/ Edital de Consulta Pública 57/2017

política de segurança cibernética para as instituições financeiras

white-paper

BAPTISTA LUZ
ADVOGADOS

À

Diretoria Colegiada do Banco Central do Brasil

Endereço eletrônico: denor@bcb.gov.br

Ref.: Edital de Consulta Pública 57/2017, de 19 de setembro de 2017

Prezados Senhores,

Conforme Edital de Consulta Pública 57/2017, de 19 de setembro de 2017 ("Audiência Pública" e "Edital"), aproveitamos a oportunidade para anexar nossos comentários e sugestões à minuta de Instrução proposta ("Minuta"), que trata da política de segurança cibernética para as instituições financeiras nacionais.

Nossos comentários e sugestões são apresentados de forma segmentada para cada dispositivo da Minuta que vislumbramos merecer alterações, iniciando com um quadro comparativo entre o texto original da Minuta (à esquerda) e o novo texto proposto por nós (à direita), seguidos das justificativas para os ajustes ou inclusões propostas.

Cumprimentamos essa D. Comissão pela iniciativa de tornar pública e colaborativa o desenvolvimento do referido documento.

Permanecemos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Baptista Luz Advogados

Anexo – Comentários e sugestões à Minuta da Resolução

1.	Art. 2 - alteração Inclusão de princípios
Texto da Minuta	**Texto Proposto**
Art. 2 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.	Art. 2. As instituições referidas no art. 1º devem implementar e manter política de segurança cibernética formulada com base em princípios, tais como os da prevenção, transparência e preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas, bem como diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.
Justificativa: Os princípios e diretrizes gerais mais importantes para nortear as Políticas de Segurança deveriam estar expressos aqui, assim como, a título exemplificativo, foi estabelecido no art. 3 da Lei 12.965/2014 (Marco Civil da Internet), pois trata-se de mandados de otimização que devem ser seguidos por todos, sem exceção. São uma forma de nortear as Políticas de Segurança e estabelecer o mínimo esperado delas. Ao se listar princípios básicos, permite-se uma co-regulação do Estado com os princípios próprios da instituição.	

2.	Art. 3, II - alteração Prevenção e reação à incidentes
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: 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;	Art. 3 A política de segurança cibernética deve, no mínimo: II - prever os controles, preventivos e reativos, bem como as tecnologias adotadas pela instituição para reduzir a sua vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética estipulados;
Justificativa: Apesar do Plano de Ação e de Resposta a Incidentes consistir em um documento diverso da Política de Segurança cibernética, acreditamos que a especificação na Política de Segurança de todos os tipos de controle operacionalizados pelas empresas previstas no Art. 1º da Minuta a torna mais clara e menos fragmentados os documentos. Desta feita, a Política de Segurança deve prever não só os controles preventivos, mas, também, de forma menos detalhada que o Plano de Ação, os controles reativos, ou seja, o que deve ser feito quando de um incidente de segurança da informação.	

3.	Art. 3, IV - alteração Análise de efeitos para os titulares dos dados
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: 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;	Art. 3 A política de segurança cibernética deve, no mínimo: 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 e para os titulares dos dados;
Justificativa: Tendo em vista que a regulação possui como objetivo principal "assegurar a confidencialidade, a integridade e a disponibilidade **dos dados** e dos sistemas de informação utilizados", como previsto no Art. 2, é importante ressaltar a necessidade de controle dos efeitos quando estes impactam, também, os titulares dos dados, e não somente a instituição financeira. Neste caso, por se tratar de dados pessoais, os danos podem ir muito além de problemas com reputação, podendo englobar até questões de uso indevido de dados para furto de identidade e prática de fraudes à pessoa natural.	

4.	Art. 3, V, b e c- alteração Melhor na redação e atualização seguindo a lesgilação
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: V - estabelecer diretrizes para: 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 responsabilidade da instituição; e	Art. 3 A política de segurança cibernética deve, no mínimo: V - estabelecer diretrizes para: b) procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem **adotados** pelas instituições financeiras e 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, observadas as classificações definidas na legislação aplicável no tocante à dados pessoais, quanto à relevância, sob responsabilidade da instituição; e
Justificativa: A palavra "definição" foi retirada do item "b" para conferir maior fluidez ao texto. As diretrizes são estabelecidas para os procedimentos, não para a definição destes. No item "c" incluímos a necessidade de observar as classificações que irão surgir com as legislações sobre dados pessoais, tais como a diferença entre dados pessoais simples e dados pessoais sensíveis. Estes recebem definição distinta da normalmente empregada pela melhor doutrina de Segurança da Informação e por esta própria Minuta, que classifica dados sensíveis não por sua eventual natureza discriminatória, mas sim com relação ao grau de importância do dado para a instituição. São classificações e conceitos distintos impostos pela legislação que devem ser levadas em consideração. A adição desse texto cria o dever de observar essas normativas e atualizar as Políticas de Segurança conforme surgirem.	

5.	Art. 3 - alteração Dever de sigilo e livre concorrência
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: VII - prever as iniciativas para compartilhamento de informações com as demais instituições sobre os incidentes relevantes mencionados no inciso IV.	Art. 3 A política de segurança cibernética deve, no mínimo: VII - prever as iniciativas para compartilhamento de informações com as demais instituições sobre os incidentes relevantes mencionados no inciso IV, respeitando o dever de sigilo e a livre concorrência.
Justificativa: É importante reforçar a ideia prevista no Art. 16 da Minuta. O compartilhamento de informações sobre incidentes de segurança da informação é prática comum no meio de segurança e são muito importantes para o desenvolvimento desse ambiente, no entanto as informações compartilhadas devem ser tratadas com cuidado para não infringir outros direitos e deveres, tais como o dever de sigilo. Ademais, o compartilhamento não deve desnecessariamente impactar a reputação da empresa perante o mercado, sob o risco de causar consequências adversas do objetivo principal de tal prática.	

6.	Art. 3, §1º - alteração Remediar impactos de incidentes
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: § 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.	Art. 3 A política de segurança cibernética deve, no mínimo: § 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 e remediar os seus impactos perante os afetados pelo incidente.
Justificativa: A inclusão do dever de remediar está atrelada ao princípio da transparência que é de grande importância para o setor de tratamento de dados. A ampla divulgação de um incidente envolvendo o tratamento de dados permite que os titulares dos dados afetados possam tomar providências para remediar os possíveis danos que poderão ser causados devido ao incidente. Nos Estados Unidos a Securities and Exchange Comission (SEC), em seu "Statement on Cybersecurity" aponta para a necessidade de notificação no caso de incidentes: "In addition to requiring SCI entities to maintain policies and procedures reasonably designed to ensure operational resiliency, the regulation requires SCI entities to take corrective action with respect to systems disruptions, compliance issues and intrusions (e.g., cybersecurity breaches). SCI entities are also required to provide notification, including to the Commission, of such events".	

7.	Art. 3 - modificação Simplificação da Minuta
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: (...) V - estabelecer diretrizes para: (...) 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; (...) § 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.	Art. 3 A política de segurança cibernética deve, no mínimo: (...) V - estabelecer diretrizes para: (...) b) procedimentos e controles voltados à prevenção e ao tratamento, que devem contemplar os mesmo níveis de complexidade, abrangência e precisão a serem **adotados** pelas instituições financeiras e 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;
Justificativa: A aglutinação do §5º ao inciso V, alínea b, busca reduzir a necessidade de autorreferência na norma, tornado a sua leitura mais contínua e simplificada. Ademais, sugere-se a substituição da palavra "acurácia" para precisão, por ter o mesmo sentido e ser um termo mais conhecido dentre os possíveis leitores e interpretadores da resolução.	

8.	Art. 3, §6º, III - alteração Notificação para titulares dos dados
Texto da Minuta	**Texto Proposto**
Art. 3 A política de segurança cibernética deve, no mínimo: § 6º A política de segurança cibernética deve ser divulgada por meio de linguagem compatível com a complexidade das funções desempenhadas: III - aos demais interessados, quando for o caso.	Art. 3 A política de segurança cibernética deve, no mínimo: § 6º A política de segurança cibernética deve ser divulgada por meio de linguagem clara, acessível e compatível com a complexidade das funções desempenhadas: III - aos demais interessados, quando for o caso, incluindo os titulares dos dados, por meio de um resumo em linguagem acessível em caso de incidente relevante.
Justificativa: A complexidade das funções desempenhadas não pode ser óbice para a utilização de linguagem clara e acessível. A ideia é que a Política de Segurança apresentada seja mais transparente e objetiva, facilitando o trabalho de fiscalização exercido pelo Banco Central. Ademais, uma vez que a Política de Segurança descreva como dados pessoais serão tratados no caso de incidentes de segurança da informação, é um direito do titular dos dados ter conhecimento sobre como seus dados são processados, se assim desejar.	

9.	Art. 4 - alteração Abrangência do plano de ação e resposta a incidentes
Texto da Minuta	**Texto Proposto**
Art. 4 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: 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	Art. 4 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: II - as empresas prestadoras de serviço e os terceiros a elas relacionados, 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
Justificativa: Os atores citados no art. 1 devem estabelecer Plano de Ação e resposta a incidentes que englobem, também, as empresas prestadoras de serviço e terceiros contratadas por ela ou terceiros com quem possua parceria. Busca-se, dessa maneira, reduzir os impactos que podem ser gerados por incidentes em toda a relação de tratamento e ciclo de vida dos dados, não se limitando a apenas uma das partes envolvidas.	

<table>
<tr><th>10.</th><th colspan="2">Art. 4 – inclusão de incisos
Notificação aos titulares dos dados e ao Banco Central</th></tr>
<tr><th colspan="2">Texto da Minuta</th><th>Texto Proposto</th></tr>
<tr><td colspan="2">Art. 4 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:</td><td>Art. 4 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:

IV – procedimento de notificação aos titulares dos dados afetados pelos incidentes.

V – procedimento de notificação ao Banco Central sobre incidente relevante que possa afetar demais participantes do mercado.</td></tr>
<tr><td colspan="3">Justificativa: A inclusão do procedimento de notificação dos titulares busca colocar em prática o princípio da transparência que é de grande importância para o setor de tratamento de dados e para todo o ecossistema do mercado financeiro e de segurança da informação. A ampla divulgação de um incidente envolvendo o tratamento de dados permite que os titulares dos dados afetados possam tomar providências para remediar os possíveis danos que poderão ser causados devido ao incidente, nos mesmos termos da sugestão 6. Tal prática, conhecida no como “data breach notification” também funciona como um fator de dissuasão (deterrant) que obriga as empresas a efetivamente implementarem políticas robustas de segurança cibernéticas, pois ao terem que publicizar incidentes sabem que isso poderá ter um grande impacto em sua reputação.

No entanto, no Art. 4 temos um termo que causa bastante insegurança jurídica: “incidentes relevantes”. O que poderia ser considerado um incidente relevante para o cumprimento da obrigação no inciso III da Minuta e dos incisos sugeridos aqui não fica claro. Necessário conceituar adequadamente o referido termo, que é utilizado nesse artigo e em outros momentos no texto da Minuta.</td></tr>
</table>

11.	Art. 5 - alteração Responsável pela Política de Segurança cibernética
Texto da Minuta	**Texto Proposto**
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. 5º As instituições referidas no art. 1º devem designar 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 responsável mencionado no caput pode desempenhar outras funções na instituição, desde que não haja conflito de interesses.
Justificativa: A necessidade de incumbir um diretor responsável por assegurar o efetivo funcionamento da Política de Segurança cibernética e pela execução do plano de ação e de respostas a incidentes parece não ser a escolha mais adequada, uma vez que as instituições citadas no art. 1 podem não possuir em seu corpo de colaboradores alguém com reais conhecimentos de cibersegurança necessários para desempenhar tal função. Além disso, a possibilidade de designar um responsável, e não um diretor, oferece maiores opções às instituições, que poderiam, inclusive, contratar responsável especializado no assunto, conferindo melhores resultados, ou até mesmo terceirizar tal função para empresa especializada ou um departamento como um todo.	

12.	Art. 6, III - alteração Prazo de retomada das atividades
Texto da Minuta	**Texto Proposto**
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. III - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.	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. III - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes, acompanhados do prazo estimado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos.
Justificativa: A apresentação de prazo estimado para normalização das atividades é importante, pois confere maior previsibilidade e segurança para o Banco Central, as empresas e instituições envolvidas e para os titulares dos dados afetados pelo incidente.	

13.	Art. 7 - alteração Disponibilização anual da Política de Segurança cibernética
Texto da Minuta	**Texto Proposto**
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.	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 e disponibilizados para o Banco Central em até 30 (trinta dias) da data base mencionada no art. 6º.
Justificativa: A necessidade de envio anual para o Banco Central, e não só a disponibilização, dos documentos citados confere maior *enforceability* para o cumprimento da instrução pelas instituições citadas no art. 1º da Minuta.	

14.	Art. 9, IV - alteração Nível de classificação de dados na Política de Segurança cibernética
Texto da Minuta	**Texto Proposto**
Art. 9º As instituições mencionadas no art. 1º, na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem: 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	Art. 9º As instituições mencionadas no art. 1º, na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem: 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 de acordo com o nível de classificação dos dados definidos pela instituição em sua política de segurança cibernética; e
Justificativa: É importante ressaltar a necessidade da coesão entre a proteção de dados e a classificação adotada na Política de Segurança das instituições. Assim, os padrões que devem ser observados para assegurar a qualidade dos controles de acesso podem repercutir por todas as áreas e ciclos de vida dos dados.	

15.	Art. 9, §1º - alteração Retificação da expressão "maneira virtual"
Texto da Minuta	**Texto Proposto**
Art. 9º As instituições mencionadas no art. 1º, na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem: § 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:	Art. 9º As instituições mencionadas no art. 1º, na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem: § 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 remota, de ao menos um dos seguintes serviços:
Justificativa: A utilização do termo "maneira virtual" é demasiada abrangente e pode causar insegurança jurídica, além de não ser um conceito definido dentro do contexto da sociedade da informação. Quando se trata de serviços em nuvem, seu destaque se dá pela possibilidade remota da sua prestação. Assim, a utilização da expressão "maneira remota" é mais precisa para identificar a prestação desse serviço como sendo de computação em nuvem.	

16.	Art. 10 - inclusão Dever de informar empresas contratadas sobre a presente resolução
Texto da Minuta	**Texto Proposto**
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. 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. Parágrafo único: é dever da instituição informar as empresas contratadas e terceirizadas, de forma expressa e simples, nos contratos, indicando que estas também estão subordinadas a presente Resolução.
Justificativa: O dever das instituições de informar, nos contratos, as empresas contratadas e terceirizadas sobre o dever de cumprir com as regras de segurança previstas na Minuta busca criar um ambiente adequado de cibersegurança entre todos os agentes desse setor e do ciclo de vida dos dados, não se limitando as instituições do art. 1, o que por consequência beneficiará todo o sistema financeiro por incentivar a adoção de medidas de segurança.	

<table>
<tr><th>17.</th><th colspan="2">Art. 11 - exclusão
Vedação da contratação de serviços em nuvem no exterior</th></tr>
<tr><th colspan="2">Texto da Minuta</th><th>Texto Proposto</th></tr>
<tr><td colspan="2">Art. 11. É vedada a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior.</td><td>Como primeira opção, propomos a exclusão do art. 11.

Caso não seja este o entendimento do Banco Central, propomos a seguinte alteração:

Art. 11. É vedada a contratação de serviços relevantes de computação em nuvem prestados no exterior sem garantias que os dados não serão acessados por terceiros não autorizados no território onde o serviço é prestado.</td></tr>
<tr><td colspan="3">Justificativa: Conhecida como cláusula de "data localization", esta visa determinar que serviços relevantes de computação em nuvem contratados pelas instituições listadas no art. 1º devem estar localizados em território nacional. Todavia, a exclusão do art. 11 da Minuta se pauta em diversos argumentos. Primeiro, o Brasil ainda possuí muitos problemas e gargalos na sua infraestrutura de rede, de forma que é necessário utilizar estruturas e pontos de troca de tráfego de backbone estrangeiros para a circulação de dados no país. Além disso, o mercado brasileiro de serviços em nuvem ainda não é desenvolvido o suficiente para atender todo o mercado financeiro, e muitas vezes é demasiadamente mais custoso do que os equivalentes localizados em outros países. Caso, o presente artigo seja aprovado, os dados só poderiam circular e serem armazenados dentro infraestrutura de rede, processamento e armazenamento brasileira, encarecendo a prestação do serviço e criando limitações para o ingresso de novas empresas no mercado, efetivamente criando uma barreira num mercado que vem fortemente se diversificando por meio de atores com pouco capital, mas ideias inovadoras com potencial de influenciar todo o ecossistema financeiro. Na prática, somente as grandes instituições financeiras teriam efetiva capacidade operacional e econômica para cumprir tal obrigação.

A título de argumentação, vale lembrar que o PL 2.621/2011, que depois se tornou a Lei 12.965/2014, comumente conhecida como Marco Civil da Internet, previa, na redação originária do artigo 12, que o Poder Executivo, por meio de decreto, poderia obrigar os provedores de aplicação a instalarem ou utilizarem bancos de dados em território nacional. A razão dessa proposição era assegurar a soberania e jurisdição brasileira sobre os dados aqui coletados. No entanto, essa proposta foi retirada pela sua inadequação ao</td></tr>
</table>

mercado e a própria arquitetura da Internet, que deve ser aberta, neutra, e não fragmentada. Dessa maneira, o presente artigo acaba por incidir no mesmo equívoco descrito.

Como já descrito anteriormente no ponto 10, outro problema identificado neste e em diversos trechos na Minuta é a utilização do termo *serviços relevantes* presentes nos artigos 11, 14 -I, II e III, 18 – III e 19. A imprecisão do termo pode ocasionar em insegurança jurídica por parte dos operadores, de forma que seria adequado definir na Minuta o que pode ser considerado serviço relevante no contexto do mercado financeiro.

18.	Art. 12 - Exclusão Necessidade de indicação do local dos serviços em nuvem prestados
Texto da Minuta	**Texto Proposto**
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;	**Propomos a exclusão do inciso I do art. 12.**
Justificativa: Serviços em nuvem raramente concentram os dados em um único servidor, em único local. Na verdade, a estrutura natural de balanceamento da rede determina quase que uma ubiquidade de locais onde os dados são armazenados. Desta forma, os dados não ficam todos concentrados no mesmo local. A identificação dos lugares onde os dados serão armazenados, processados e gerenciados não é adequada, pois prejudica a escalabilidade da prestação de serviços em nuvem, que deverá concentrar o tráfego em uma única rede, algo bastante improdutivo quando tratamos de comunicação pela rede. Além da concentração dos dados não ser uma prática do mercado, ela inviabiliza a utilização de tecnologias mais modernas como *blockchain,* que funciona por meio da descentralização do poder computacional e dos locais de armazenamento das informações. Destaca-se que o blockchain é, hoje, uma das tecnologias mais promissoras para o mercado financeiro. Cláusulas de "data localization" efetivamente inviabilizariam a adoção de tais tecnologias. A indicação do local onde os dados estarão armazenados também não parece adequada, pois compromete a sua segurança, tendo em vista que sua localização é facilitada.	

19.	Art. 12, IV, a e b - alteração Objetividade na leitura, interoperabilidade e exclusão de metados

Texto da Minuta	Texto Proposto
Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: 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;	Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: IV - a possibilidade, em caso de substituição da empresa contratada, de: a) transferência dos dados ao novo prestador de serviços de acordo com os padrões do mercado de interoperabilidade; e b) exclusão dos dados e dos metadados pela empresa contratada substituída, após a confirmação de recebimento dos dados pelo novo contratado;

Justificativa: A supressão da referência ao inciso I procura tornar a leitura mais objetiva, tendo em vista que a referência a quais dados a norma se refere é clara.

É importante também estabelecer a necessidade de observância dos padrões de interoperabilidade para facilitar o processo de transição de prestação de serviços em nuvem pelas empresas.

Além disso, é necessário obrigar não só a exclusão dos dados, mas também dos seus metadados. Tal prática confere maior segurança a esse procedimento, tendo em vista que esses podem ser aproveitados de diversas formas sem o consentimento da empresa contratante, até mesmo para fins comerciais, por exemplo, no mercado de "*Market data*".

20.	Art. 12, VIII - exclusão Cópias de segurança
Texto da Minuta	**Texto Proposto**
Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: 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;	**Como primeira opção, propomos a exclusão do inciso VII do art. 12.** **Caso o artigo seja mantido, propomos a seguinte redação:** Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: 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 que devem ser disponibilizados ao Banco Central;
Justificativa: Devem aqui ser levados em consideração os mesmos argumentos apresentados para a exclusão do art. 11 (ver referência acima). O dever de disponibilização desses contratos ao Banco Central confere maior *enforcement* à aplicação da norma.	

21.	Art. 12, X - alteração Medidas adicionais e prazos para a sua adoção
Texto da Minuta	**Texto Proposto**
Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: X - a possibilidade da adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil.	Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: X - a possibilidade da adoção de medidas adicionais pela instituição contratante, em decorrência de determinação do Banco Central do Brasil, que deve conferir prazo razoável pra implementação de tal medida.
Justificativa: A utilização do termo medidas adicionais reforça a necessidade de constante atenção e atualização de procedimentos de cibersegurança. Além disso, é muito importante que o Banco Central estabeleça prazos razoáveis para que as instituições adotem essas medidas adicionais, tendo em vista que suas implementações possam ser trabalhosas e demoradas.	

22.	Art. 12, §2º, I - alteração Padronização de acordo com as práticas e normas de dados pessoais
Texto da Minuta	**Texto Proposto**
Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: § 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	Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: § 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, respeitados os direitos de proteção de dados pessoais em legislação vigente; e
Justificativa: É muito importante que todos esses procedimentos descritos no inciso I estejam de acordo com as normativas e boas práticas acerca de dados pessoais, seguindo as devidas atualizações.	

23.	Art. 12, § 2º, II - alteração Aprimoramento de redação
Texto da Minuta	**Texto Proposto**
Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: § 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: 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:	Art. 12. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem prever: § 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: II – a obrigação do responsável pelo regime de resolução de notificar previamente a empresa contratada sobre a intenção de interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:
Justificativa: A estrutura gramatical do texto da Minuta pode ser simplificada, tornando-a mais clara.	

24.	Art. 14, III - alteração Prazo para notificação ao Banco Central
Texto da Minuta	**Texto Proposto**
Art. 14. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios: 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. 14. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios: III - a comunicação ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, no prazo de 24 horas contadas a partir da ciência da instituição sobre o incidente, que gerem decretação de situação de crise pela instituição financeira, bem como as providências para o reinício das suas atividades.
Justificativa: O estabelecimento de um prazo de 24 horas concreto oferece maior segurança jurídica aos atuantes no setor financeiro e aos titulares dos dados sujeitos do incidente de segurança da informação. O termo tempestivo não parece adequado diante da necessidade de notificação pela sua vagueza. Além disso, reforçamos a necessidade de conceituar os termos "incidente relevantes" e "serviço relevante" para conferir maior segurança jurídica ao texto da Minuta.	

25.	Art. 17, V - alteração Contagem de prazo
Texto da Minuta	**Texto Proposto**
Art. 17. Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos: V - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 15.	Art. 17. Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos: V - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 15, contados a partir de sua implementação.
Justificativa: Nos demais incisos do presente artigo, fica claro a partir de qual data deve-se contar o prazo de 5 anos. Contudo, esse início de contagem não fica evidente na redação do inciso V, ensejando que o início do prazo se dê com a implementação dos mecanismos de acompanhamento.	

26.	Art. 18 - alteração Definição das certificações e estabelecimento de prazos
Texto da Minuta	**Texto Proposto**
Art. 18. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer: 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;	Art. 18. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer: II - a exigência de certificações e outros requisitos técnicos, de acordo com padrões internacionais e de mercado, a serem requeridos das empresas contratadas, pela instituição financeira contratante, na prestação dos serviços de que trata o art. 9º, dentro de prazos razoáveis;
Justificativa: É importante definir quais seriam essas certificações para tornar a redação do inciso mais precisa. Além disso, as instituições contratantes precisam estabelecer prazos razoáveis, observando o tempo de demora para a realização das mudanças necessárias e da própria emissão de um determinado certificado.	

27.	Art. 18, IV - alteração Adoção de novas medidas solicitadas pelo Banco Central
Texto da Minuta	**Texto Proposto**
Art. 18. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer: IV - os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para o cumprimento desta Resolução.	Art. 18. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer: IV - os requisitos técnicos e procedimentos operacionais, compatíveis com os padrões nacionais e internacionais de mercado, a serem observados pelas instituições para o cumprimento desta Resolução.
Justificativa: É importante ressaltar que essas medidas sejam compatíveis com as melhores práticas encontradas no mercado. Dessa maneira, impede-se a implementação de novidades estranhas que podem trazer inseguranças ao setor.	