



São Paulo, 14 de dezembro de 2018.

A

Comissão de Valores Mobiliários

Rua Sete de Setembro, 111/2, 34º andar, Centro
Rio de Janeiro/RJ CEP 20050-901 – Brasil

Ref.: EDITAL DE AUDIÊNCIA PÚBLICA SDM Nº 05/18

A **FEDERAÇÃO BRASILEIRA DE BANCOS** agradece a essa D. Autarquia a oportunidade de apresentar considerações aos termos do Edital de Audiência Pública SDM nº 05/18, cujo objeto versa sobre alterações na Instrução CVM nº 505, de 27 de setembro de 2011 e revogação da Instrução CVM nº 380, de 23 de dezembro de 2002.

Dessa forma, apresentamos as sugestões de alteração e demais considerações devidamente detalhadas no quadro comparativo abaixo:

COMISSÃO DE VALORES MOBILIÁRIOS
Edital de Audiência Pública SDM nº 05/18

Texto original	Sugestão de alteração/ considerações gerais
INSTRUÇÃO CVM Nº [●], DE [●] DE [●] DE [●]	
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.	
O PRESIDENTE DA COMISSÃO DE VALORES MOBILIÁRIOS - CVM torna público que o Colegiado, em reunião realizada em [●] de [●] de [●], com fundamento no disposto no art. 18, inciso II, alíneas “a” e “c” da Lei nº 6.385, de 7 de dezembro de 1976, APROVOU a seguinte Instrução:	
Art. 1º Os arts. 1º, 3º a 5º, 12 a 21, 24, 31 a 36 e 38, os títulos das subseções que antecedem os arts. 14 e 15 e o título do capítulo e da seção que antecedem o art. 24 da Instrução CVM nº 505, de 27 de setembro de 2011, passam a vigorar com a seguinte redação:	

“Art. 1º	
II – REVOGADO	
V – ordem: ato prévio pelo qual o cliente determina que um intermediário negocie ou registre operação com valor mobiliário, nos termos do art. 12, em seu nome e nas condições que especificar;	Sugestão de alteração: <i>V – ordem: ato prévio pelo qual o cliente, procurador ou seu respectivo representante legal determina que um intermediário negocie ou registre operação com valor mobiliário, nos termos do art. 12, em seu nome e nas condições que especificar;</i>
VII – oferta: ato pelo qual o intermediário manifesta a intenção de realizar um negócio com valor mobiliário, para si ou para terceiro, registrando os termos e condições necessários no sistema de negociação de entidade administradora de mercados organizados;	Considerações gerais: Sugerimos avaliação sobre a pertinência de mencionar, expressamente, que as negociações privadas, na forma do inciso I, do artigo 59, da Instrução CVM 461, de 23/10/2007, não integram a definição de “oferta”, em especial para afastar qualquer dúvida de que as operações privadas do intermediário, levadas ao registro em entidade administradora de mercados organizados, não se subordinam ao regime da Instrução CVM 505.
VIII – conta-corrente: posição gráfica das movimentações financeiras dos clientes junto ao intermediário;	Sugestão de alteração: <i>VIII – sistema de conta-corrente: sistema para registro das movimentações financeiras referentes às operações dos clientes junto ao intermediário, bem como qualquer movimentação financeira acessória realizada para suportar as operações do cliente junto ao intermediário;</i>
IX – entidade autorreguladora: entidade responsável pelo exercício das atividades de autorregulação de que trata a regulamentação específica;	
X – órgãos de administração do intermediário: são os órgãos assim definidos nos seu estatuto ou contrato social;	
XI – diretor responsável: diretor estatutário responsável pelas atividades previstas no inciso I do art. 4º; e	
XII – diretor de controles internos: diretor estatutário responsável pelas atividades previstas no inciso II do art. 4º.”(NR)	
“Art. 3º	
III – estar disponíveis para consulta das pessoas mencionadas no art. 1º, inciso VI, alíneas “a” a “c”, da CVM, das entidades administradoras dos mercados organizados em que o intermediário seja autorizado a operar e da entidade autorreguladora, se for o caso.	
§ 4º Sem prejuízo da responsabilidade dos diretores	

referidos nos incisos I e II do caput do art. 4º, cabe aos órgãos de administração dos intermediários:	
I – aprovar as regras e procedimentos de que trata o caput ; e	
II – supervisionar o cumprimento e efetividade dos procedimentos e controles internos de que trata o caput. ” (NR)	
“Art. 4º	
	Sugestão de inclusão de texto: “§3º-A. Sem prejuízo da obrigação prevista no inciso II deste art., o intermediário pode designar responsável pelo cumprimento dos capítulos VIII-A e VIII-B desta Instrução, desde que não haja conflito de interesses, e que conste na política de segurança da informação prevista no art. 35-D desta Instrução a responsabilidade atribuída a cada um deles.
§ 5º O diretor de controles internos a que se refere o inciso II do caput deve encaminhar aos órgãos de administração do intermediário, até 30 de abril do ano seguinte ao da data base, relatório contendo, no mínimo:	Sugestão de alteração: § 5º O diretor de controles internos a que se refere o inciso II do caput deve encaminhar aos órgãos de administração do intermediário, até <u>o último dia útil do mês</u> 30 de abril do ano seguinte ao da data base, relatório contendo, no mínimo:
I – descrição detalhada e atualizada:	
a) dos controles internos implantados, informando os tipos de controles existentes e as atividades e operações abrangidas;	
b) da metodologia aplicada para a escolha e realização dos exames, indicando, por exemplo, mecanismos de monitoramento, parâmetros utilizados para verificação de anormalidades ou falhas, bem como critérios estabelecidos para a seleção de amostras; e	
c) dos procedimentos realizados para análise das deficiências encontradas.	
II – detalhamento dos testes realizados e das conclusões obtidas quanto à eficiência e eficácia dos controles internos para garantir o cumprimento do disposto nos Capítulos III a IX desta Instrução envolvendo:	
a) as atividades de cadastro de clientes, transmissão e execução de ordens, especificação de comitentes, operações com pessoas vinculadas, repasse de operações, pagamento e recebimento de valores, normas de conduta e manutenção de arquivos, abrangendo tanto a atuação do intermediário no mercado de bolsa quanto no mercado de balcão organizado; e	

<p>b) monitoramento da infraestrutura de tecnologia da informação, previsto nos capítulos VIII-A e VIII-B, com destaque para o programa de segurança cibernética de que trata o art. 35-H;</p>	
<p>III – recomendações quanto às eventuais deficiências identificadas pelo diretor de controles internos, pelo regulador e pela entidade autorreguladora, com o estabelecimento de planos de ação e de cronogramas de saneamento para correção, quando for o caso;</p>	<p>Sugestão de alteração: <i>III – recomendações do diretor de controles internos quanto às eventuais deficiências identificadas pelo diretor de controles internos pelo intermediário, pelo regulador e pela entidade autorreguladora, apuradas no período de referência do relatório, com o estabelecimento de planos de ação e de cronogramas de saneamento para correção, quando for o caso;</i></p>
<p>IV – relação das comunicações previstas no inciso IV do art. 32 e no art. 35-I que tiverem sido realizadas no período de referência do relatório, ou menção de não ter havido qualquer comunicação no período, quando for o caso;</p>	<p>Considerações gerais: Sugerimos a exclusão total do inciso IV, visto que que as comunicações já são realizadas no âmbito da ICVM 505 e ter que incluí-las no relatório seria um retrabalho.</p>
<p>V – avaliação de riscos para o intermediário em relação aos seus controles internos e quanto à sua vulnerabilidade a ataques cibernéticos; e</p>	
<p>VI – manifestação do diretor responsável de que trata o inciso I do caput a respeito das deficiências encontradas, contendo, no mínimo:</p>	
<p>a) em relação a cada uma das deficiências identificadas na última avaliação, incluindo as identificadas pela CVM e pela entidade autorreguladora, descrição das ações planejadas para saná-las;</p>	<p>Sugestão de alteração: <i>a) em relação a cada uma das deficiências identificadas na última avaliação do relatório de controles internos relativa ao ano anterior do calendário base, incluindo as identificadas pela CVM e pela entidade autorreguladora, descrição das ações planejadas para saná-las;</i></p>
<p>b) em relação às deficiências apontadas nos relatórios anteriores, informar se os cronogramas de saneamento foram implementados e o resultado das ações adotadas para sanar as deficiências;</p>	
<p>c) avaliação fundamentada sobre a evolução do intermediário no cumprimento das exigências desta Instrução durante o período de competência do relatório; e</p>	
<p>d) avaliação sobre a adequação do plano de continuidade de negócios, indicando as necessidades de aperfeiçoamento, quando necessário.</p>	
<p>§ 6º Todas as atividades mencionadas no inciso II do § 5º devem constar no relatório anual, ainda que não sejam aplicáveis aos processos internos do intermediário, sejam de pequena relevância ou</p>	

ofereçam baixo risco no contexto das atividades do intermediário, devendo ser apenas apresentado o motivo que justifica a ausência de menção às conclusões dos testes realizados nesses casos.	
§ 7º O relatório de que trata o § 5º deve ficar disponível na sede do intermediário para consulta da CVM, da entidade administradora do mercado em que esteja autorizado a operar e da entidade autorreguladora, se for o caso, não sendo necessário seu envio, exceto quando solicitado pela CVM e pelas entidades mencionadas neste parágrafo.” (NR)	
“Art. 5º	
§ 3º REVOGADO.	
§ 4º Os intermediários devem identificar as pessoas autorizadas a emitir ordens em nome de mais de um comitente e informar às entidades administradoras de mercado organizado nas quais operarem, se for o caso, nos termos e padrões por elas estabelecidos.”(NR)	
“Art. 12. O intermediário somente pode executar negócio ou registrar operação com valores mobiliários mediante ordem prévia do cliente e nas condições por este estabelecidas.	
§ 1º A ordem pode ser transmitida:	
I – por telefone ou outros sistemas de transmissão de voz;	
II – por escrito, incluindo as ordens recebidas presencialmente, por correio eletrônico ou por outros sistemas de mensagens eletrônicas; ou	
III – por sistemas eletrônicos de negociação de acesso direto ao mercado (direct market access – DMA).	
§ 2º Todas as ordens devem ser registradas, identificando-se o horário do seu recebimento, o cliente que as tenha emitido e as condições para a sua execução.	
§ 3º O cadastro do cliente deve identificar as formas de transmissão de ordens autorizadas ao cliente.	Sugestão de alteração: § 3º O cadastro do cliente intermediário deve formalizar junto ao cliente identificar as formas de transmissão de ordens por ele autorizadas ao cliente.
§ 4º O intermediário deve identificar o cliente, bem como seu procurador ou representante, por ocasião das transmissões de ordens nos termos do § 1º.”(NR)	Sugestão de alteração: § 4º O intermediário deve identificar e registrar o emissor da ordem, seja esta e transmitida pelo cliente, bem como seu procurador ou por seu representante, por ocasião das transmissões de ordens nos termos do § 1º.
“Art. 13.	

Parágrafo único. Sem prejuízo de outros procedimentos e controles adotados em função do art. 35-F, o intermediário deve possuir procedimentos específicos de arquivamento dos registros de dados e de voz relativos às ordens transmitidas que garantam:	
I – a confidencialidade, autenticidade, integridade e disponibilidade das informações;	Sugestão de alteração: <i>I – a confidencialidade, autenticidade, integridade e disponibilidade das informações;</i>
II – o atendimento ao disposto no parágrafo único do art. 5º-A; e	
III – a manutenção de cópias de segurança em ambiente distinto do destinado ao armazenamento das informações a que se refere o caput , em condições seguras de armazenamento, acesso e preservação.”(NR)	
“Subseção I – Gravação de Ordens	
Art. 14. O intermediário que atue em mercado organizado deve manter sistema de gravação de todos os diálogos mantidos com seus clientes, inclusive por intermédio de prepostos, de forma a gravar as ordens transmitidas por telefone ou outros sistemas de transmissão de voz.	
.....”(NR)	
“Subseção III - Ordens Transmitidas por Sistemas de Negociação de Acesso Direto ao Mercado	
Art. 15. O intermediário pode receber ordens de seus clientes por meio de sistemas eletrônicos de negociação de acesso direto ao mercado, de acordo com as condições e regras estabelecidas pelas entidades administradoras de mercados organizados.	Sugestão de alteração: <i>Art. 15. O intermediário pode receber ordens de seus clientes, bem como de seu procurador ou representante, por meio de sistemas eletrônicos de negociação de acesso direto ao mercado, de acordo com as condições e regras estabelecidas pelas entidades administradoras de mercados organizados.</i>
§ 1º O intermediário que receba ordens de seus clientes nas condições previstas no caput deve:	Sugestão de alteração: <i>§1º O intermediário que receba ordens de seus clientes, bem como de seu procurador ou representante, nas condições previstas no caput deve: (...)</i>
I – adotar procedimentos para identificar as origens das ordens e assegurar o rastreamento de seu emissor; e	Sugestão de alteração: <i>I – adotar procedimentos para buscar a identificação da origem das ordens identificar as origens das ordens e assegurar o rastreamento de seu emissor; e</i>
II – manter sistema de controle de gerenciamento de riscos pré-operacionais, incluindo o	Sugestão de alteração: II – manter sistema de controle de

<p>estabelecimento e monitoramento de limites operacionais e parâmetros para identificar transmissão de ordens fruto de erro, tais como ordens duplicadas ou com preço e volume atípicos.</p>	<p>gerenciamento de riscos pré-operacionais, incluindo o estabelecimento e monitoramento de limites operacionais e parâmetros para identificar transmissão de ordens fruto de erro. tais como ordens duplicadas ou com preço e volume atípicos.</p> <p>Considerações gerais: Embora o mercado brasileiro não apresente fragmentação pré-negociação, pode não ser oportuna a referência às ordens duplicadas ou ordens com preços e volumes atípicos como indicadores de erros , especialmente em razão de poderem integrar estratégias legítimas de negociação empregadas em negociação algorítmica (algorithmic trading – AT) e operações de alta frequência (high-frequency trading – HFT).</p>
<p>§ 2º Os sistemas de controles de gerenciamento de risco devem rejeitar ordens que excedam os limites operacionais estabelecidos pelo intermediário para cada cliente.”(NR)</p>	
<p>“Art. 16. O intermediário e o administrador de carteira não residentes somente podem ser usuários de terminais de sistemas eletrônicos de negociação de acesso direto ao mercado se atenderem aos seguintes requisitos:</p>	
<p>.....”(NR)</p>	
<p>“Art. 17. As entidades administradoras de mercados organizados devem adotar regulamento sobre o funcionamento dos sistemas eletrônicos de negociação de acesso direto ao mercado.</p>	
<p>§ 2º Nas regras de que trata o caput, as entidades administradoras de mercado organizado devem estabelecer que os intermediários que não sejam pessoas autorizadas a operar se submetam, por meio de disposição contratual expressa, ao seu poder de autorregulação, em relação às regras sobre a utilização de sistemas eletrônicos de negociação de acesso direto ao mercado.”(NR)</p>	
<p>“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.</p>	
<p>Parágrafo único. A entidade autorreguladora deve incluir as operações de que trata o caput no seu programa de trabalho.”(NR)</p>	
<p>“Art. 19.”</p>	
<p>§ 1º É vedado ao intermediário transmitir oferta de negócio previamente ao recebimento de ordem por</p>	

parte de seu cliente.	
§ 2º Para aferir as melhores condições para a execução de ordens, o intermediário deve levar em conta o preço, o custo, a rapidez, a probabilidade de execução e liquidação, o volume, a natureza e qualquer outra consideração relevante para execução da ordem.”(NR)	
“Art. 20.”	
§ 4º As regras de que trata o caput e suas alterações devem ser previamente informadas aos clientes e estar disponíveis na página do intermediário na rede mundial de computadores, nos aplicativos e em outras interfaces oferecidas a seus clientes.”(NR)	Sugestão de alteração: <i>§ 4º As regras de que trata o caput e suas alterações devem ser previamente informadas aos clientes <u>e/ou</u> estar disponíveis na página do intermediário na rede mundial de computadores, <u>e/ou</u> nos aplicativos, <u>via link para a página do intermediário</u> e em outras <u>interfaces formas de interação</u> oferecidas a seus clientes.</i>
“Art. 21. Os intermediários devem arquivar, previamente à sua entrada em vigor, as regras de que trata o art. 20 e suas alterações na entidade autorreguladora, nos termos e prazos estabelecidos pela entidade administradora de mercado organizado em que estejam autorizados a operar.”(NR)	
“CAPÍTULO V – PESSOAS VINCULADAS”(NR)	
“Seção I – REVOGADO.”(NR)	
“Art. 24. REVOGADO.”(NR)	
ART 25	
	Sugestão de inclusão de texto: <i>“§ 4º Exceção a esse requerimento pode ocorrer quando o intermediário estabelecer parceria com outro intermediário para que sejam, mediante autorização expressa do vinculado, fornecidas informações a respeito das operações efetuadas pelos vinculados ao intermediário a que são vinculados com a finalidade de acompanhamento interno de acordo com processos estabelecidos pelo intermediário. Cabendo a este a responsabilidade por esses monitoramentos.”</i>
“Art. 31.”	
Parágrafo único.”	
III – estabelecer mecanismos para informar ao cliente que o intermediário e as pessoas a ele vinculadas estão agindo em conflito de interesses e	

as fontes desse conflito, antes de efetuar uma operação.”(NR)	
“Art. 32.	
III – manter registro de conta-corrente de todas as movimentações financeiras de seus clientes;	Sugestão de alteração: <i>III – manter registro sistema de conta-corrente para registro de todas as movimentações financeiras de seus clientes;</i>
IV – informar à CVM sempre que verifique a ocorrência ou indícios de violação da legislação que incumba à CVM fiscalizar, no prazo máximo de 5 (cinco) dias úteis da ocorrência ou identificação, sem prejuízo da comunicação às entidades administradoras dos mercados organizados em que seja autorizado a operar ou à entidade autorreguladora, mantendo registro das evidências encontradas;	
IX – monitorar continuamente as operações por ele intermediadas, de maneira a identificar as que visem proporcionar vantagem indevida ou lucro para uma das partes, ou causar dano a terceiros, conforme regulação específica;	
X – garantir a implementação do plano de continuidade e da política de segurança da informação, nos termos dos Capítulos VIII-A e VIII-B;	
XI – manter controle da identificação das pessoas que tenham acesso aos seus fóruns de comunicação digital; e	
XII – colocar em sua página na rede mundial de computadores, aplicativos ou outras interfaces um atalho para página da CVM na rede mundial de computadores ou aviso em destaque, com o seguinte informe:	Sugestão de alteração: <i>XII – colocar em sua página na rede mundial de computadores, aplicativos ou outras interfaces formas de interações que tenha com o cliente um atalho para a página da CVM na rede mundial de computadores ou aviso em destaque, com o seguinte informe: (...)</i>
"Toda transmissão de ordens por meio digital está sujeita a interrupções ou atrasos, podendo impedir ou prejudicar o envio de ordens ou a recepção de informações atualizadas".	
§ 1º A estrutura de tecnologia da informação deve ser compatível com o volume, natureza e complexidade de suas operações, inclusive no que diz respeito aos sistemas eletrônicos de negociação de acesso direto ao mercado, bem como a outras interfaces com seus clientes.	
§ 2º Os sistemas tecnológicos utilizados pelo intermediário devem ser passíveis de auditoria, devendo o intermediário submetê-los a testes	Considerações gerais: Não foi especificada a periodicidade na qual os sistemas tecnológicos dos

periódicos para verificar o seu funcionamento em cenários de estresse.”(NR)	intermediários devem ser submetidos a testes de estresse, o que gera insegurança jurídica acerca do regular cumprimento da regra.
“Art. 33. O intermediário deve divulgar, em sua página na rede mundial de computadores, antes do início de suas operações, as regras internas elaboradas para o cumprimento desta Seção e suas alterações, exceto no que diz respeito aos planos previstos nos arts. 35-A e 35-H.”(NR)	
“Art. 34. Os intermediários devem arquivar, previamente à sua entrada em vigor, as regras internas adotadas para o cumprimento do disposto nesta Seção e no Capítulo II e suas alterações, na entidade administradora de mercado organizado em que estejam autorizados a operar e na entidade autorreguladora, se for o caso.	
§ 1º Cabe à entidade administradora de mercado organizado em que o intermediário estiver autorizado a operar e à entidade autorreguladora definir o conteúdo mínimo das regras internas adotadas por cada intermediário e fiscalizá-las.”	
.....”(NR)	
“Art. 35.	
VI – cobrar dos clientes corretagem ou qualquer outra comissão referente a negociações com valores mobiliários durante o período de sua distribuição pública, com exceção de negociação em mercados organizados com valores mobiliários já negociados em tal mercado e desde que o cliente seja devidamente informado sobre a distribuição pública em curso;	
VII – permitir que analistas, consultores ou gestores com quem mantenha vínculo empregatício ou contrato de prestação de serviços exerçam atividades para as quais não estejam expressamente autorizados pela CVM;	Sugestão de alteração: <i>VII – contratar permitir que analistas, consultores ou gestores com quem mantenha vínculo empregatício ou contrato por meio de prestação de serviços exerçam para atividades que não estejam expressamente autorizados pela CVM;</i>
VIII – executar transferências de recursos entre contas correntes gráficas de clientes de titularidades diferentes;	Sugestão de alteração: <i>VIII – executar transferências de recursos entre sistema de contas-correntes gráficas de clientes de titularidades diferentes;</i>
IX – realizar movimentações financeiras ou transferências de custódia sem que esteja autorizado pelo cliente;	Sugestão de alteração: <i>IX – realizar movimentações financeiras ou transferências de custódia sem que esteja autorizado pelo cliente, observadas as exceções legais e regulamentares;</i>

X – permitir a presença de clientes, em qualquer hipótese, no ambiente da mesa de operações; e	
XI – aplicar, na constituição e operação de sua carteira, recursos de clientes.” (NR)	
“Art. 36. Os intermediários devem manter, pelo prazo mínimo de 5 (cinco) anos contados do recebimento ou da geração pelo intermediário, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos por esta Instrução, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções, sejam eles físicos ou eletrônicos, assim como a íntegra das gravações referidas no art. 14, as trilhas de auditoria referidas no art. 5º-A e no inciso II do parágrafo único do art. 13, e os registros das origens das ordens referidos no § 1º, inciso I, do art. 15.	
§ 1º As imagens digitalizadas são admitidas em substituição aos documentos originais, desde que submetidas previamente a procedimento consistente, formal e verificável de autenticação de dados.	Sugestão de alteração: <i>§ 1º As imagens digitalizadas são admitidas em substituição aos documentos originais, desde que submetidas previamente a procedimento consistente, formal e verificável de autenticação das informações constantes dos documentos originais. de dados.</i>
§ 2º Os prestadores de serviços responsáveis pelos documentos digitalizados e as cópias de segurança dos documentos digitalizados devem estar sediados no país ou em países signatários dos Memorandos Multilaterais de Entendimento da IOSCO (MMoU).”(NR)	Considerações gerais: Sugerimos a exclusão integral do § 2º, visto que a restrição contida na Resolução CMN 4474/16 no sentido de que os documentos digitalizados e cópias de segurança devem ser armazenados no Brasil foi revogada pela Resolução CMN 4697/18. Na mesma linha, entendemos que não deveria haver restrições para a contratação de prestadores de serviços responsáveis pela digitalização de documentos no exterior. Cumpre indicar que a restrição para contratar prestador de serviços até para serviços relevantes de processamento, armazenamento e <i>cloud</i> deixou de existir, conforme os termos da Resolução 4.658/2018.
“Art. 38. Considera-se infração grave, para efeito do disposto no § 3º do art. 11 da Lei nº 6.385, de 1976, a infração às normas contidas nos arts. 2º a 5º; 12 a 14; 19 a 23; 29 a 32; 35, 35-A a 35-I e 36.”(NR)	
Art. 2º A Instrução CVM nº 505, de 27 de setembro	

de 2011, passa a vigorar acrescida dos artigos 5º-A, 14-A, e dos Capítulos VIII-A e VIII-B, com a seguinte redação:	
“Art. 5º-A. O cadastro de clientes mantido pelo intermediário deve permitir a identificação da data e do conteúdo de todas as alterações e atualizações realizadas.	
Parágrafo único. Sem prejuízo de outros procedimentos e controles adotados em função do art. 35-B, o intermediário deve garantir que os sistemas eletrônicos de cadastro contenham trilhas de auditoria íntegras e suficientes para assegurar o rastreamento das inclusões, alterações e exclusões, e que permitam identificar, no mínimo:	
I – o usuário responsável;	
II – a data e horário da ocorrência do evento; e	
III – se o evento se trata de inclusão, alteração ou exclusão.”(NR)	
“Art. 14-A. A ordem recebida presencialmente deve ser documentada, em meio físico ou digital, previamente à sua execução, contendo, no mínimo:	
I – data e horário de recebimento;	
II – assinatura do cliente;	
III – identificação de quem recebeu;	
IV – natureza e tipo de ordem, conforme previsto na regulamentação da entidade administradora de mercados organizados;	
V – prazo de validade da ordem; e	
VI – descrição do valor mobiliário, das quantidades e, se for o caso, dos preços.	
Parágrafo único. Os documentos referidos no caput devem ser arquivados pelo prazo estabelecido no art. 36 desta Instrução.”(NR)	
“CAPÍTULO VIII-A – PLANO DE CONTINUIDADE DE NEGÓCIOS	
Seção I – Regras Gerais	
Art. 35-A. O intermediário deve implementar e manter:	
I – processo de análise de impacto de negócios de forma a:	
a) identificar e classificar os processos críticos de negócio; e	
b) avaliar os potenciais efeitos da interrupção dos processos críticos de negócio sobre suas atividades; e	
II – planos de continuidade de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as ações de comunicação necessárias a clientes e às entidades administradoras de mercado	<i>Sugestão de alteração: II – planos de continuidade de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as</i>

<p>organizado em que sejam autorizados a operar.</p>	<p><i>ações de comunicação necessárias. e clientes e às entidades administradoras de mercado organizado em que sejam autorizados a operar</i></p>
<p>§ 1º O plano de continuidade deve, no mínimo, abranger os processos relacionados à recepção e execução de ordens, liquidação junto às entidades administradoras de mercados organizados, liquidação de seus clientes, conciliação e atualização das posições de seus clientes, além de outros considerados críticos pelo intermediário.</p>	<p><i>Sugestão de alteração:</i></p> <p><i>§ 1º O plano de continuidade deve, no mínimo quando aplicável, abranger os processos relacionados à recepção e execução de ordens, liquidação junto às entidades administradoras de mercados organizados, liquidação de seus clientes, conciliação e atualização das posições de seus clientes, além de outros considerados críticos pelo intermediário.</i></p>
<p>§ 2º O plano de continuidade deve conter plano de contingência desenvolvido pelo intermediário para seus sistemas , com o objetivo de preservar o atendimento aos investidores nos casos de suspensões no atendimento pela rede mundial de computadores, períodos de indisponibilidade ou picos de demanda.</p>	<p><i>Sugestão de alteração:</i></p> <p><i>§2º O plano de continuidade deve conter plano de contingência desenvolvido pelo intermediário para assegurar a continuidade das atividades da instituição e o estabelecimento de procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio.</i></p>
<p>§ 3º O intermediário deve realizar testes periódicos para monitorar a eficiência e eficácia do seu plano de continuidade de negócios.</p>	<p><i>Sugestão de alteração:</i></p> <p><i>§ 3º O intermediário deve realizar testes periódicos para monitorar a eficiência e eficácia do seu plano de continuidade de negócios com periodicidade adequada.</i></p> <p><i>Considerações gerais:</i> Não foi especificada a periodicidade na qual o plano de continuidade de negócios dos intermediários deve ser submetido a testes de eficiência e eficácia, o que gera insegurança jurídica acerca do regular cumprimento da regra.</p>
<p>Seção II – Sistemas críticos</p>	
<p>Art. 35-B. Sistemas críticos são aqueles que se vinculam aos processos críticos e que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios do intermediário.</p>	<p><i>Considerações gerais:</i> Sugerimos que esta redação seja indicada no rol de definições.</p>
<p>Parágrafo único. Devem ser considerados críticos, no mínimo, os sistemas que envolvem à recepção e execução de ordens, liquidação junto às entidades</p>	

administradoras de mercados organizados, liquidação com clientes e atualização das posições de seus clientes.	
Art. 35-C. O intermediário deve desenvolver e implementar políticas e práticas visando garantir a confidencialidade, a integridade e a disponibilidade dos sistemas críticos utilizados, que estabeleçam:	Considerações gerais: Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar a continuidade de negócios. Sugerimos observância aos termos do Art 20 da Resolução CMN 4.658/2018.
I – as diretrizes para a avaliação da relevância dos incidentes; e	
II – os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes que impliquem na interrupção de seus sistemas críticos, suas causas e impactos sobre o intermediário.	Considerações gerais: Um dos pontos de maior preocupação é a obrigação de prever expressamente na política. Indicar o detalhamento das tecnologias, das rotinas e dos controles adotados, além de revelar segredos de negócio de cada entidade com relação à sua estratégia de segurança, exporia o intermediário a vulnerabilidades. Neste ponto, muito embora fosse desejável que o público em geral pudesse conhecer as práticas de segurança de cada instituição, tal exigência é muito crítica do ponto de vista de segurança. Dessa forma entendemos que o apontamento de forma genérica tão somente dos controles adotados já seria suficiente.
Parágrafo único. O intermediário deve, tempestivamente, comunicar à Superintendência de Relações com o Mercado e Intermediários (SMI) a ocorrência de incidentes relevantes que tenham afetado seus sistemas críticos.”(NR)	<i>Sugestão de alteração:</i> Parágrafo único. O intermediário deve, tempestivamente, comunicar à Superintendência de Relações com o Mercado e Intermediários (SMI) a ocorrência de incidentes relevantes que tenham afetado seus sistemas relevantes críticos .”(NR)
“CAPÍTULO VIII-B – SEGURANÇA DAS INFORMAÇÕES	
Seção I – Abrangência	
Art. 35-D. O intermediário deve desenvolver política de segurança da informação que defina regras, procedimentos e controles internos relacionados:	<i>Sugestão de alteração:</i> Art. 35-D. O intermediário deve desenvolver política de segurança da informação que defina regras, procedimentos e controles internos relacionados: Considerações gerais: O intermediário deve desenvolver política de segurança da informação compatível com o porte, o perfil de risco e o modelo de negócio da instituição; com a natureza das operações e a complexidade dos

	produtos, serviços, atividades e processos da instituição; e compatível com a sensibilidade dos dados e das informações sob responsabilidade da instituição.
I – ao tratamento e controle de dados de clientes;	
II – à segurança cibernética; e	
III – à contratação de serviços prestados por terceiros.	<p><i>Sugestão de alteração:</i> III – à contratação de serviços prestados por terceiros.</p> <p><i>Considerações gerais:</i> Caso o pedido de exclusão total não seja acatado, alternativamente sugerimos alterar o texto para:</p> <p>“à contratação de serviços críticos, nos termos do art.35-B desta instrução”, de forma a deixar claro que os serviços críticos ou relevantes para fins dessa resolução são aqueles de envio e recebimento de ordem e de liquidação. A contratação de serviços poderia abarcar apenas o que sejam considerados relevantes pelo intermediário, desde que tenham como objeto o processamento e armazenamento de dados e computação em nuvem e sejam relacionados aos processos críticos do intermediário.</p>
§ 1º Admite-se, no caso de conglomerados financeiros, a adoção de uma única política a que se refere o caput , desde que as instituições que não constituírem política própria formalizem essa opção em reunião de seu conselho de administração ou de sua diretoria.	
	<p><i>Sugestão de inclusão de texto:</i> § 2º A política mencionada no caput deve:</p> <p>I - ser compatível com:</p> <p>a. o porte, o perfil de risco e o modelo de negócio do intermediário; b. a natureza das operações e a complexidade dos produtos, serviços, atividades e processos do intermediário; e c. a sensibilidade dos dados e das informações sob responsabilidade do intermediário.</p> <p>II - ser dirigida aos funcionários e prestadores de serviço;</p>
Seção II – Tratamento e Controle de Dados de	

Clientes	
<p>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:</p>	<p>Sugestão de alteração de texto: <i>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 sensíveis ou que sejam relevantes, contemplando:</i></p> <p>Considerações gerais: A autenticidade não deve ser validada no momento do armazenamento do dado e sim no momento de sua captura.</p>
<p>I – a classificação dos dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;</p>	<p>Considerações gerais: Sugerimos a exclusão total do inciso, visto que o tema já foi contemplado no item 35-D.</p>
<p>II – as diretrizes para a avaliação da relevância dos incidentes; e</p>	
<p>III – os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos.</p>	
<p>Parágrafo único. O intermediário deve considerar, no mínimo, os dados que permitem a identificação dos seus clientes e a suas operações como informações sensíveis.</p>	
<p>Art. 35-F. As regras, procedimentos e controles internos relacionados aos dados e informações sensíveis devem contemplar:</p>	
<p>I – proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso não autorizado, vazamento, adulteração e destruição;</p>	<p>Sugestão de alteração de texto: I – proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso não autorizado, vazamento, adulteração ou destruição não autorizada;</p>
<p>II – concessão e administração de acessos individualizados a sistemas, a bases de dados e a redes;</p>	
<p>III – segregação de funções, de forma a garantir o rastreamento e reduzir o risco de acesso não autorizado e de modificação ou mau uso das informações;</p>	<p>Sugestão de alteração de texto: III – segregação de dados e dos controles de acesso funções, de forma a mitigar garantir o rastreamento e reduzir o risco de acesso não autorizado e de adulteração modificação ou mau uso das informações;</p>
<p>IV – manutenção de política de segurança da informação dirigida aos funcionários, parceiros e prestadores de serviço; e</p>	<p>Considerações gerais: Tendo em vista o grau de detalhamento de informações que a norma está exigindo e que as informações constantes da política têm caráter estratégico, a manutenção de seu sigilo é necessária, justamente, para</p>

	<p>não expor as instituições e os clientes a riscos. Desse modo, não é aconselhável, sob o ponto de vista de segurança da informação, permitir que a política e a estratégia de segurança sejam de conhecimento do público em geral. Assim, sugerimos a exclusão deste inciso. Caso este não seja o entendimento desta D. Autarquia, a norma deve permitir que apenas a versão simplificada e genérica da política possa ser divulgada a terceiros, mediante solicitação destes e, preferencialmente, limitando os terceiros que poderiam ter acesso a esta política.</p>
<p>V – avaliação periódica sobre as ameaças e vulnerabilidades.</p>	<p>Sugerimos que este item seja movido para item 35 D, pois refere-se a um item de contexto geral e não somente de dados.</p> <p>Considerações gerais: Não foi especificada a periodicidade na qual as ameaças e as vulnerabilidades dos intermediários devem ser submetidas à avaliação, o que gera insegurança jurídica acerca do regular cumprimento da regra.</p>
<p>Parágrafo único. O intermediário deve manter programa de treinamento contínuo para funcionários, colaboradores e agentes autônomos contratados, destinado a divulgar as regras, procedimentos e controles internos mencionados no caput.</p>	<p>Sugestão de alteração de texto: <i>O intermediário deve manter programa de treinamento contínuo destinado a divulgar as regras, procedimentos e controles internos mencionados no § 3º para funcionários, colaboradores e agentes autônomos contratados que tenham acesso a informação e dados. destinado a divulgar as regras, procedimentos e controles internos mencionados no caput.</i></p>
<p>Art. 35-G. O intermediário deve manter público e orientar seus clientes e prepostos sobre suas boas práticas de segurança das informações, abordando, no mínimo;</p>	<p>Sugestão de alteração de texto: Art. 35-G. O intermediário deve manter público e orientar seus clientes e prepostos sobre suas boas práticas de segurança das informações, abordando, no mínimo;</p>
<p>I – práticas adotadas pelo intermediário quanto:</p>	<p>Sugestão de alteração de texto: I – práticas adotadas pelo intermediário quanto:</p>
<p>a) aos controles de acesso lógico;</p>	<p>Sugestão de alteração de texto: a) aos controles de acesso lógico;</p>
<p>b) à proteção da confidencialidade dos dados cadastrais, operações e posição de custódia de seus clientes; e</p>	<p>Sugestão de alteração de texto: b) à proteção da confidencialidade dos dados cadastrais, operações e posição de custódia de seus clientes; e</p>
<p>c) a comunicações ao cliente em caso de incidentes de segurança envolvendo informações de cadastro e de operações realizadas que possam acarretar risco</p>	<p>Sugestão de alteração de texto: c) a comunicações ao cliente em caso de incidentes de segurança envolvendo</p>

ou dano relevante ao cliente; e	informações de cadastro e de operações realizadas que possam acarretar risco ou dano relevante ao cliente; e
II – cuidados a serem tomados pelos clientes com a segurança cibernética no acesso aos sistemas providos pelo intermediário.	<p>Sugestão de alteração de texto:</p> <p>II – cuidados a serem tomados pelos clientes com a segurança cibernética no acesso aos sistemas providos pelo intermediário.</p> <p>Considerações gerais: A política de segurança da informação deve ser divulgada aos funcionários da instituição e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. As instituições devem divulgar ao público resumo contendo as linhas gerais da política de segurança da informação.</p>
Seção III – Segurança cibernética	
Art. 35-H. A política a que se refere o art. 35-D, inciso II, deve contemplar o programa de segurança cibernética, abrangendo, no mínimo:	
I – a identificação e avaliação dos riscos cibernéticos internos e externos a que o intermediário esteja exposto, incluindo a categorização de eventos de segurança;	
II – as medidas que devem ser adotadas para reduzir a vulnerabilidade da instituição contra ataques cibernéticos;	
III – procedimentos e controles internos que serão adotados para:	
a) verificar a implementação, a aplicação e a eficácia das medidas adotadas na forma do inciso II; e	
b) efetuar o monitoramento contínuo e a detecção de ataques cibernéticos em tempo hábil;	
IV – plano de resposta para tratamento de incidentes cibernéticos e recuperação de dados e sistemas, incluindo plano de comunicação interna e externa;	
V – plano de revisão do programa de segurança cibernética, de forma a identificar e a avaliar novos riscos cibernéticos e a necessidade de adotar e implementar novas regras, procedimentos e controles internos com o objetivo de prevenir e proteger contra ataques cibernéticos;	
VI – plano de treinamento periódico de seus funcionários e prepostos, de forma a prevenir e proteger os sistemas contra ataques cibernéticos;	<p>Considerações gerais: Não foi especificada a periodicidade na qual as vulnerabilidades dos intermediários</p>

	<p>contra ataques cibernéticos devem ser submetidas a teste, o que gera insegurança jurídica acerca do regular cumprimento da regra.</p>
<p>VII – realização de testes periódicos para avaliar a vulnerabilidade da instituição contra ataques cibernéticos; e</p>	
<p>VIII – formas de participação em iniciativas que objetivem o compartilhamento de informações sobre incidentes relevantes.</p>	<p><i>Sugestão de alteração:</i> VIII – formas de participação em iniciativas que objetivem o compartilhamento de informações sobre ameaças ou vulnerabilidades relevantes.</p> <p><i>Considerações gerais:</i> Entendemos que o compartilhamento de informações sobre incidentes relevantes de terceiros deve ser facultativo e só pode ocorrer desde que não infrinja contratos e acordos já estabelecidos. Por essa razão ficaria a critério da instituição a possibilidade de compartilhamento de informações de incidentes de terceiros após a avaliação de possíveis riscos contratuais e legais dessa ação.</p>
<p>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.</p>	<p><i>Sugestão de alteração:</i> Art. 35-I. O intermediário deve comunicar tempestivamente 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.</p> <p><i>Considerações gerais:</i> Sugerimos adequar para os termos já utilizados na Resolução CMN 4.658/2018 e na Lei 13.709/2018, dependendo da magnitude do incidente, o prazo indicado é extremamente exíguo.</p>
<p>§ 1º Considera-se relevante o incidente de segurança cibernética que afete dados sensíveis ou sistemas críticos de forma a impactar significativamente os clientes.</p>	<p><i>Sugestão de alteração:</i> § 1º Para fins dessa Instrução, considera-se serviços críticos relevantes aqueles relacionados aos processos críticos identificados no âmbito da análise a que se refere o inciso I do art. 35-A.</p>
<p>§ 2º No prazo de 45 (quarenta e cinco) dias O intermediário deve encaminhar relatório à SMI, contendo, no mínimo:</p>	<p><i>Considerações gerais:</i> Sugerimos adequação aos termos já utilizados na Resolução CMN 4.658/2018 e na Lei 13.709/2018, dependendo da magnitude do incidente, o prazo indicado é</p>

	extremamente exíguo.
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;	<i>Sugestão de alteração:</i> II – cópia das comunicações realizadas com seus clientes, quando aplicável ;
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.	
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:	<i>Sugestão de alteração:</i> <i>Art. 35-J. No caso de serviços prestados por terceiros, o intermediário deve identificar e relacionar seus prestadores de serviços críticos relevantes, avaliar os controles realizados por estes provedores e prever em seu contrato de prestação de serviços, o cumprimento</i>
I – das exigências previstas no art. 36;	
II – o acesso da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviços; e	
III – a confidencialidade, integridade, disponibilidade e a recuperação dos dados e informações processados ou armazenados pelo prestador de serviços.	
§ 1º Para fins dessa Instrução, considera-se serviços críticos aqueles relacionados aos processos críticos identificados no âmbito da análise a que se refere o inciso I do art. 35-A.	<i>Sugestão de alteração:</i> <i>§ 1º Para fins dessa Instrução, considera-se serviços críticos relevantes aqueles relacionados aos processos críticos identificados no âmbito da análise a que se refere o inciso I do art. 35-A.</i>
§ 2º A contratação de terceiros não afasta a responsabilidade do intermediário pelo registro e armazenagem dos documentos e informações mencionadas no art. 36.	
29 § 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 serviço; e	
III – às dependências do contratado.” (NR)	<p><i>Sugestão de alteração:</i> III - aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados.</p> <p>Considerações gerais: Não haveria necessidade de impor ao terceiro contratado o acesso às dependências do fornecedor pela CVM. Inclusive, tal obrigação foi excluída da versão final da Resolução CMN 4.658/18, tendo sido mantido o acesso aos relatórios de auditoria especializada.</p>
Art. 3º A redação do título da subseção II do Capítulo IV, que antecede o art.14-A, da Instrução CVM nº 505, de 27 de setembro de 2011, passa a vigorar com a seguinte redação:	
“Subseção II - Ordens Transmitidas Presencialmente”(NR)	
Art. 4º Ficam revogados:	
I – a Instrução CVM nº 380, de 23 de dezembro de 2002; e	
II – os arts. 1º, inciso II; 5º, § 3º; e a seção I do Capítulo V da Instrução CVM nº 505, de 27 de setembro de 2011.	
Art. 5º Esta Instrução entra em vigor 180 (cento oitenta) dias após a sua publicação.	
<i>Original assinado por</i> MARCELO BARBOSA Presidente	

Nesse sentido, colocamo-nos à disposição dessa Autarquia para buscar alternativas para endereçar as preocupações aqui manifestadas, discutir nossos comentários ou outros temas relacionados que sejam considerados relevantes para a adequada redação para a regulação pretendida.

Cordialmente,

FEDERAÇÃO BRASILEIRA DE BANCOS