



AUDIÊNCIA PÚBLICA ANBIMA: FIDCS/FICS, CYBER E REGISTRO DE ATIVOS

Associação colocou novas regras em Audiência Pública, no dia 10.06.22.

INTRODUÇÃO

A exemplo do que já havia feito antes com os Fundos de Renda Fixa e de Ações, a ANBIMA, nesta Audiência Pública (“AP”), estende seu foco de ESG para os FIDCs e FICs, determinando regras e requisitos para o seu reconhecimento como veículos sustentáveis.

Vale lembrar que os fundos (geridos por aqueles associados ou aderentes à ANBIMA) que não tenham o compromisso ESG como objetivo/tese de investimento não podem usar a sigla “IS” em sua denominação, mas, mesmo assim, contam com diferenciações em seus materiais de venda perante os investidores.

A AP traz ainda novas regras pertinentes à segurança cibernética, prescrevendo a obrigação da implementação e manutenção de documento escrito, de regras e de procedimentos para preservação das informações pessoais de clientes a que as instituições tiverem acesso, sobretudo no que diz respeito à confidencialidade e gerenciamento desses dados.

Por último, estão também na AP regras para registro de operações com CRIs, CRAs, debêntures e cotas de fundos fechados no Sistema REUNE da ANBIMA (plataforma de pré-registro de negociação no mercado secundário, exigência esta válida para operações cursadas em bolsa ou em ambientes administrados por entidades de mercado organizado).

A audiência pública tem prazo limite para envio de informações no dia 13 de julho, sugestões podem ser encaminhadas no e-mail audiencia.publica@anbima.com.br.

Destacaremos a seguir, alguns aspectos das novas normas em AP.

FIDCS/FICS SUSTENTÁVEIS

No universo da ANBIMA (no caso, as “Regras e Procedimentos para Identificação de Fundos de Investimento Sustentável - IS”), existe uma gradação entre fundos 100% sustentáveis (os quais devem usar a sigla “IS” em sua



denominação) e fundos que “apenas consideram” questões ESG em sua gestão.

Os gestores dos primeiros devem obedecer a uma série de requisitos, como por exemplo:

(i) contar com documento escrito que descreva as diretrizes, procedimentos, critérios e controles adotados pela instituição referentes ao seu compromisso ESG;

(ii) contar com uma estrutura funcional e de tomada de decisões interna adequada para o cumprimento das responsabilidades relacionadas à gestão dos fundos de investimento sustentável, com atribuição clara das respectivas responsabilidades, linhas de reporte e independência no desempenho das funções;

(iii) demonstrar o alinhamento da carteira com os objetivos de investimento sustentável; e

(iv) divulgar em seu site na internet, de forma clara, objetiva e transparente, o documento de que trata o item “i” acima, com o objetivo de dar transparência aos investidores de quais diretrizes e procedimentos de sustentabilidade são adotados pela instituição.

Já os gestores de fundos que apenas integram questões ESG às suas estratégias devem informar na documentação dos fundos as linhas gerais da metodologia respectivamente adotada para tanto, além de:

(a) adotar metodologia de integração de questões ESG incluindo, no mínimo, os critérios de seleção de investimentos e a alocação de ativos de acordo com uma avaliação das características ESG dos ativos;

(b) identificar as limitações da metodologia de integração de questões ESG utilizada e ações de diligência e monitoramento a respeito de seus efeitos;

(c) utilizar informações, métricas e/ou indicadores materiais que permitam identificar as características ASG dos ativos; e

(d) divulgar publicamente em seu site, mantendo atualizada, e em linha com as melhores práticas internacionais de relato e expectativas do mercado, a forma como integra sistematicamente as questões ESG na sua gestão de ativos.

Assim, o que de fato se sobressai na leitura das regras da ANBIMA sobre o tema é (1) uma clara preocupação em distinguir os veículos alinhados com o tema ESG (ou com a sua integração à gestão e estratégias dos fundos) daqueles que não assim procedem, e (2) assegurar o devido cumprimento dos compromissos de quem se pretende inserido no universo ESG – sobretudo perante o público investidor –, por meio de obrigações de transparência, divulgação, acompanhamento e monitoramento.

No caso dos FIDCs e FICs, em linhas gerais, as obrigações se equivalem àquelas já aplicáveis aos Fundos Sustentáveis de Ações e de Renda Fixa, apenas levando em conta as devidas peculiaridades pertinentes a cada modalidade.

Assim, relativamente aos FIDCs que adotarem compromissos ESG (“FIDCs IS”), além das obrigações comuns a todos os fundos que assim atuam,¹ deverá haver a demonstração de que a carteira está alinhada com o respectivo objetivo, “considerando, de forma justificada, o cedente e/ou sacado, conforme o caso, e com a garantia de que a contraparte da operação (cedente e/ou o sacado, conforme aplicável) não gerará danos ao objetivo ASG” (cf. art. 10, II, letra “b” da norma em AP).

Não fica claro na minuta como se daria exatamente essa “garantia” de que *não haverá danos* ao compromisso ESG do gestor, e nem mesmo se deveriam ser os próprios cedentes/sacados a assegurar isso, cabendo aqui, a nosso ver, um maior esclarecimento por parte da ANBIMA a esse respeito.

Novamente no caso dos FIDCs IS, a minuta diz que caberá aos gestores demonstrar quais estratégias de desinvestimento ou recomposição da carteira

¹ Ou seja, documento escrito, estrutura interna adequada, transparência, monitoramento etc.



que o fundo poderá adotar com vistas a evitar e/ou remediar situações de desalinhamento entre o objetivo ESG do fundo e os ativos em carteira, e questões relacionadas à liquidez dos ativos que impeça a recomposição imediata da carteira do fundo (v. art. 10, III, letra “b”).

Não é dito em quais circunstâncias ou em que documento deveria o gestor fazer essa demonstração, com o agravante de que a parte final poderia induzir a uma interpretação errônea, condicionando a obrigação em questão mais a cenários afetos a risco e liquidez: o gestor, por exemplo, poderia se ver numa situação de necessidade de vender um ativo se descobrisse que o cedente/sacado desmatou área protegida ou utiliza trabalho escravo – ou seja, contextos que nada teriam a ver com situações de mercado propriamente ditas; nesse caso, o fundo poderia experimentar problemas, seja para cumprir com a sua obrigação ESG, seja para tirar da carteira um ativo com pouco – ou à vezes *nenhum* – mercado secundário (aliás, tais situações, para os FIDCs IS, inclusive já deveriam estar endereçadas *a priori* em seu material publicitário, por força do art. 10, IV, letra “b”).

Relativamente aos gestores dos FIDCs que apenas integram questões ESG em suas estratégias/gestão – sem assumir um compromisso ESG de fato –, a minuta diz que eles devem “elaborar material, contendo as questões ESG adotadas na análise dos investimentos, explicitando se a integração dos aspectos ESG se dá, de forma justificada, a partir do cedente e/ou sacado, conforme o caso” (art. 13, I, letra “b”).

Novamente, o comando é um tanto vago a respeito do “material” em que deve constar essa obrigação: não fica claro se seria no regulamento, numa política própria, em material publicitário, num outro documento específico, ou mesmo em todos os anteriores. Assim, entendemos que aqui também seria cabível um maior detalhamento, a fim de possibilitar ao gestor a efetiva certeza de estar cumprindo adequadamente a norma da ANBIMA.

Relativamente aos FICs, também existe a

distinção entre FICs que investem em Fundos IS e FICs que investem em outros veículos que apenas integram questões ESG em sua gestão/estratégias.

Entretanto, a norma em AP fala explicitamente em FICs que investem *exclusivamente* (i) em Fundos IS ou (ii) em fundos que integram questões ESG (sendo que, na definição da ICVM 555, já poderia ser considerado FIC um veículo que tivesse 95% de seu patrimônio investido em cotas de outros fundos).

Assim, será considerado um FIC IS **apenas** o fundo com 100% de seu patrimônio alocado em Fundos IS, podendo, nessa hipótese (e somente nela), utilizar a abreviação “IS” em sua denominação, identificando-se assim como “fundo de investimento sustentável” – no caso dos FICs que investirem em fundos que *apenas integram* questões ESG em sua gestão, estes poderão evidenciar essa condição em seu material publicitário também apenas no caso de investimento da totalidade de seu patrimônio em fundos desse tipo.

Igualmente no caso dos FICs, o respectivo gestor deverá preparar um documento escrito contendo no mínimo os seguintes fatores:

(a) os procedimentos prévios que serão adotados para verificar se o gestor e o fundo investido cumprem com o disposto nas regras aplicáveis da ANBIMA;

(b) os procedimentos que serão adotados para monitorar os gestores e o fundo investido de modo a garantir o cumprimento contínuo de tais regras (isto é, o gestor do FIC deve ter um papel “fiscalizador” ativo nesse sentido);

(c) a periodicidade do monitoramento de que trata o item anterior, assim como o prazo para nova diligência nos termos do item “a” acima; e

(d) caso seja identificado no curso do monitoramento, ou em nova diligência, que os gestores dos fundos investidos não estejam cumprindo com o disposto nas regras aplicáveis da ANBIMA, o plano de ação a ser adotado.

Novamente lembramos que o racional dessas



normas parece ter sido de fato a tentativa de delimitar, de forma bastante rígida, o universo dos Fundos ESG (ou meramente “integradores de ESG”) dos demais fundos existentes no mercado: independente de se tratar de Fundos 555 ou FIDCs, a Associação foi na direção de obrigações e compromissos – sobretudo de transparência e de monitoramento – no caso dos veículos identificados com essa temática, a ponto inclusive de proibir o uso de expressões potencialmente “indutoras de erros” na sua devida caracterização (v. art. 2.º, § 1.º): dito de outro modo, para os associados e aderentes à ANBIMA, *apenas estes veículos, seguidores dessas regras*, é que poderão, daqui em diante, se identificar perante o público como tais.

É (muito) importante lembrar neste ponto que as questões ESG não se resumem apenas a aspectos “verdes”, “ambientais” etc., mas, englobando também aspectos de *governança corporativa*, podem ter impacto bastante relevante nas práticas sobretudo dos gestores de *equity* atualmente:² gestores com perfil mais ativo (ou ativista) em suas alocações poderiam ser afetados pelas novas normas, devendo, portanto, estudar bem o novo texto da ANBIMA.

Portanto, os fundos que atualmente se identificam como “fundos verdes”, “fundos sociais”, “fundos de impacto”, “fundos ASG”, “fundos ESG”, ou quaisquer outros termos similares, terão até **04.07.22**, para se adaptarem (a norma seria válida *imediatamente* para aqueles que já se caracterizam como Fundos IS e fundos que integram questões ESG em sua gestão/estratégias).

Para Fundos 555 de Ações, atualmente classificados na ANBIMA como “de sustentabilidade/governança”, e para os FICs que investirem em Fundos IS e fundos que integram questões ESG, o prazo é **03.01.23**. E, por fim, para os FIDCs, o prazo é de 180 dias contados da

vigência da nova regra.

Já como último aspecto a destacar neste tema, a redação proposta na AP para o art. 15, “considerando-se que a integração de questões ASG nos processos de tomada de decisão do gestor é um indicativo de boa prática de gestão de ativos”, recomenda que “*todos os gestores* busquem, gradualmente, incorporar os recursos e práticas necessários para que possam integrar questões ASG de forma *sistemática e processual*, sem prejuízo da divulgação de boas práticas por meio do guia ASG ANBIMA” (grifos nossos).

Não saberíamos dizer se isso conota um desejo ou plano futuro da Associação, mas certamente não nos parece apropriada nem adequada uma previsão dessa natureza em texto normativo (e, portanto, como tal, necessariamente *prescritivo e obrigatório*).

SEGURANÇA CIBERNÉTICA

A ANBIMA também colocou em AP novas regras de segurança cibernética (a serem inseridas no “Código de Administração de Recursos de Terceiros” – “Código”).

A AP, nesse tema, traz novas regras pertinentes à obrigação de implementação e manutenção de um documento escrito contendo regras e procedimentos para preservação das informações pessoais de clientes a que as instituições tiverem acesso, sobretudo no que diz respeito à confidencialidade e gerenciamento desses dados (as instituições deverão inclusive elaborar planos de continuidade de negócios e regras para o tratamento de incidentes e de questões de governança a esse respeito).

Segundo a nova redação proposta para o art. 13 do Código, o referido documento deverá conter no mínimo:³

² A norma em AP acertadamente considera também temas de governança corporativa na definição de “questões ASG” (cf. item XXII – e também VIII e XVIII – do Glossário).

³ Esse racional está em sintonia com as determinações da Lei n.º 13.709/18 (LGPD), e, no caso dos gestores, é particularmente relevante na prestação do serviço de



(a) como se dá o controle de privacidade e dados pessoais a que a instituição tem acesso, identificando, no mínimo, controlador, processador, bases legais, finalidade, duração de tratamento, compartilhamento e responsabilidades;

(b) critérios adotados para a proteção da confidencialidade dos ativos de informação e dos dados pessoais tratados durante todo o seu ciclo de vida, conforme classificação da informação, abordando desde a sua geração até o seu descarte, incluindo armazenamento, acesso, criptografia, tratamento, transmissão e transporte;

(c) regras aplicáveis aos colaboradores para o gerenciamento de identidade e acesso aos ativos de informação e dados pessoais a que tenham acesso, desde o início até o término do relacionamento do colaborador com a instituição, inclusive nos casos de mudança de atividade dentro da mesma instituição, de forma a garantir o adequado tratamento dos dados; e

(d) prazo para atualização do documento de que aqui se trata, que não deve ser superior a 24 meses, ou sempre que necessário, se a regulamentação exigir.

A AP introduz também algumas mudanças no Plano de Continuidade de Negócios já aplicável atualmente: a nova redação proposta para o art. 14, inciso I, prevê o estabelecimento de “formas alternativas para processamento em situações de contingência, assegurando a continuidade das atividades em tempo hábil para cumprimento de suas responsabilidades”.

Não está claro exatamente “processamento” de quê se trataria aqui, mas o contexto em princípio permitiria a interpretação de serem em verdade as ordens emitidas pelo gestor (embora, a rigor, não lhe caiba propriamente um “processamento” do que quer que seja a esse respeito enquanto tal). Assim, o que a nova redação parece pretender nesse ponto seria apenas a

enumeração das alternativas ao alcance do gestor na hipótese de eventual(is) contingência(s), de modo a permitir uma ciência prévia acerca da sua capacidade de manter funcionais as suas atividades nessas situações ou não – não fica claro, nesse contexto, se a ANBIMA entrará no mérito das alternativas listadas pelo gestor.

Além disso, no item II do mesmo artigo, a Associação deseja agora a enumeração dos riscos potenciais a que a instituição julga estar exposta, com a indicação da respectiva medida de contingência a ser adotada – ou seja, o gestor deve agora listar *a priori* todas as situações de mitigação dos riscos a que entender ter exposição no desempenho de suas atividades.

Apontamos também que a minuta retirou a necessidade de validação e de testes anuais do PCN.

No que diz respeito à Segurança da Informação e Cibersegurança propriamente ditas, houve mudanças importantes também.

A política respectiva agora deverá indicar os procedimentos adotados para controle de informações consideradas pela instituição como confidenciais, reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, colaboradores e também terceiros contratados; além disso, deverá igualmente avaliar os riscos pertinentes, identificando os ativos considerados relevantes pela instituição, sejam eles equipamentos, sistemas, dados ou processos e suas vulnerabilidades, considerando a identificação de probabilidades e impactos de possíveis ameaças cibernéticas e possíveis cenários de ameaças – ou seja, essa (nova) circunstância deve ser devidamente avaliada na formulação da respectiva política nesse ponto.

Outro aspecto interessante é que não é mais obrigatória a criação de um plano de resposta a incidentes, nem a designação específica de um responsável na instituição para respostas a



questões de segurança cibernética.

A AP também prevê que as instituições exijam que seus colaboradores e/ou terceiros contratados assinem, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes venham a ser confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei, exceção feita apenas a contratos de prestação de serviços em que constar a cláusula respectiva.

Outro aspecto a merecer atenção – especialmente no contexto pós-pandemia – é o dever de assegurar a contratação de serviços de armazenamento e processamento de dados e computação em nuvem (no país ou no exterior), no relacionamento com terceiros, quando se tratar de fatores considerados críticos ou de maior risco, conforme o critério da instituição: desta forma, qualquer contratação que tenha por objeto um aspecto relevante ao desempenho normal de suas atividades deverá conter essa cláusula, cabendo ao gestor assegurar que ela conste devidamente dos serviços do terceiro contratado.

Nesse aspecto, caberá também ao gestor contratante o dever de verificar uma série de condições quanto à capacidade do potencial prestador de serviço, no mínimo quanto ao seguinte:

- (1) o seu cumprimento da regulamentação em vigor;
- (2) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- (3) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- (4) a aderência do prestador de serviço a certificações exigidas pela instituição para a prestação do serviço a ser contratado, caso aplicável;

(5) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

(6) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

(7) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

No que diz respeito a incidentes cibernéticos, a instituição deverá estabelecer um plano de ação e resposta, visando à implementação das regras, procedimentos e controles internos de privacidade, proteção de dados pessoais, segurança da informação, segurança cibernética e contingência, que conterà, no mínimo:

(a) as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes das regras, procedimentos e controles internos de privacidade, proteção de dados pessoais, segurança da informação, segurança cibernética e contingência;

(b) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes indicadas acima;

(c) a área responsável pelo registro e controle dos efeitos de incidentes considerados relevantes pela instituição; e

(d) alçada de reporte dos incidentes identificados.

Além desses fatores, o plano deverá conter pelo menos o procedimento de comunicação com órgãos reguladores e titulares dos dados comprometidos pelo incidente, incluindo cenários, processo de decisão de comunicação e prazo para efetivação da comunicação.

Para monitorar e acompanhar tudo isso, as instituições deverão instituir mecanismos que visem a assegurar a implementação e a efetividade das regras, procedimentos e controles internos pertinentes, definindo as áreas e/ou profissionais responsáveis por assegurar o



cumprimento das respectivas obrigações, e os processos e controles adotados no seu acompanhamento incluindo, sem limitação, a trilha de auditoria. Além disso, deverá também haver a definição de metodologias, métricas, critérios e indicadores utilizados, e o mapeamento dos cenários de estresse, incidentes e risco e formas de tratamento, bem como a realização de testes com plano de ação para tratamento e correção de eventuais deficiências encontradas. Não está especificado exatamente na norma *onde* devem constar todas essas medidas, mas cremos ser recomendável reduzi-las a termo escrito ao menos na respectiva política. Destacamos aqui que tudo isso deverá ser objeto de mecanismo e testes de validação no mínimo anuais (ou em prazo inferior se assim exigido pela regulamentação em vigor).⁴

Por último, a AP apresenta também um “programa de conscientização” sobre práticas gerais de proteção de informações confidenciais, reservadas ou privilegiadas e dados pessoais, segurança da informação e cibersegurança, e sobre os protocolos de continuidade de negócios e prevenção de incidentes, de forma que, no mínimo anualmente (ou em prazo inferior se assim exigido pela regulamentação aplicável), as instituições deverão realizar a revisão das políticas, documentos, conteúdo do programa de conscientização e planos de continuidade de negócios.

REGISTRO DE OPERAÇÕES

Finalizando este *paper*, a ANBIMA também colocou em AP as regras para registro de certos ativos por parte dos gestores: os CRIs, CRAs, debêntures e cotas de fundos fechados, se negociados em bolsa ou em ambientes administrados por entidades de mercado organizado, passariam a ser registrados no REUNE (sistema da ANBIMA de pré-registro de

negociação no mercado secundário).

Assim, o gestor de recursos terá o prazo máximo de 1 (uma) hora, contado da realização da operação, para registrar as informações no sistema, considerado como horário da realização da operação, para fins da norma, o momento em que houve o fechamento da operação entre as partes (a comprovação da realização da operação seria feita pela emissão da boleta – seja esta eletrônica ou manual –, devendo qualquer uma delas conter evidências de data e hora de sua emissão). Se ambas as partes na operação forem gestores de recursos sujeito ao Código, os dois terão que realizar o registro.

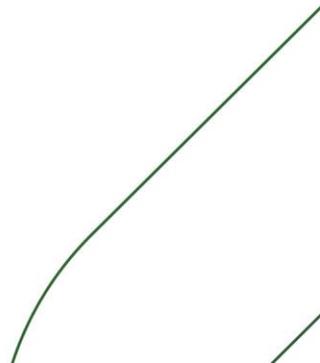
As informações das operações a serem registradas são as seguintes:

- (I) preço ou referência de preço (taxa);
- (II) quantidade ou volume financeiro aproximado;
- (III) horário da execução;
- (IV) identificação da contraparte;
- (V) identificação do tipo da operação (compra ou venda); e
- (VI) identificação do ativo negociado

O gestor de recursos deverá observar, se aplicável, os critérios de cálculo estabelecidos pela ANBIMA por meio da metodologia de precificação disponível no site da Associação na internet. Caso opte, nas situações que for possível, por não utilizar os critérios de cálculo da referida metodologia, o gestor deverá explicitar esta condição para as partes previamente à negociação e deixar o motivo justificado e à disposição da ANBIMA.

A AP possibilita também que o gestor possa autorizar prestadores de serviços e/ou bolsa de valores e/ou entidades administradoras de mercados organizados para enviar ao REUNE, em seu nome, as operações realizadas com os ativos mencionados neste item.

⁴ Assim, o PCN não demanda mais os respectivos testes, mas a Política de Cibersegurança sim.



BONS NEGÓCIOS

José Brazuna

Raphael Castro

Patrícia Lima

