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

À Superintendência de Desenvolvimento de Mercado ("SDM")

Rua Sete de Setembro, 111, 23º andar, Rio de Janeiro – RJ, CEP 20050-901.

Endereço eletrônico: audpublicaSDM0518@cvm.gov.br

Ref.: Edital de Consulta Pública 55/2017, de 30 de agosto de 2017

Prezados Senhores,

Conforme Edital de Audiência Pública SDM nº 05/2018 ("Audiência Pública" e "Edital", conforme o caso), aproveitamos a oportunidade para anexar à presente nossos comentários e sugestões à minuta de Instrução proposta ("Minuta") que visa aprimorar os mecanismos de controles internos dos intermediários no que se refere a risco de eventos de qualquer natureza que possam provocar a parada da execução de suas atividades, em decorrência da interrupção de seus processos críticos, e o risco de falhas relacionadas à segurança da informação associadas aos processos, sistemas e infraestrutura de tecnologia da informação

Nossos comentários e sugestões são apresentados de forma segmentada para cada dispositivo da Minuta, iniciando com um quadro comparativo entre o texto da Minuta (à esquerda) e o texto com nossas propostas de ajuste ou de inclusão (à direita), tendo em seguida as justificativas para o ajuste ou inclusão proposto.

Do lado esquerdo marcamos em vermelho as partes que sugerimos retirar do texto da Minuta e do lado direito marcamos em verde as sugestões de inclusão. As primeiras alterações se referem à inclusão de novos termos definidos no artigo 1° e em seguida sugerimos alterações conforme a ordem da Minuta.

Cumprimentamos essa D. Comissão pela iniciativa de atualizar os procedimentos de operações envolvendo valores mobiliários com as discussões mais atuais de segurança da informação, principalmente à luz da aprovação da Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados ("LGPD").

Permanecemos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Baptista Luz, Gimenez & Freitas Advogados

Anexo – Comentários e sugestões à Minuta da Resolução

<table>
<tr><td>1.</td><td colspan="2">Art. 1° – Alteração
Assunto: Inclusão de termo definido</td></tr>
<tr><td colspan="2">Texto da Minuta</td><td>Texto Proposto</td></tr>
<tr><td colspan="2">Art. 35-I.

(...)

<s>§ 1º Considera-se relevante o incidente de segurança cibernética que afete dados sensíveis
ou sistemas críticos de forma a impactar significativamente os clientes</s></td><td>Art. 1º. Considera-se, para os efeitos desta Instrução:

(...)

XIII – incidente de segurança da informação e uso inadequado dos dados: ocorrência conforme descrito no artigo 46 da Lei nº 13.709, de 14 de agosto de 2018;

XIV - incidente relevante de segurança da informação e uso inadequado dos dados: ocorrência conforme descrito no artigo 46 da Lei nº 13.709, de 14 de agosto de 2018 que afete dados sensíveis ou sistemas críticos de forma a impactar significativamente os clientes apresentando risco ou dano a estes;</td></tr>
<tr><td colspan="3">Justificativa:

Notamos que ao longo da Minuta foram utilizadas diversas vezes os termos “incidentes cibernéticos”, “incidentes de segurança cibernética”, “incidentes
relevantes” ou até apenas “incidentes”. Acreditamos que a ausência de termos definidos no artigo 1° e a falta de padronização da nomenclatura geraram ambiguidade, especialmente porque entendemos que existem dois tipos diferentes de incidentes que a Minuta aborda. Discutiremos aqui um destes incidentes e o outro tipo de incidente abordaremos na próxima alteração sugerida.

O primeiro tipo de incidente que identificamos é o que a Minuta chama algumas vezes de “incidentes de segurança cibernética” e outras de “incidentes cibernéticos”. No nosso entendimento este evento é o que a LGPD se refere em seu artigo 46 e por isso sugerimos a criação de uma remissão.

Para utilizar o vocabulário da LGPD e descrever melhor o fenômeno sugerimos que estes eventos sejam chamados de “incidente de segurança da informação e uso inadequado dos dados”.

Contudo, o Art. 35-I, § 1º cria uma definição para os casos relevantes de “incidente de segurança cibernética”. Com isso em mente, sugerimos que além de incluir no artigo 1°</td></tr>
</table>

1.	Art. 1° – Alteração Assunto: Inclusão de termo definido
a definição para "incidente de segurança da informação e uso inadequado dos dados" façamos o mesmo para os casos relevantes, levando em conta a redação trazida pelo Art. 35-I, § 1º. Caso estes termos sejam incorporados alguns artigos teriam que ser alterados refletindo a nova nomenclatura. O termo "incidente relevante de segurança da informação e uso inadequado dos dados" deveria substituir os seus sinônimos nos artigos: 4°, V; 35-C, I; 35-C, II; 35-C, Parágrafo Único; 35-E, II; 35-E, III; 35-G, I, c; 35-H, IV; 35-H, VIII; 35-I, caput; 35-I, §2º, I; 35-I, §2º, III; e 35-I, §2º, IV. [1] Importante notar que com isso o Art. 35-I, § 1º seria excluído uma vez que seu conteúdo configuraria na definição do termo no Art. 1°, XIV.	

[1] Conforme mencionaremos mais adiante, acreditamos que alguns dos artigos do capítulo de Segurança da Informação devem mencionar ambos os tipos de incidentes relevantes ("incidente relevante de segurança da informação e uso inadequado dos dados" e "incidente relevante de interrupção") principalmente no que se refere a fazer o *disclosure* do evento.

2.	Art. 1° – Alteração Assunto: Inclusão de termo definido
Texto da Minuta	**Texto Proposto**
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: (...) 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.~~	Art. 1º. Considera-se, para os efeitos desta Instrução: **XV – incidente relevante de interrupção: aquele que afete ou implique na interrupção dos sistemas críticos do intermediário.** **XVI – incidentes relevantes: entende-se por incidentes relevantes os incidentes relevantes de segurança da informação e uso inadequado dos dados e os incidentes relevantes de interrupção.**

Justificativa:

Conforme mencionamos no item acima, entendemos que existam dois tipos principais de incidentes que a Minuta aborda, contudo, a falta de padronização da nomenclatura gerou ambiguidade. Assim, entendemos que o segundo tipo de incidente é aquele indiretamente definido pelo inciso II do Art. 35-C, conforme excerto acima do lado esquerdo.

Portanto, sugerimos que este tipo de incidente passe a ser denominado de "incidente relevante de interrupção" para diferenciá-lo do outro tipo que sugerimos ser chamado de "incidente relevante de segurança da informação e uso inadequado dos dados".

Para simplificar a redação da norma, sugerimos que o termo "incidentes relevantes" seja usado quando forem se referir a ambos os "incidentes relevantes de segurança da informação e uso inadequado dos dados" e os "incidentes relevantes de interrupção".

Caso este termo seja incorporado alguns artigos teriam que ser alterados refletindo a nova nomenclatura. O termo "incidente relevante de interrupção" deveria substituir os seus sinônimos nos artigos: 4°, V; 35-C, I; 35-C, II; 35-C, Parágrafo Único; 35-E, II e 35-E, III.[2]

Importante notar que com isso o Art. 35-C, II seria parcialmente excluído uma vez que seu conteúdo configuraria na definição do termo no Art. 1°, XV.

[2] Conforme mencionaremos mais adiante, acreditamos que alguns dos artigos do capítulo de Segurança da Informação devem mencionar ambos os tipos de incidentes relevantes ("incidente relevante de segurança da informação e uso inadequado dos dados" e "incidente relevante de interrupção") principalmente no que se refere a fazer o *disclosure* do evento.

3.	Art. 1° – Alteração Assunto: Inclusão de termo definido
Texto da Minuta	**Texto Proposto**
N/A	Art. 1º. Considera-se, para os efeitos desta Instrução: **XVII – dado pessoal: informação relacionada a pessoa natural identificada ou identificável conforme definido no artigo 5° da Lei nº 13.709, de 14 de agosto de 2018;**
Justificativa: A inclusão da definição de dados pessoal presente no art. 5º, I, da Lei 13.709/2018 no art. 1º da Instrução CVM 505, confere maior segurança ao termo utilizado e intensifica a criação de um sistema de proteção de dados coeso com nomenclatura coincidente.	

4.	**Art. 1° – Alteração** **Assunto: Inclusão de termo definido**
Texto da Minuta	**Texto Proposto**
N/A	Art. 1º. Considera-se, para os efeitos desta Instrução: **XVIII – dado 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, conforme definido no artigo 5° da Lei nº 13.709, de 14 de agosto de 2018;**
Justificativa: A inclusão da definição de dados pessoal sensível presente no art. 5º, II, da Lei 13.709/2018 no art. 1º da Instrução CVM 505, confere maior segurança ao termo utilizado e intensifica a criação de um sistema de proteção de dados coeso com nomenclatura coincidente.	

5.	Art. 1° – Alteração Assunto: Inclusão de termo definido

Texto da Minuta	Texto Proposto
~~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~~ ~~Parágrafo único. Devem ser considerados críticos, no mínimo, os sistemas que envolvem à recepção e execução de ordens, liquidação junto às entidades administradoras de mercados organizados, liquidação com clientes e atualização das posições de seus clientes.~~	Art. 1º Considera-se, para os efeitos desta Instrução: **XIX – Sistemas críticos: são aqueles que se vinculam aos processos críticos que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios do intermediário** **XX – Processos críticos: são os sistemas que envolvem à recepção e execução de ordens, liquidação junto às entidades administradoras de mercados organizados, liquidação com clientes e atualização das posições de seus clientes.**

Justificativa:

A subdivisão do artigo 35 em diversos itens não parece prática ou didática, de forma que sua redução ou transformação em outros artigos contribuiria para tornar a instrução mais clara.

No caso do Art. 35-B ele se limita a apresentar duas definições. Dentro da lógica normativa da Instrução CVM 505, definições são apresentadas em seu Art. 1°. Portanto, a realocação dos termos para o Art. 1° nos parece mais acertada.

Tendo em vista que os dois termos do artigo Art. 35-B serem complementares é essencial que eles sejam apresentados em sequência. Os sistemas críticos englobam a definição de processos críticos de forma que o primeiro consiste nos sistemas que executam funções essenciais ao funcionamento do sistema de ordens. Enquanto que o segundo explica quais seriam essas funções essenciais.

6.	Art. 3°, § 4º, II – Alteração Assunto: Intermediário
Texto da Minuta	**Texto Proposto**
Art. 3º O intermediário deve adotar e implementar: (...) § 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: ~~II – supervisionar o cumprimento e efetividade dos procedimentos e controles internos de que trata o caput.”~~	Art. 3º O intermediário deve adotar e implementar: (...) § 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: **II – REVOGADO**
Justificativa: Atribuir competência aos órgãos colegiados da administração, no sentido de supervisionar o cumprimento das regras implica em procedimentos demasiados. Uma vez que a própria norma atribui responsabilidades individualizadas aos diretores, diferente por exemplo da aprovação das regras e procedimentos, tendo em vista que essas, sim, trazem diretrizes essenciais para as empresas e por isso e devem ser aprovadas pelos órgãos colegiados.	

7.	Art. 4°, § 5º – Alteração Assunto: Intermediário
Texto da Minuta	**Texto Proposto**
Art. 4º O intermediário deve indicar: § 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:	Art. 4º O intermediário deve indicar: § 5º O diretor **estatutário** 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:
Justificativa: Ao utilizar a atribuição da responsabilidade indicada no §5º do art. 4º ao diretor de controles internos, isso poderá gerar potencial conflito com o disposto no art. 4º, inciso I e II. Isso porque, o intermediário tem a faculdade de atribuir ao diretor de controles internos as responsabilidades indicadas no inciso I, deixando atribuição indicada no inciso II, cujo §5º faz referência, ao diretor de risco/*compliance.*	

8.	Art. 4°, V – Alteração Assunto: Incidentes de segurança
Texto da Minuta	**Texto Proposto**
Art. 4º O intermediário deve indicar: V – avaliação de riscos para o intermediário em relação aos seus controles internos e quanto à sua vulnerabilidade a ~~ataques cibernéticos~~; e	Art. 4º O intermediário deve indicar: V – avaliação de riscos para o intermediário em relação aos seus controles internos e quanto à sua vulnerabilidade a **incidentes relevantes e a outros incidentes que possam comprometer a segurança dos dados sob sua responsabilidade**;
Justificativa: O termo "ataque cibernético", apesar de ser usado popularmente, não é o mesmo termo adotado pela LGPD e é bastante amplo. Conforme nossos comentários nos itens 1 e 2, sugerimos a diferenciação de duas categorias de incidentes, os "incidentes relevantes de segurança e uso indevido de dados" e os "incidentes relevantes de interrupção". Como neste caso mencionamos ambos, optamos pela utilização de "incidentes relevantes" conforme sugestão de termo definido no Art. 1°, XVI. No mesmo sentido, acreditamos que o termo "ataque cibernético" deve ser substituído conforme fizemos aqui nos seguintes artigos: 4°, §5°, V; 35-H, II; 35-H, III, b; 35-H, V; 35-H, VI; e 35-H, VII.	

9.	Art. 31, III – Alteração Assunto: Controle de conflitos de interesse
Texto da Minuta	**Texto Proposto**
Art. 31. O intermediário deve estabelecer regras, procedimentos e controles internos que sejam aptos a prevenir que os interesses dos clientes sejam prejudicados em decorrência de conflitos de interesses. 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~~.”	Art. 31. O intermediário deve estabelecer regras, procedimentos e controles internos que sejam aptos a prevenir que os interesses dos clientes sejam prejudicados em decorrência de conflitos de interesses. 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, **quando possível, antes de efetuar uma operação.**
Justificativa: O mecanismo de inserção das ordens é dinâmico de modo que, na prática, os procedimentos prévios de controle para detecção e avisos não conseguem indicar os potenciais conflitos de interesses existentes. Dessa forma, muito embora seja interessante propor o estabelecimento de mecanismos preventivos para esta finalidade a norma deve traze-lo como uma possibilidade e não como uma obrigação, tendo em vista que na prática pode não haver tempo hábil para a identificação do conflito de interesse antes de efetuada a operação, ao exemplo das operações realizadas em mercado secundário.	

10.	Art. 35-C, I, II e III – Alteração Assunto: Incidente de segurança
Texto da Minuta	**Texto Proposto**
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: 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.~~ 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)	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: I – as diretrizes para a avaliação da relevância **de incidentes relevantes, conforme definido pelo artigo 1°, inciso XVI desta norma**; 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. 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)

Justificativa:

O art. 35-C (assim como vários outros artigos) utilizou-se o termo "incidente relevante" sem estabelecer o seu significado exato conforme apontamos nos itens 1 e 2. Assim, criamos a definição de "incidente relevante" no artigo 1°, inciso XVI. Dessa forma, utilizamos "incidente relevante" como sendo os "incidentes relevantes de segurança e uso indevido de dados" e os "incidentes relevantes de interrupção", ambos também definidos no artigo 1°.

É importante notar que isso implicaria em estabelecer que o SMI receberia a comunicação de ambos os tipos de incidentes tornando esta fiscalização mais compreensiva.

11.	Art. 35-E, caput – Alteração Assunto: Dados pessoais
Texto da Minuta	**Texto Proposto**
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:	Art. 35-E. O intermediário deve desenvolver e implementar suas políticas e práticas visando garantir a confidencialidade, a autenticidade, a integridade, a disponibilidade e a proteção dos **dados pessoais e não pessoais e informações pessoais e não pessoais**, contemplando:
Justificativa: Além das garantias já oferecidas na Minuta, optamos pela inclusão da proteção dos dados pessoais e não pessoais. Essa garantia busca alinhar as expectativas dos titulares dos dados com os ditames LGPD. Dessa forma, atrelar os dispositivos da presente instrução normativa com a LGPD busca conferir maior segurança jurídica sobre o assunto.	

12.	Art. 35-E, I e II – Alteração Assunto: Dados pessoais e incidente de segurança
Texto da Minuta	**Texto Proposto**
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	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, **pessoais ou não**, 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 relevantes**;

Justificativa:

Acreditamos que incluir "dados pessoais ou não" na redação do inciso I do Art. 35-E confere maior proteção para os titulares dos dados pois especifica melhor o escopo de informações em questão.

As propostas de inclusão nos incisos I e II estão ligadas ao que discutimos nos itens 1 e 2 visando trazer maior clareza ao termo "incidentes relevantes", que definimos no artigo 1°, inciso XVI. Esta alteração acaba consequentemente solucionando a ambiguidade do uso de "incidentes relevantes" no inciso III deste artigo também.

13.	Art. 35-F, I – Alteração Assunto: Incidente de segurança
Texto da Minuta	**Texto Proposto**
Art. 35-F. As regras, procedimentos e controles internos relacionados aos dados e informações sensíveis devem contemplar: I – proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso não autorizado, vazamento, adulteração e destruição;	Art. 35-F. As regras, procedimentos e controles internos relacionados aos dados e informações sensíveis devem contemplar: I – proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso não autorizado, vazamento, adulteração, destruição e **vedação de utilização para propósitos além daqueles para os quais os dados foram disponibilizados;**
Justificativa: A inclusão proposta coaduna-se com o princípio da limitação de propósitos da utilização de dados nos termos do art. 6º, I, da Lei 13.709/2018. A ideia é que os dados podem ser utilizados somente para os propósitos que foram disponibilizados para uso.	

14.	Art. 35-G, I, c – Alteração Assunto: Incidente de segurança
Texto da Minuta	**Texto Proposto**
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; I – práticas adotadas pelo intermediário quanto: (...) c) a comunicações ao cliente em caso de ~~incidentes de segurança~~ envolvendo informações de cadastro e de operações realizadas que possam acarretar risco ou dano relevante ao cliente; e	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; I – práticas adotadas pelo intermediário quanto: (...) c) a comunicações ao cliente em caso de **incidentes relevantes de segurança e uso indevido de dados** envolvendo informações de cadastro e de operações realizadas que possam acarretar risco ou dano relevante ao cliente; e

Justificativa:

O tipo de incidente que o artigo 35-G trata é aquele que nós sugerimos classificar como incidentes relevantes de segurança e uso indevido de dados, conforme explicamos mais detalhadamente no item 1.

Para trazer maior coesão e clareza para a norma sugerimos especificar o tipo de incidente de segurança, conforme fizemos. Isso ajuda a não haver confusão com o incidente relevante de interrupção, que não caberia aqui.

15.	Art. 35-H – Alteração Assunto: Incidente de segurança
Texto da Minuta	**Texto Proposto**
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: (...) 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: (...) 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~~;	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: (...) II – as medidas que devem ser adotadas para reduzir a vulnerabilidade da instituição contra **incidentes relevantes de segurança e uso indevido de dados.** III – procedimentos e controles internos que serão adotados para: (...) b) efetuar o monitoramento contínuo e a detecção de **incidentes relevantes de segurança e uso indevido de dados**; IV – plano de resposta para tratamento de **incidentes relevantes de segurança e uso indevido de dados** 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 **incidentes relevantes de segurança e uso indevido de dados**; VI – plano de treinamento periódico de seus funcionários e prepostos, de forma a

15.	Art. 35-H – Alteração Assunto: Incidente de segurança
VII – realização de testes periódicos para avaliar a vulnerabilidade da instituição contra ~~ataques cibernéticos~~; e VIII – formas de participação em iniciativas que objetivem o compartilhamento de informações sobre ~~incidentes relevantes~~.	prevenir e proteger os sistemas contra **incidentes que possam comprometer a segurança dos dados sob sua responsabilidade como os incidentes relevantes de segurança e uso indevido de dados**; VII – realização de testes periódicos para avaliar a vulnerabilidade da instituição contra **incidentes relevantes**; e VIII – formas de participação em iniciativas que objetivem o compartilhamento de informações sobre **incidentes relevantes**.
Justificativa: Nossa proposta aqui é continuar a padronização de termos que estamos sugerindo nos itens anteriores conforme termos definidos dos itens 1 e 2.	

16.	Art. 35-I – Alteração Assunto: Incidente de segurança

Texto da Minuta	Texto Proposto
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: (...) 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.	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 da informação e uso inadequado de dados** relevantes. § 2º No prazo de 45 (quarenta e cinco) dias o intermediário deve encaminhar relatório à SMI, contendo, no mínimo: (...) IV – os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de **incidentes de segurança da informação e uso inadequado de dados**, com o estabelecimento de cronograma de implementação, se for o caso.

Justificativa:

Nossa proposta aqui é continuar a padronização de termos que estamos sugerindo nos itens anteriores conforme termos definidos dos itens 1 e 2.

17.	Art. 35-J, III – Alteração Assunto: Uso adequado dos dados
Texto da Minuta	**Texto Proposto**
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: (...) III – a confidencialidade, integridade, disponibilidade, ~~a e~~ a recuperação dos dados e informações processados ou armazenados pelo prestador de serviços. (...)	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: (...) III – a confidencialidade, integridade, disponibilidade, a recuperação **e o uso adequado** dos dados e informações processados ou armazenados pelo prestador de serviços, **conforme estipula o artigo 46 da Lei nº 13.709, de 14 de agosto de 2018**. (...)
Justificativa: Incluir no texto proteção quanto ao uso dos dados de maneira adequada tutelando os direitos dos titulares dos dados conforme estipula o artigo 46 da LGPD.	

18.	Art. 36 – Alteração Assunto: Prazo para manutenção de documentos e informações
Texto da Minuta	**Texto Proposto**
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.	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. **I – O prazo máximo para manutenção dos documentos e informações que o *caput* deste artigo menciona dependerá da permanência da utilidade destes documentos e informações. Quando estes não forem mais úteis para a finalidade ao qual foram fornecidos deverão seguir o disposto nos artigos 15 e 16 da Lei nº 13.709, de 14 de agosto de 2018.**
Justificativa: A norma determina um prazo mínimo contudo deve ser estipulado um prazo máximo também uma vez que os dados não podem ficar disponíveis para sempre com o intermediário, apenas enquanto foram úteis para a função ao qual eles foram fornecidos conforme estipulam os artigos 15 e 16 da LGPD.	