e armazenamento de dados prevejam que as entidades regulamentadas tenham acesso aos seus dados e capacidade de recuperá-los, bem como que a confidencialidade e integridade de tais dados sejam mantidas, independentemente de onde as informações sejam armazenadas ou de outra forma processadas. Além disso, o Artigo 9 também prevê que as instituições financeiras devem garantir que tenham a capacidade de auditar o provedor de serviços de armazenamento de dados ou de outros serviços em nuvem .

Se as diretrizes previstas no Artigo 9 forem seguidas, então o Banco Central do Brasil terá o mesmo grau de controle que teria se as próprias instituições financeiras estivessem hospedando os dados. O Banco Central tem jurisdição sobre a entidade regulamentada e pode, com estas obrigações contratuais estabelecidas, exigir que a entidade regulamentada forneça os dados (independentemente de onde estiverem armazenados). É irrelevante se os dados estejam armazenados no Brasil, fora do Brasil, por uma entidade regulamentada ou um terceiro. Portanto, a localização dos dados e da infraestrutura não impedirá o Banco Central de licitamente obter os dados de uma instituição regulamentada.

Por fim, o inciso VIII do Artigo 12 requer que cópias de backup de dados sejam armazenadas no Brasil. Pelos motivos mencionados acima, a localização do armazenamento das informações é irrelevante para fins de acesso ou segurança. Portanto, este dispositivo deve ser alterado de modo a permitir que cópias de backup de dados sejam armazenadas em qualquer localidade, sujeito às exigências contratuais discutidas acima.

Outros bancos centrais e reguladores financeiros que consideraram esta questão concluíram que exigências de localização de dados são desnecessárias --em parte porque proporcionam muito pouco em termos de benefícios adicionais, mas também porque inibem a concorrência e a escolha da tecnologia mais adequada para as necessidades de

instituições financeiras. Ao exigir que os dados sejam hospedados no Brasil, o Banco Central eliminará diversos provedores de armazenamento de dados e de serviços em nuvem daqueles disponíveis às entidades regulamentadas. Mesmo nos casos em que um provedor em particular tenha instalações de hospedagem no Brasil, é provável que alguma funcionalidade por ele oferecida exija que dados sejam armazenados fora do Brasil devido a forma de configuração das plataformas. É simplesmente impraticável para provedores terem todos os serviços e funcionalidade disponíveis em todos os países. Parte das economias e eficiências de custo que provedores de serviços em nuvem podem oferecer resultam de economias de escala, que podem exigir o armazenamento de dados fora do Brasil.

Recomendações:

- *A BSA recomenda fortemente ao Banco Central do Brasil que reconsidere a proibição de contratação de serviços de provedores que armazenam ou de outra forma processam informações fora do Brasil e remova o Artigo 11 da Proposta de Resolução.*
- *A BSA também recomenda a remoção dos itens mencionados acima do Artigo 12, pois são desnecessários e prejudiciais aos interesses brasileiros conforme explicado acima.*
    - *Estas alterações não afetarão a capacidade do Banco Central do Brasil de acessar dados.*

III – Exigências para localização de Dados e Infraestrutura enfraquecem a Segurança Cibernética

Um dos objetivos declarados da Proposta de Resolução é melhorar as práticas de segurança cibernética adotadas por instituições financeiras e outras instituições regulamentadas pelo Banco Central do Brasil.

A segurança de dados efetivamente não depende da localização física dos dados ou da localização de sua infraestrutura de suporte. Pelo contrário, a segurança é uma função da qualidade e eficácia dos mecanismos e controles mantidos para proteger os dados em questão. As empresas levam em conta muitos fatores para decidir onde sua infraestrutura digital (como por exemplo servidores e gateways) será localizada, incluindo a maximização da velocidade e do acesso à Internet, a implementação de recursos de redundância e backup e garantindo a utilização da melhor tecnologia de segurança para os dados do usuário.

As exigências de localização de dados do Artigo 11 e do Artigo 12 impediriam que as entidades regulamentadas pelo Banco Central aumentassem sua segurança ao realizar o back-up de dados em múltiplas localizações em diferentes regiões. Portanto, a exigência de localização de servidores coloca os dados em risco.

Além disso, muitos provedores de serviços em nuvem que oferecem excelente segurança não tem servidores no Brasil. A exigência de localização de dados excluiria tais provedores e impediria o uso de soluções com forte segurança por instituições financeiras brasileiras.

Recomendação:

- *A BSA recomenda fortemente que a exigência de localização de dados prevista na Proposta de Resolução seja eliminada. Portanto, o Artigo 11 e o Artigo 19 devem ser eliminados.*

IV – Uso de Software Licenciado e Práticas de Gestão de Ativos de Software

O Banco Central do Brasil deveria recomendar às instituições por ele reguladas o uso de software licenciado e práticas de gestão de ativos de software baseadas em padrões internacionais para aumentar a segurança cibernética.

O uso de software não licenciado expõe empresas a maiores riscos de infecções por malware e outras vulnerabilidades de segurança. De fato, um estudo da IDC[2] identificou uma forte correlação (0.79) entre a presença de software não licenciado e a incidência de encontros com malware. Como é menos provável que software não licenciado receba atualizações críticas de segurança que atenuariam os riscos associados à exposição a malware, o seu uso aumenta o risco de incidentes prejudiciais a segurança cibernética.

Infelizmente, o uso de software que não seja devidamente licenciado ainda é um problema significante. De acordo com os dados mais recentes, a taxa de uso de software não licenciado no Brasil é de 47 por cento[3]. Em muitos casos, o uso de software não licenciado é simplesmente uma questão de falta de conscientização de organizações sobre os ativos de software residentes em seus sistemas. A maioria das organizações não possuem políticas adequadas de gestão de licenças de software.

Práticas de gestão de ativos de software (SAM) transparentes e verificáveis identificam situações em que entidades estão usando software não licenciado, bem como situações

---

[2] IDC White Paper, *Unlicensed Software and Cybersecurity Threats (2015)*, disponível, em inglês, em http://globalstudy.bsa.org/2013/cyberthreat.html

[3] Os dados sobre as taxas de uso de software não licenciado e os valores comerciais foram obtidos da pesquisa 2016 BSA Global Software em http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . Este estudo avaliou as taxas de uso de software não licenciado e os valores comerciais de software não licenciado instalado em computadores pessoais durante 2015 em mais de 100 mercados. O estudo inclui uma discussão detalhada da metodologia utilizada.

em que as licenças que possuem excedem o número de usuários. O licenciamento insuficiente cria responsabilidade jurídica e riscos de segurança, enquanto o licenciamento excessivo cria ineficiências e custos desnecessários.

Todas as instituições regulamentadas pelo Banco Central do Brasil deveriam adotar práticas de gestão de ativos de software baseadas em padrões internacionais, que podem aumentar a eficiência e simultaneamente melhorar a segurança cibernética.

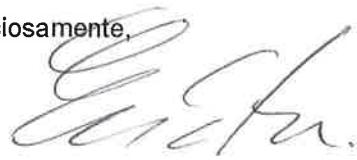
Recomendação:

- *O Banco Central do Brasil deve considerar exigir o uso de melhores práticas de gestão de ativos de software baseadas em padrões internacionais como parte de sua proposta de resolução.*

****

A BSA agradece a oportunidade de participar neste processo de consulta pública. Esperamos continuar este diálogo importante e permanecemos prontos para responder quaisquer perguntas.

Atenciosamente,



Antonio Eduardo Mendes da Silva
Country Manager - Brasil