**BAPTISTA LUZ ADVOGADOS**
R. Ramos Batista . 444 . Vila Olímpia
04552-020 . São Paulo – SP
**baptistaluz.com.br**

# BACEN LANÇA CONSULTA PÚBLICA SOBRE SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES FINANCEIRAS

## / INTRODUÇÃO

No dia 19.09.2017, o Banco Central do Brasil (BACEN) anunciou a publicação do Edital de Consulta Pública 57/2017, que trata 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".

Trata-se de **minuta de resolução sobre segurança da informação que toca em questões centrais relativas ao armazenamento, compartilhamento, transferência e segurança de dados e informações inerentes ao efetivo funcionamento das instituições financeiras e de seus correntistas, e impõe obrigações ainda não previstas em normas anteriores, como às relativas à incidentes de segurança da informação.**

A proposta, cuja minuta está aberta a análise, virá para complementar algumas exigências que já incidem sobre essas instituições – como, por exemplo, relacionadas à digitalização e ao armazenamento de documentos eletrônicos. A ideia é listar requisitos essenciais de *segurança da informação no meio digital*, e com base nisso impor às instituições que **implementem e mantenham uma política mínima de segurança no trato com as informações com as quais lidam no seu cotidiano**.

## / PRINCIPAIS EXIGÊNCIAS PROPOSTAS

As exigências, de acordo com o texto da minuta inicial, levarão em conta **o modelo de negócio de cada instituição, o seu perfil de risco, a complexidade dos seus produtos e dos serviços que presta, e a sensibilidade dos dados com os quais lida** – ou seja, quão privilegiados eles são, quão impactante é na vida do usuário que eles sejam acessados

por invasores ou quaisquer pessoas não autorizadas. A política pode ser única, valendo tanto para instituições individuais quanto para conglomerados econômicos.

Segundo a proposta, a política implementada pelas instituições reguladas deve, no mínimo, prever:

- os controles e as tecnologias adotadas pela instituição para evitar incidentes de segurança da informação;
- os controles voltados para a rastreabilidade das informações, durante todo o seu ciclo de vida, principalmente as de natureza sensível;
- medidas para analisar a causa e o impacto de eventuais incidentes, além de planos para garantir a continuidade dos negócios.

Para implementar as medidas acimas, as instituições terão que, no mínimo, se valer de tecnologias para autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, controle de atualizações de *hardware* e de *software*, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos e controles de acesso e de segmentação da rede de computadores.

**Incidentes recentes como o do *ransomware* "WannaCry", que atingiu diversos setores nacionais e internacionais, paralisando sistemas inteiros por meio de vulnerabilidades que poderiam ter sido evitadas, deixam claro que tais tecnologias são, hoje, essenciais para o funcionamento contínuo de estruturas essenciais como as de instituições financeiras**.

## / RESPOSTA A INCIDENTES E GOVERNANÇA

Ainda, as instituições vão ter que estabelecer um **plano de ação e de resposta a incidentes** – que terá um diretor como responsável – e **emitir relatórios anuais sobre o plano adotado, compartilhando informações sobre sua implementação e desenvolvimento**. A política de segurança cibernética, o plano de ação e resposta a incidentes e o relatório de desenvolvimento e implementação de tais procedimentos deve ser aprovado pelo conselho de administração da instituição, ou pela diretoria ou administradores na ausência deste.

**Esse nível de autorização demonstra que o tema de segurança da informação não mais se restringe ao respectivo departamento, tornando-se um dos principais eixos de sustentação das instituições.**

Um ponto importante dessa proposta, e que ainda não é uma prática comum no mercado nacional, é a obrigatoriedade de que os dados e as informações com as quais esse tipo de instituição lida sejam classificados de acordo com a sua relevância e a sua natureza. Isso é chamado, no meio, de **mapeamento de dados** –, método que, ao identificar como os dados são coletados, armazenados, protegidos e compartilhados, visa, principalmente, permitir o estabelecimento de formas adequadas de tratamento e segurança proporcional ao tipo dos dados.

## / SERVIÇOS DE NUVEM

A minuta proposta determina que instituição que contratar serviços na nuvem de processamento de dados, armazenamento, infraestrutura e outros será responsável por exigir que a empresa contratada zele adequadamente pelo acesso, segurança, confidencialidade, e auditoria dos dados e informações que ela armazenar e manipular para atender à contratante.

Ainda, as instituições **estarão proibidas de deixar serviços relevantes de processamento e de armazenamento de dados nas mãos de empresas contratadas no exterior** – princípio conhecido com *data localization*. Essa medida provavelmente provocará não só impacto financeiro, como também operacional no cotidiano das instituições.

Hoje em dia é muito comum que estas se valham de serviços de *data storage* (armazenamento ou custódia de dados) e *data processing* (processamento de dados) oferecidos por estruturas montadas inteiramente em outros países, em virtude dos seus custos mais atraentes. Pela proposta, as instituições financeiras que hoje utilizam serviços no exterior deverão apresentar para o BACEN plano para nacionalização das suas operações.

Pela proposta, os contratos de prestação dos serviços classificados como nuvem devem:

- indicar o local das instalações físicas onde os serviços serão prestados e os dados armazenados, gerenciados;
- prever a possibilidade do BACEN ter acesso às informações referentes aos serviços prestados, as práticas de processamento de tais dados e às cópias de segurança dos dados, que também devem ser mantidas em território nacional

## / CONSULTA PÚBLICA

A consulta pública está no ar até 21 de novembro. O Baptista Luz montou grupo de estudos para estudar a minuta, pensar nos seus impactos futuros,

e responder à consulta pública, visando contribuir para torná-la mais robusta, aplicável e condizente com a realidade, viabilizando que ela traga mais segurança para todos os agentes atuantes no mercado financeiro.

**Contribuições, sugestões e apontamentos** – **mesmo na forma de questões para discussão** – **são muito bem-vindos** e podem ser encaminhados para pesquisa@baptistaluz.com.br, para que possamos acrescentá-las às elaborações do nosso time e respondê-las à nossa rede de contatos.

**Também é possível contribuir diretamente, entrando em contato com o BACEN** via e-mail (denor@BACEN.gov.br), via correspondência (dirigida ao Departamento de Regulação do Sistema Financeiro - Denor, SBS, Quadra 3, Bloco "B", 9º andar, Edifício-Sede, Brasília (DF), CEP 70074-900), ou por meio da URL divulgada no edital.

Estamos à disposição para quaisquer dúvidas, sugestões e solicitações sobre o tema.

Atenciosamente,

**BAPTISTA LUZ ADVOGADOS**

/ **Pedro H. Ramos**
pedro@baptistaluz.com.br

/ **Renato Leite Monteiro**
renato.leite@baptistaluz.com.br