Item	Artigo
Introdução	Altera, acrescenta e revoga dispositivos à Instrução CVM nº 505, de 27 de setembro de 2011, e revoga a Instrução CVM nº 380, de 23 de dezembro de 2002.
Art 18	**Art. 18.** As operações decorrentes de ordens transmitidas por meio de sistemas eletrônicos de negociação de acesso direto ao mercado devem ser supervisionadas pela entidade autorreguladora. **Parágrafo único.** A entidade autorreguladora deve incluir as operações de que trata o caput no seu programa de trabalho.
Art 35-E	**Art. 35-E**. O intermediário deve desenvolver e implementar suas políticas e práticas visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações, contemplando: **I –** a classificação dos dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; **II –** as diretrizes para a avaliação da relevância dos incidentes; e **III –** os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos. **Parágrafo único.** O intermediário deve considerar, no mínimo, os dados que permitem a identificação dos seus clientes e a suas operações como informações sensíveis.

Art 35-I	**Art. 35-I.** O intermediário deve comunicar, no prazo 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. **§ 1º** Considera-se relevante o incidente de segurança cibernética que afete dados sensíveis ou sistemas críticos de forma a impactar significativamente os clientes. **§ 2º** No prazo de 45 (quarenta e cinco) dias o intermediário deve encaminhar relatório à SMI, contendo, no mínimo: **I** – descrição do incidente e das medidas tomadas, indicando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes; **II** – cópia das comunicações realizadas com seus clientes; **III** – cópia dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados; e IV – os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, com o estabelecimento de cronograma de implementação, se for o caso.

Proposta de alterações A
Alteração
Altera, acrescenta e revoga dispositivos à Instrução CVM nº 505, de 27 de setembro de 2011, e revoga a Instrução CVM nº 380, de 23 de dezembro de 2002. Estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e estipula diretrizes de proteção de dados e segurança cibernética no âmbito da intermediação de valores mobiliários.
Art. 18. As operações decorrentes de ordens transmitidas por meio de sistemas eletrônicos de negociação de acesso direto ao mercado devem ser supervisionadas pela respectiva entidade autorreguladora. **Parágrafo único.** A entidade autorreguladora deve incluir as operações de que trata o caput no seu programa de trabalho.
Art. 35-E. As políticas e práticas de segurança da informação sobre o tratamento e controle de dados de clientes devem ser desenvolvidos de forma a garantir a confidencialidade, autenticidade e integridade, seguindo os fundamentos básicos do respeito à privacidade e a inviolabilidade da intimidade, honra e imagem dos titulares dos dados. Para tanto, as políticas devem contemplar: **I** – a classificação dos dados ou informações sensíveis tal como estabelecido no inciso II, art. 5º da Lei nº 13.709/18; **II** – as diretrizes para a avaliação da relevância dos incidentes; e **III** – os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos. **Parágrafo único**. O intermediário deve considerar, no mínimo, os dados que permitem a identificação dos seus clientes e a suas operações como informações sensíveis.

Art. 35-I. O intermediário deve comunicar, no prazo 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.

§ 1º Considera-se relevante o incidente de segurança cibernética que afete dados sensíveis ou sistemas críticos de forma a impactar significativamente os clientes.

§ 2º No prazo de 30 (trinta) dias, prorrogáveis por mais 15 (quinze) a pedido do intermediário, o intermediário deve encaminhar relatório à SMI, contendo, no mínimo:

I – descrição do incidente e das medidas tomadas, indicando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes;

II – cópia das comunicações realizadas com seus clientes;

III – cópia dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados; e

IV – os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, com o estabelecimento de cronograma de implementação, se for o caso.

udiência Pública
Justificativa
Sugestão meramente formal a fim de apresentar claramente os objetivos da nova Instrução Normativa.
Sugestão meramente formal, apenas para deixar a sentença mais clara.
A Lei de Proteção de Dados Pessoais (Lei 13.709/18 - "LGPD") foi publicada em agosto de 2018 e prevê o vacatio legis de 18 meses. No entanto, a CVM já demonstrou a importância que dá ao tema incluindo na Minuta de alteração da Instrução CVM nº 505/2011 ("Minuta") novos artigos relacionados a segurança das informações. O art. 5-A da Minuta traz o cadastro dos clientes e requisitos mínimos de auditoria para garantir que o rastreamento das inclusões, alterações e exclusões de dados sejam suficientemente identificáveis. O art. 35-E traz, especificamente, as regras de tratamento e controle de dados tal qual é exigido pela LGPD. Entendemos que a LGPD é aplicável tendo em vista seu art. 3º: "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional." Sendo assim, os intermediários devem tomar as medidas legais estabelecidas da LGPD, que também traz algumas definições importantes: "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a

O prazo de 45 (quarenta e cinco) dias nos pareceu longo, considerando as 24 horas para comunicação prevista no caput. Assim, sugerimos que o prazo seja de 30 dias, prorrogáveis por mais 15 a pedido no intermediador.