CONTRIBUIÇÕES DA BRASSCOM AO EDITAL DE AUDIÊNCIA PÚBLICA SDM Nº 05/18

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, é uma entidade que congrega seleto grupo de empresas fornecedoras de software, soluções e serviços de Tecnologia da Informação e Comunicação (TIC) e que tem como missão trabalhar em prol do desenvolvimento do setor, disseminando seu alcance e potencializando seus efeitos sobre a economia e o bem-estar social.

Tendo em vista que a Comissão de Valores Mobiliários (CVM) publicou, no dia 8 de outubro de 2018, o Edital de Audiência Pública SDM n.º 05/2018, com propostas de alteração da Instrução CVM n.º 505/2011[1], que dispõe sobre normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários, e revogação da Instrução CVM n.º 380/2002[2], a Brasscom vem através da presente manifestação apresentar as sugestões e comentários das empresas do setor TIC com o objetivo de auxiliar a CVM na elaboração dessa nova Instrução.

A Brasscom recebe com otimismo a consulta pública apresentada pela CVM, certa de que o Regulador apreciará contribuições com o objetivo de esclarecer e ajustar determinados pontos da minuta de instrução ("Minuta") de forma a adequá-la, dentre outras questões, às melhores práticas de mercado nas áreas de segurança cibernética e de segurança da informação aplicadas às suas entidades reguladas, temas que ocupam espaço central na agenda de entidades tanto do setor público quanto do setor privado de diferentes indústrias e nacionalidades.

As alterações propostas pela CVM na Minuta relacionadas à segurança cibernética e à segurança da informação, e que também são o objeto específico de nossos comentários e sugestões nesta manifestação, estão associadas aos processos, sistemas e infraestrutura de tecnologia da informação.

I. Alterações propostas e respectivas justificativas

Adotamos uma contribuição bastante pontual, reunindo um conjunto de modificações de menor relevância ou de aperfeiçoamento do texto; sugestões de inclusão de redação para gerar maior precisão técnica naquilo que compete à segurança cibernética e à segurança da informação; e a sugestão de exclusão de dispositivos que em seu comando podem gerar interpretação dúbia, podendo gerar impactos tanto para CVM, quanto para seus regulados e usuários dos serviços regulados.

Na dicção dos dispositivos legais transcritos no texto, adota-se a seguinte notação:

- **Fragmento de texto ~~tachado~~** - propõe a eliminação do fragmento de texto da Minuta
- **Fragmento de texto <u>sublinhado</u>** - propõe que o fragmento de texto seja acrescentado à Minuta.
- **[...]** - refere-se à manutenção do fragmento de texto original da Minuta.

No intuito de melhor fundamentar as proposições manifestadas neste documento, a Brasscom se coloca à disposição para esclarecimentos adicionais e/ou mais detalhados.

II. Sugestões Específicas

A Brasscom considera relevante que a CVM inclua uma definição de computação em nuvem em sua política, conforme sugerido abaixo:

"*A computação em nuvem é a entrega sob demanda de serviços de processamento, armazenamento, aplicações e outros recursos que se enquadram na esfera da Tecnologia da Informação por meio de uma plataforma de serviços de nuvem virtual ofertada através da Internet, com uma definição de preço conforme o uso e paga a partir de diversos modelos*."

<u>CONSIDERAÇÕES SOBRE O CAPÍTULO V – PESSOAS VINCULADAS</u>

> Art. 32. (...)
> § 2º Os sistemas tecnológicos utilizados pelo intermediário devem <u>possuir certificação de auditoria emitida por entidades terceiras independentes</u> ~~ser passíveis de auditoria~~, devendo o intermediário submetê-los a testes periódicos para verificar o seu funcionamento em cenário de estresse." (NR)

Justificativa

Da análise do texto acima verifica-se que a CVM exige na redação originalmente proposta que os sistemas tecnológicos utilizados pelo intermediário possam ser auditados. No entanto, importa salientar que os prestadores de serviços de tecnologia dispõem de certificações de auditoria para os serviços por eles prestados emitidos por entidades terceiras independentes, que são disponibilizados aos seus clientes (no presente, os intermediários). Estas certificações de auditoria dizem respeito tanto à segurança física da infraestrutura global dos sistemas de tecnologia quanto à segurança dos dados dos clientes.

Da mesma forma, cabe frisar que os prestadores de serviços de tecnologia fornecem seus serviços para milhões de clientes. Assim, se cada regulador de valores mobiliários ao redor do mundo permitir que os milhões de clientes a quem os fornecedores de serviços de tecnologia fornecem seus serviços façam auditorias em seus sistemas e/ou instalações, a todo e qualquer tempo, esta conduta constituirá uma grave ameaça à segurança física da infraestrutura. Veja-se que, se esta

permissão for ampliada e aplicada em toda a sua extensão, por vários setores de mercado, poderá gerar como resultado dezenas de milhares de auditorias por ano. Isto significaria que, como resultado da abertura das instalações e infraestrutura dos prestadores de serviços de tecnologia para milhares de auditorias, estar-se-ia a pôr em risco e a prejudicar a segurança física das instalações, assim como, a criar potenciais ameaças à segurança e confidencialidade dos dados do cliente.

Atente-se para o fato de que, ao invés da CVM optar por este perigoso cenário, os objetivos de gerenciamento de risco são atendidos por um programa de auditoria independente, desde que o programa de auditoria do prestador de serviços de tecnologia atenda os padrões mínimos definidos pelos reguladores. Por exemplo, os reguladores podem exigir que o programa de auditoria independente:

(a) seja realizado por auditores profissionais independentes de renome;
(b) seja realizado considerando relevantes padrões internacionais objetivos aplicáveis à segurança da informação, tais como ISO 27001, ISO 27017, SOC 1 e 2, e PCI-DSS ou padrões futuros alternativos que substituam ou sejam substancialmente equivalentes a estes padrões;
(c) resulte na apresentação de relatórios de auditoria independentes que estão disponíveis para os intermediários, e podem ser fornecidos pelo intermediário ao Regulador; e
(d) envolva tais auditorias e relatórios com uma frequência mínima definida pelo Regulador.

A disponibilização de relatórios de auditoria permite que os intermediários e a CVM validem se os serviços e os controles de segurança de um prestador de serviços de tecnologia estão operando de acordo com os padrões internacionais, sem comprometer a segurança e a confidencialidade do prestador de serviços de tecnologia ou dos seus demais clientes, incluindo outros intermediários.

Nestes moldes, a Brasscom sugere que a CVM estabeleça na redação da Minuta a aceitação de certificado de auditoria de uma entidade terceira independente, de acordo com as melhores práticas internacionais. Existem diversas entidades terceiras independentes reconhecidas nacional e internacionalmente, as quais conduzem uma avaliação e disponibilizam um certificado de auditoria que atesta o cumprimento dos requisitos de segurança internacionais. Tal procedimento, no nosso entendimento, endereça assim, da forma mais rápida, eficaz e segura, as preocupações da CVM levantadas nesta audiência pública.

É neste contexto que encorajamos a CVM a esclarecer e alterar a redação utilizada no § 2º, para que se possa assegurar de forma clara que os intermediários poderão confiar em um certificado de auditoria emitido por uma entidade terceira independente, contínuo e com escopo delimitado.

Face ao exposto, a Brasscom gostaria de sugerir que a CVM estabeleça na Minuta a aceitação expressa de um certificado de auditoria de entidades terceiras independentes conforme a sugestão de redação apresentada para o § 2º do Art. 32, acima.

CONSIDERAÇÕES CAPÍTULO VIII-A – PLANO DE CONTINUIDADE DE NEGÓCIOS

Seção III – Segurança Cibernética

Art. 35-I. O intermediário deve comunicar, ~~no prazo~~ em prazo razoável ~~de até 24 (vinte e quatro) horas a partir da identificação da ocorrência,~~ à SMI, para fins de informação, a ocorrência de incidentes de segurança cibernética relevantes.

Justificativa

O Art. 35-I exige que o intermediário comunique, no prazo de até 24 horas a partir da identificação da ocorrência, à SMI o incidente de segurança cibernética. A experiência mostra que as empresas precisam de tempo para estabelecer os fatos e a natureza do incidente, quais os dados envolvidos, impactos, riscos e danos que podem advir de um eventual incidente.

É preciso tempo para realizar o diagnóstico e as perícias iniciais e não há nenhuma vantagem significativa em notificar e alardear a Superintendência de Relações com o Mercado e Intermediários antes mesmo de conhecer os fatos e avaliar os riscos e potenciais danos. Além disso, em algumas circunstâncias, como no curso de ações penais de iniciativa privada (em oposição aos processos de iniciativa pública) ou de outras investigações sob sigilo, é indispensável a não-revelação de detalhes publicamente.

Assim, é mais recomendável que a Minuta preveja que as comunicações sobre eventuais incidentes de segurança aconteçam após o estabelecimento dos fatos e da natureza do incidente, assim como do estabelecimento, ainda que inicial, do potencial impacto, riscos e danos para os titulares.

Seção IV – Contratação de Serviços Prestados por Terceiros

Art. 35-J. No caso de serviços prestados por terceiros, o intermediário deve identificar e relacionar seus prestadores de serviços críticos, avaliar os controles realizados por estes provedores e garantir em seu contrato de prestação de serviços, o cumprimento:
[...]
II – o acesso lógico da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviços; e
[...]

Justificativa

Sugerimos que seja incluído o termo "lógico" para que não restem dúvidas com relação à forma como este acesso se dará.

Aqui é importante tecermos algumas considerações com vistas a elucidar, ainda que de forma muito simplista, os tipos de controle de acesso e suas diferenças. Segundo o Tribunal de Contas da União ("TCU"), em seu documento *Boas Práticas em Segurança da Informação*[3], **os controles de acesso, físicos ou lógico, têm como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Os sistemas computacionais, bem diferentes de outros tipos de recursos, não podem ser facilmente controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardar de segurança[4]. Daqui surge a relevância dos controles de acesso lógico para os sistemas computacionais e para os serviços em nuvem**.

Ainda segundo o TCU, **os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas de computador**. Neste sentido, a proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário, enquanto a identificação e a autenticação do usuário (confirmação de que o usuário realmente é quem ele diz ser) são feitas normalmente por meio de um identificador de usuário (ID) e uma senha durante o processo de login no sistema.

> Art. 35-J. No caso de serviços prestados por terceiros, o intermediário deve identificar e relacionar seus prestadores de serviços críticos, avaliar os controles realizados por estes provedores e garantir em seu contrato de prestação de serviços, o cumprimento:
> [...]
> ~~§ 3º. O intermediário deve fazer constar dos contratos referentes à prestação de serviços terceirizados a permissão de acesso da CVM e da entidade autorreguladora:~~
> ~~I – ao conteúdo dos contratos;~~
> ~~II – a documentos, dados e informações processadas ou armazenadas pelos prestadores de~~ serviços~~; e~~
> ~~III – às dependências do contratado." (NR)~~

Justificativa

A Brasscom solicita a exclusão do § 3º do Art. 35-J em sua integralidade por que tais medidas não geram qualquer garantia específica de segurança, confidencialidade e integridade dos dados e informações armazenados e processados pelos prestadores de serviços de tecnologia.

Na hipótese da preocupação da CVM estar relacionada com a integridade dos dados e informações, essa preocupação está sanada pelo fato de que o prestador de serviços de armazenamento e processamento não tem acesso aos dados e informações, pois somente os seus clientes – no presente caso, os Intermediários regulados pela CVM – têm esse acesso. Os prestadores de serviço de armazenamento e processamento de dados fornecem aos seus clientes uma infraestrutura lógica. Nesse contexto, estes prestadores de serviços não têm visibilidade ou conhecimento sobre o que os clientes têm.

Conforme mencionado anteriormente, os provedores de serviços de nuvem geralmente seguem estruturas de segurança reconhecidas internacionalmente e padrões de certificação (por exemplo, o ISO 27001), que fornecem informações amplas sobre a estrutura de segurança operacional de um prestador de nuvem. Acreditamos que, para o fornecimento de serviços em nuvem e a garantia de segurança, resiliência e integridade de dados, não há necessidade de ter acesso a contratos adicionais, documentação e informações sobre a prestação do serviço.

Adicionalmente, veja-se que a previsão de acesso físico às instalações é contraditório com as preocupações de segurança abordadas no Item 2.2.2. - Segurança Cibernética do documento preliminar que apresenta as razões e as alterações propostas no texto da Minuta. Isto ocorre porque a forma que os prestadores de serviços de nuvem têm para gerenciarem a segurança de seus data centers é limitar o acesso aos detalhes de localização específicos dos datacenters que operam. Uma obrigação para divulgar a localização específica dos data centers prejudicaria as práticas de segurança e tornaria as instalações dos provedores de serviços em nuvem mais vulneráveis. Quando a supervisão regulatória obriga à divulgação do endereço do local físico do data center para requisitos de localização de dados, ela falha em atender aos principais objetivos de sua intenção. Assim, por motivos de segurança, é imperativo manter a confidencialidade dos endereços físicos das instalações dos provedores de serviços de nuvem. Em resumo, a exigência de acesso às premissas não auxilia no cumprimento do objetivo da CVM. Na verdade, o requisito é contrário aos objetivos de segurança.

É nestes moldes que a Brasscom reforça a sugestão dada de exclusão desta parte relativa ao acesso físico às instalações no item 2.2.3. e Artigo 35-J, §3, III do documento submetido a audiência pública pela CVM.

---

[1] Instrução CVM 505, de 27 de setembro de 2011.
[2] Instrução CVM 380, de 23 de dezembro de 2002.
[3] Disponível em https://goo.gl/Tnzj8R.
[4] Disponível em https://goo.gl/Tnzj8R, p. 16.