Perguntas e Respostas

Autorregulação de custódia de ativos virtuais

Agosto de 2026

Documento orientativo para instituições participantes
Base normativa: regime experimental Anbima e Resolução BC 520/25

ANBIMA

Sumário

Introdução

Este FAQ foi elaborado como material de apoio às Instituições Participantes da Anbima que desempenham atividades relacionadas a Ativos Virtuais, especialmente no que diz respeito à custódia de ativos virtuais. O objetivo é esclarecer, por meio de perguntas e respostas organizadas por categorias, os principais pontos do Regime Experimental de Autorregulação Anbima.

O regime experimental da Anbima se alinha à implementação do novo arcabouço regulatório editado pelo Banco Central, cujas regras passam a valer plenamente a partir de 30 de outubro de 2026, data a partir da qual fica vedada a realização de operações com entidades não autorizadas (art. 91 da Resolução BCB nº 520/25). Considerando seu caráter experimental, as disposições não ensejarão, neste momento, aplicação de taxas, supervisão e/ou quaisquer penalidades por parte da Anbima. A atuação terá como foco o acompanhamento educativo e a promoção de boas práticas.

Nota metodológica: as respostas empregam, por vezes, vocabulário cogente ("deve", "exige"), que reflete as melhores práticas recomendadas pelo Regime Experimental e o conteúdo esperado do futuro código vinculante. Nesta fase, tais formulações não constituem obrigações exigíveis pela Anbima nem se confundem com os requisitos da regulação do Banco Central, cuja origem, quando pertinente, é indicada pela referência expressa à Resolução BCB nº 520/25 e às Instruções Normativas aplicáveis.

Dúvidas e orientações podem ser enviadas para: ativos.virtuais@anbima.com.br ou autorregulacao.representacao@anbima.com.br.

1. Regime Experimental: Natureza, Abrangência, Obrigatoriedade e Monitoramento

P1: O que é o Regime Experimental de Autorregulação da ANBIMA para custódia de ativos virtuais e quais são seus objetivos formais?

R: É um conjunto de princípios, parâmetros de conduta e melhores práticas que visa promover padrões éticos elevados, transparência, segurança e rastreabilidade nas atividades de custódia de ativos virtuais, excedendo os limites da simples observância regulatória. O regime experimental permite que o mercado e as instituições adaptem gradualmente suas práticas às especificidades dos ativos virtuais, estabelecendo um framework robusto de governança e controles antes da consolidação regulatória definitiva. O Regime Experimental elenca oito objetivos formais: (I) promover padrões éticos elevados e melhores práticas nas atividades de custódia de ativos virtuais; (II) fomentar a transparência e a rastreabilidade das operações; (III) estabelecer princípios de conduta aplicáveis às Instituições Participantes; (IV) orientar a implementação de controles internos e de governança adequados; (V) estimular a adoção de padrões de segurança da informação e de proteção de dados; (VI) contribuir para a convergência de práticas de mercado antes da consolidação regulatória plena; (VII) facilitar a transição das instituições para o regime regulatório definitivo do Banco Central; e (VIII) servir de base para a futura elaboração de código vinculante. Esses objetivos refletem a natureza dupla do Regime: instrumento educativo imediato e plataforma de desenvolvimento normativo futuro.

P2: O regime experimental é obrigatório?

R: Não. Nesta fase, o Regime Experimental possui natureza orientativa e educativa, não gera adesão obrigatória, cobrança de taxas, supervisão sancionadora ou penalidades. No futuro, o material deve subsidiar a consolidação de regras vinculantes (Código).

P3: Se o Regime não tem supervisão nem penalidades, qual o sentido de aderir?

R: A participação permite testar práticas, identificar dificuldades de implementação, trocar experiências com o mercado e antecipar a organização de políticas, contratos e controles. O regime também cria um canal estruturado de aprendizado para aperfeiçoamento do material. Adicionalmente, garante voz no fórum de revisão, influenciando o desenho da versão vinculante futura (Código).

P4: Se o Regime não recebe informação dos aderentes, como a ANBIMA acompanhará a aplicação?

R: A ANBIMA pretende acompanhar o regime por meio de reuniões temáticas, consultas voluntárias, eventos, recebimento de dúvidas e coleta qualitativa de aprendizados. Não haverá reporte obrigatório enquanto não houver deliberação específica nesse sentido. Eventuais

informações compartilhadas deverão observar confidencialidade, proteção de dados e finalidade previamente informada.

P5: O que a autorregulação acrescenta em relação à Resolução BCB nº 520/2025?

R: A autorregulação da ANBIMA não substitui nem se sobrepõe à Regulação (Resolução BCB nº 520), mas acrescenta um conjunto de melhores práticas operacionais, de governança e de segurança, com maior detalhamento e padronização setorial. Enquanto a Regulação estabelece os requisitos regulatórios mínimos obrigatórios, a autorregulação define como implementar esses requisitos na prática, incluindo: (i) maior detalhamento sobre gestão de chaves, conciliação e controles operacionais; (ii) padronização de contratos, políticas e processos; (iii) diretrizes de governança, transparência e comunicação com clientes; (iv) incentivo à convergência de práticas antes da supervisão regulatória plena. Além disso, a autorregulação antecipa a preparação do mercado para a entrada em vigor plena das normas do Banco Central (30 de outubro de 2026, nos termos do art. 91 da Resolução BCB nº 520/25), atuando como instrumento de transição do modelo regulatório para o modelo de implementação prática. Esse detalhamento será complementado por guias operacionais e materiais de apoio a serem produzidos no âmbito da autorregulação, aos quais este FAQ fará remissão em suas versões futuras.

P6: Quais instituições estão sujeitas a este regime experimental? A extensão aos integrantes do Conglomerado implica responsabilidade solidária?

R: O regime alcança Instituições Participantes que efetivamente prestem custódia de ativos virtuais, inclusive quando a atividade estiver inserida em modalidade autorizada que acumule custódia. A extensão a integrantes do conglomerado depende da participação concreta de cada entidade na atividade. Essa extensão não cria solidariedade automática; cada entidade responde pelas atribuições que efetivamente desempenha.

P7: Sou prestador de tecnologia que oferece infraestrutura de carteira como serviço, sem deter chaves nem assumir obrigações fiduciárias. Estou sujeito ao Regime?

R: O Regime não se aplica diretamente a provedores exclusivamente tecnológicos. A caracterização depende da função efetivamente exercida: se a empresa oferece apenas infraestrutura técnica, sem decisão sobre movimentação dos ativos nem responsabilidade fiduciária, está fora do Regime. A exclusão não se aplica, porém, a arranjos que na prática resultem em terceirização integral de atividades essenciais sem a assunção das responsabilidades pela PSAV.

P8: Sou gestora de recursos com fundos que investem em ativos virtuais. O Regime se aplica?

R: O regime de custódia de ativos virtuais não se aplica à gestora apenas pelo fundo investir em ativos virtuais, salvo se ela própria prestar custódia de ativos virtuais. Contudo, administrador fiduciário e gestor permanecem sujeitos aos deveres de seleção, contratação,

monitoramento e supervisão do custodiante previstos no Código e nas Regras de AGRT, conforme suas competências.

P9: Como se relacionam o Regime Experimental e os Códigos Anbima? Um prevalece sobre o outro em caso de conflito?

R: O Regime não se sobrepõe nem contradiz os Códigos Anbima vigentes. Em caso de aparente contradição entre o Regime Experimental e disposições dos Códigos, prevalece o texto dos Códigos. O Regime Experimental opera em camada complementar: acrescenta melhores práticas e orientações operacionais específicas para custódia de ativos virtuais sem revogar, alterar ou criar exceções às normas dos Códigos Anbima. Eventuais tensões interpretativas devem ser reportadas ao GT de Ativos Virtuais para análise e, se necessário, esclarecimento pela Anbima.

2. Atividade de Custódia de Ativos Virtuais

P10: Quais são os princípios gerais de conduta que as Instituições Participantes devem observar?

R: As Instituições Participantes devem observar dois conjuntos de deveres:

I. Princípios gerais de conduta: boa-fé, diligência, lealdade e transparência; cuidado equivalente ao de uma pessoa prudente com seus próprios negócios; idoneidade moral e profissional; prevenção e administração de conflitos de interesse; vedação a práticas abusivas, discriminatórias ou de concorrência desleal; tratamento equitativo aos clientes; identificação, avaliação, monitoramento e mitigação dos riscos associados às atividades e aos ativos custodiados; e disponibilização de informações claras, precisas e adequadas sobre os serviços e seus riscos.

II. Obrigações transversais: manter controles compatíveis com a complexidade operacional; adotar padrões de segurança da informação, cibersegurança e proteção de dados pessoais; assegurar sigilo das informações dos clientes; e observar integralmente as normas de PLD/FTP (prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa).

Esses princípios e obrigações devem orientar todas as decisões e processos, servindo de base para governança, gestão de riscos, controles internos e relacionamento com clientes.

P11: O que compreende a atividade de custódia de ativos virtuais? Quem pode prestar esse serviço?

R: A custódia de ativos virtuais compreende a guarda fiduciária, o controle e a administração dos instrumentos que viabilizam o exercício dos direitos relacionados aos ativos virtuais, especialmente chaves privadas (art. 9º da Resolução BCB nº 520/25). Abrange, entre outras

atividades: (i) a guarda e o gerenciamento de chaves criptográficas; (ii) o registro e a conciliação das posições dos clientes; (iii) o atendimento de instruções de movimentação e transferência; (iv) o registro e a gestão de ônus, gravames e bloqueios; (v) o tratamento de eventos incidentes aos ativos virtuais, como forks, airdrops e staking, quando aplicável; (vi) a administração e disponibilização de informações relacionadas aos ativos custodiados; e (vii) a implementação de mecanismos de segregação patrimonial, conciliação e prova de reservas.

A PSAV Custodiante é a pessoa jurídica que tem por objeto social a prestação de serviços de custódia de ativos virtuais e que assume a responsabilidade perante clientes e autoridades pela guarda, administração, controle e proteção dos ativos custodiados, ainda que utilize prestadores tecnológicos, subcustodiantes ou outros terceiros para execução de atividades específicas.

P12: A Prova de Reservas é parte da atividade de custódia em sentido estrito?

R: Sim. O Regime Experimental elenca os mecanismos de Prova de Reservas (PoR) como componente integrante da atividade de custódia. Trata-se de melhor prática fortemente recomendada: a expectativa do Regime é que a PSAV Custodiante implemente metodologia de PoR auditável, observadas as características e limitações do mecanismo (ver P50). A Resolução BCB nº 520/25 não condiciona o exercício da custódia à adoção de PoR; sua implementação constitui diferencial de transparência promovido pela autorregulação e tende a integrar o futuro código vinculante.

P13: Qual a diferença entre custódia qualificada e prestação de serviços tecnológicos de suporte?

R: A custódia qualificada pressupõe a assunção integral de responsabilidades fiduciárias, contratuais, regulatórias e informacionais perante o cliente, incluindo a guarda, administração e proteção dos ativos virtuais custodiados, ainda que determinadas funções tecnológicas sejam terceirizadas. Já a prestação de serviços tecnológicos de suporte consiste no fornecimento infraestrutura, sistemas ou soluções tecnológicas que auxiliam a execução da atividade, sem assunção direta de deveres fiduciários perante os clientes.

A contratação de prestadores tecnológicos não altera a responsabilidade da PSAV Custodiante perante clientes, autoridades e demais partes interessadas. A instituição permanece integralmente responsável pela custódia dos ativos virtuais, pelos controles adotados e pelo cumprimento das obrigações previstas na regulação e na autorregulação, ainda que utilize terceiros para execução de atividades específicas.

P14: As PSAV Intermediárias podem realizar custódia?

R: Não. A instituição autorizada apenas como intermediária não deve prestar custódia fora do escopo de sua autorização. A modalidade que acumula intermediação e custódia poderá exercer ambas as atividades, desde que autorizada e que observe integralmente os requisitos aplicáveis à custódia. Assim como a regulação, o Regime Experimental reserva a atividade de custódia qualificada — guarda fiduciária, controle de chaves, conciliação e responsabilidade

integral perante clientes — exclusivamente às instituições Custodiantes, conforme definições do Regime. A PSAV Intermediária (corretora ou prestadora de serviços de negociação) não tem como objeto social a custódia e não pode assumir responsabilidades fiduciárias sobre os ativos dos clientes sem se constituir ou contratar uma PSAV Custodiante. O arranjo permitido é a contratação formal de uma PSAV Custodiante pela PSAV Intermediária, com: (i) contrato escrito definindo escopo e responsabilidades; (ii) segregação contábil dos ativos de clientes na PSAV Custodiante; (iii) reconciliação individualizada; e (iv) responsabilidade integral da PSAV Custodiante perante os clientes finais, mesmo que o relacionamento comercial seja mediado pela Intermediária. A PSAV Intermediária permanece responsável pela adequada seleção e monitoramento da custodiante contratada.

P15: A custódia inclui atividades de staking?

R: Sim. A custódia pode viabilizar operações de staking quando o serviço for permitido, expressamente contratado e operacionalmente suportado. O staking não integra automaticamente a custódia e deve observar disciplina própria, transparência sobre riscos, tratamento de recompensas, períodos de bloqueio, slashing, terceiros validadores e condições de devolução. Assim, quando oferecido pela PSAV Custodiante, o staking deve estar expressamente previsto no contrato de custódia, com definição clara das atribuições, responsabilidades, riscos envolvidos, critérios de distribuição de recompensas e hipóteses de indisponibilidade ou perda decorrentes da operação.

Além disso, a instituição deve manter controles que assegurem a adequada identificação e segregação dos ativos dos clientes envolvidos nas operações de staking, inclusive nos casos em que sejam utilizados arranjos operacionais compartilhados permitidos pelo Regime. As posições e recompensas geradas devem ser passíveis de rastreabilidade, reconciliação e prestação de contas aos clientes, permitindo a identificação individualizada dos direitos de cada titular.

P16: Quais cuidados especiais devem ser observados com ativos referenciados em moeda fiduciária (stablecoins)?

R: Na oferta, custódia, intermediação ou listagem de AVRFs (stablecoins), deve-se observar: avaliação da regularidade do emissor e ativo, qualidade, liquidez e governança dos ativos de reserva, clareza sobre direitos do cliente, existência de informações públicas e auditorias, vedação a ativos cujo controle de reservas seja feito por algoritmos, sem reservas tangíveis demonstráveis. O contrato deve descrever as características específicas do ativo referenciado custodiado.

3. Responsabilização e Deveres da Prestadora de Serviço de Custódia de Ativos Virtuais

P17: Em quais situações ativos virtuais de clientes podem ser utilizados, onerados ou empregados em operações específicas?

R: Como regra, os ativos virtuais dos clientes não podem ser utilizados, onerados, emprestados, dados em garantia ou empregados para finalidades próprias da instituição, na forma da Resolução BCB nº 520/25. Qualquer exceção depende de autorização expressa na regulação aplicável e, quando cabível, de consentimento prévio, específico e destacado do cliente, previsão contratual, segregação adequada e divulgação dos riscos.

P18: Quais políticas, manuais e documentos a PSAV Custodiante deve manter?

R: A PSAV Custodiante deve manter políticas, manuais, procedimentos operacionais e documentação formal que demonstrem a estrutura de controles aplicável à atividade de custódia de ativos virtuais. Essa documentação deve contemplar, no mínimo, a descrição do modelo operacional, governança, gestão de riscos, controles internos, segregação patrimonial, gestão de chaves, conciliação, continuidade de negócios, tratamento de incidentes, contratação de terceiros e mecanismos de supervisão e controle.

As políticas e manuais devem ser formalmente aprovados, periodicamente revisados e acompanhados de registros e evidências que demonstrem sua efetiva implementação e observância.

P19: Com que frequência as políticas e manuais devem ser revisados?

R: As políticas e manuais relacionados à atividade de custódia devem ser revisados, no mínimo, a cada 24 meses ou sempre que ocorrer mudança material no modelo operacional, tecnológico, regulatório ou na estrutura de riscos da instituição. A revisão deve ser formalmente documentada e aprovada conforme a governança interna da instituição.

P20: A contratação de subcustodiante ou prestador tecnológico transfere a responsabilidade da PSAV Custodiante?

R: Não. A contratação de subcustodiantes, prestadores tecnológicos ou outros terceiros não afasta nem reduz a responsabilidade da PSAV Custodiante perante clientes, reguladores e demais autoridades competentes. A instituição permanece integralmente responsável pela guarda dos ativos virtuais, pela efetividade dos controles adotados e pelo cumprimento das obrigações regulatórias e de autorregulação, inclusive quando parte das atividades for executada por terceiros, subcustodiantes ou prestadores localizados em jurisdições estrangeiras. A divisão operacional de tarefas deve ser formalizada e monitorada, mas a supervisão, a governança e o dever de assegurar a conformidade permanecem com a custodiante.

P21: O que deve conter o atesto anual da alta administração?

R: O atesto anual deve declarar a adequação dos controles adotados pela instituição, registrar eventuais deficiências identificadas, descrever mudanças relevantes ocorridas no período e indicar os respectivos planos de ação corretiva. O documento deve ser formalmente aprovado na estrutura de governança da instituição.

P22: Qual o prazo de elaboração e guarda das evidências relacionadas às atividades de custódia?

R: O atesto anual deve ser elaborado até o encerramento do primeiro trimestre subsequente ao exercício de referência. Os registros, documentos, evidências de conciliação, trilhas de auditoria, relatórios de auditoria, logs de sistemas e demais informações necessárias para demonstrar a execução das atividades de custódia devem ser mantidos por, no mínimo, cinco anos. Os controles adotados devem assegurar rastreabilidade, integridade, auditabilidade e capacidade de reconstituição histórica das informações.

P23: Quais requisitos de retenção de evidências, rastreabilidade e controles de integridade se aplicam aos registros operacionais da atividade de custódia?

R: A PSAV custodiante deve manter registros contábeis e operacionais individualizados por cliente e ativo, contendo identificação do cliente, tipo e quantidade de ativo, data de entrada e saída. Deve haver reconciliação com posições on-chain documentada, retenção de evidências por 5 anos e proteção dos sistemas por controles de integridade. O Regime exige a retenção por no mínimo 5 (cinco) anos de todas as evidências de conciliação, incluindo snapshots de posições on-chain, relatórios de reconciliação, logs de divergências e respectivas sanações. O inciso IV determina que os sistemas de registro devem implementar controles de integridade e versionamento que impeçam a alteração retroativa de registros sem registro de auditoria. Na prática, isso significa que: (i) qualquer correção de registro deve gerar novo lançamento com referência ao original, nunca sobrescrita; (ii) as trilhas de auditoria dos sistemas devem ser imutáveis ou protegidas por mecanismo equivalente (e.g., hash criptográfico); e (iii) a PSAV deve ser capaz de reconstituir o estado de qualquer posição em qualquer data passada dentro do período de guarda.

P24: Quais informações periódicas devem ser disponibilizadas aos clientes?

R: A PSAV Custodiante deve disponibilizar aos clientes informações claras, completas e atualizadas sobre os ativos custodiados e os serviços prestados, incluindo, no mínimo: posição consolidada dos ativos, saldos e movimentações do período, reconciliações aplicáveis, eventos relevantes incidentes sobre os ativos, informações sobre Prova de Reservas, terceiros relevantes utilizados na cadeia de custódia, canais de atendimento disponíveis e demais informações necessárias para que o cliente acompanhe a situação de seus ativos e os riscos associados ao serviço prestado.

P25: Quais cláusulas mínimas devem constar do contrato de custódia?

R: O contrato deve prever, no mínimo: identificação da PSAV e do cliente; modelo de custódia; prazos e condições de devolução; riscos e responsabilidades; regras de movimentação, bloqueio e devolução; política de remuneração; planos de continuidade e contingência; atribuições quanto a staking; mecanismos de controles internos e auditoria; fonte informacional dos dados; especificação dos ativos e aspectos técnicos; tratamento de dados pessoais; formas de comunicação de incidentes; e foro contratual.

P26: Como deve ser tratado o tema de proteção de dados pessoais?

R: O contrato deve prever tratamento de dados pessoais em conformidade com a LGPD. Cláusulas de confidencialidade e proteção de dados devem estar presentes em contratos com terceiros. A PSAV deve observar deveres de proteção de dados pessoais e sigilo legal/regulatório, com controles de autenticação e acesso baseados em perfis.

P27: O que deve constar sobre remuneração no contrato?

R: O contrato deve prever política de remuneração e encargos de forma clara, incluindo valores, periodicidade, forma de pagamento e eventuais condições para alteração. Deve especificar se há cobrança para serviços adicionais como staking ou tratamento de eventos on-chain.

4. Guarda Segura, Controle e Gerenciamento de Chaves

P28: Quais requisitos devem ser observados na gestão do ciclo de vida das chaves privadas?

R: A PSAV Custodiante deve adotar controles que cubram todo o ciclo de vida das chaves privadas, incluindo sua geração, armazenamento, utilização, autorização, rotação, substituição, backup, recuperação e descarte. Esses processos devem ser formalmente documentados, auditáveis e suportados por controles que assegurem confidencialidade, integridade, disponibilidade, segregação de funções e rastreabilidade das operações realizadas.

P29: Como deve ser realizada a geração de chaves privadas?

R: A geração de chaves privadas deve ser conduzida de forma aleatória, confidencial, auditável e em ambiente controlado, sem conexão externa indevida, observando segregação de responsabilidades e participação de signatários independentes. Devem ser utilizados padrões criptográficos reconhecidos e mantidos registros auditáveis do processo, sem exposição do material criptográfico gerado.

P30: Tecnologias como MPC, multisig e HSM podem ser utilizadas para atendimento dos requisitos do Regime?

R: Sim. O Regime adota abordagem baseada em funções e controles, sem limitar o uso a uma tecnologia específica. Soluções como HSM, MPC, multisig ou tecnologias equivalentes podem ser utilizadas, desde que demonstrem nível adequado de segurança criptográfica, segregação de responsabilidades, controle de acesso, resiliência operacional e rastreabilidade compatíveis com os requisitos da regulamentação e da autorregulação. A avaliação de adequação pode tomar como referência padrões reconhecidos de mercado, como o CCSS (Cryptocurrency Security Standard), a ISO 27001 e relatórios SOC 2 Tipo II, sem que sua menção configure homologação ou certificação pela Anbima.

P31: Quais requisitos se aplicam ao armazenamento, backup e recuperação de chaves privadas?

R: O armazenamento das chaves privadas deve utilizar mecanismos de proteção compatíveis com a criticidade dos ativos custodiados, observando segregação de acessos, criptografia adequada e controles contra comprometimento indevido. Devem ser mantidos backups protegidos, em localizações distintas e submetidos a testes periódicos de integridade e recuperação, de forma a garantir a continuidade da custódia e a recuperação segura das chaves em caso de falhas, incidentes ou desastres.

P32: Como devem ser controlados os acessos e responsabilidades relacionados às chaves privadas?

R: A PSAV Custodiante deve adotar controles que assegurem segregação adequada de funções, autenticação robusta, rastreabilidade de acessos e limitação de privilégios. As responsabilidades relativas à geração, guarda, autorização de uso, movimentação e auditoria das chaves devem ser distribuídas de forma a evitar concentrações inadequadas de poder e reduzir riscos operacionais e de fraude.

P33: O gerenciamento das chaves privadas deve ser auditado?

R: Sim. Os controles relacionados à guarda e ao gerenciamento de chaves privadas devem ser objeto de auditoria periódica e independente, realizada, no mínimo, anualmente, nos termos da Resolução BCB nº 520/25, permitindo verificar a efetividade dos processos de geração, armazenamento, utilização, recuperação e descarte, bem como a aderência às políticas e procedimentos internos.

P34: Como a instituição deve responder a incidentes envolvendo chaves privadas?

R: A PSAV Custodiante deve manter plano formal de resposta a incidentes envolvendo chaves privadas, contemplando procedimentos de contenção, substituição de chaves comprometidas, migração segura dos ativos, comunicação aos clientes afetados, análise das causas do incidente e implementação de medidas corretivas. O plano deve ser periodicamente testado e integrado aos mecanismos de continuidade de negócios da instituição.

5. Movimentação e Transferências

P35: Quais controles devem ser observados nas movimentações e transferências de ativos virtuais?

R: Toda movimentação ou transferência de ativos virtuais deve estar sujeita a controles que assegurem sua autorização, rastreabilidade, integridade e adequada documentação. A PSAV Custodiante deve manter registros da operação, identificação do solicitante, ativo envolvido, quantidade, destino, data e horário da movimentação, bem como evidências que permitam sua verificação posterior. Os controles adotados devem contemplar segregação de funções, mecanismos de validação compatíveis com o risco da operação, incluindo aprovações adicionais para operações de maior materialidade quando aplicável e retenção das evidências por período mínimo regulamentar.

P36: Como devem ser tratados ônus, gravames e bloqueios incidentes sobre ativos custodiados?

R: A PSAV Custodiante deve manter controles que permitam identificar, registrar e administrar adequadamente ônus, gravames, bloqueios judiciais, administrativos ou quaisquer outras restrições incidentes sobre ativos virtuais custodiados. Esses eventos devem ser refletidos nos registros operacionais da instituição, impedir movimentações incompatíveis com a restrição existente e ser comunicados ao cliente quando aplicável.

P37: Como devem ser tratados eventos on-chain que afetem ativos custodiados?

R: A PSAV Custodiante deve manter política formal para identificação, avaliação e tratamento de eventos on-chain que possam afetar os ativos sob sua guarda, incluindo forks, airdrops, reorganizações de rede, migração de protocolos, alterações relevantes de governança e outros eventos similares. A política deve estabelecer critérios objetivos para tomada de decisão, execução operacional, comunicação aos clientes, registro das decisões adotadas e tratamento dos ativos ou direitos eventualmente decorrentes do evento.

P38: A PSAV Custodiante pode deixar de processar determinado airdrop?

R: Sim, desde que a decisão esteja fundamentada em critérios objetivos previamente definidos na política de tratamento de eventos on-chain, tais como riscos operacionais, jurídicos, reputacionais, regulatórios ou de segurança. Os critérios adotados devem ser documentados, aplicados de forma consistente e divulgados de forma transparente aos clientes. A decisão deve preservar os melhores interesses dos clientes e observar as disposições contratuais e os deveres de informação aplicáveis.

P39: Quais obrigações de PLD/FTP e de monitoramento de transações se aplicam às movimentações de ativos virtuais custodiados?

R: As movimentações e transferências de ativos virtuais custodiados devem observar integralmente as normas de PLD/FTP aplicáveis, incluindo procedimentos de conhecimento do cliente (KYC), monitoramento de transações (KYT), triagem (screening) de endereços e verificação de listas de sanções, com apoio de ferramentas de análise on-chain compatíveis com o porte e o perfil de risco da instituição. Operações atípicas ou suspeitas devem ser identificadas, registradas e comunicadas às autoridades competentes na forma da regulamentação vigente. Esses controles devem estar integrados à política de PLD/FTP da instituição e alcançar também os arranjos com terceiros e subcustodiantes.

P40: Como a PSAV Custodiante deve observar a Travel Rule nas transferências de ativos virtuais?

R: Nas transferências de ativos virtuais, a instituição deve observar os requisitos de transmissão de informações sobre originador e beneficiário (Travel Rule), conforme a Recomendação 16 do GAFI e a regulamentação aplicável, adotando soluções interoperáveis para envio e recebimento dessas informações entre prestadores. Devem ser definidos procedimentos específicos para transferências envolvendo carteiras autocustodiadas, com medidas de verificação baseadas em risco, além de controles de proteção de dados pessoais na transmissão das informações. As dificuldades práticas de implementação, como a fragmentação de soluções e o alcance transfronteiriço das transferências, devem ser consideradas na política da instituição e nos contratos com terceiros.

6. Disponibilização, Acesso Contínuo e Devolução

P41: Como a PSAV Custodiante deve assegurar o acesso contínuo dos clientes aos ativos custodiados?

R: A PSAV Custodiante deve manter mecanismos contratuais, operacionais e tecnológicos que assegurem aos clientes o acesso aos seus ativos virtuais mesmo em situações de descontinuidade operacional, liquidação, insolvência, falência ou substituição da instituição. Esses mecanismos podem contemplar a transferência para custodiante substituto, a devolução direta dos ativos aos clientes ou outras soluções equivalentes previamente definidas e testadas. Ressalvadas as hipóteses legais de bloqueio ou restrição, o acesso aos ativos dos clientes deve ser preservado de forma contínua e segura. Trata-se de obrigação de meios: a instituição deve manter estruturas, planos e testes aptos a maximizar a proteção e o acesso dos clientes, registrando-se que o tratamento dos ativos custodiados em regimes de insolvência ou de resolução ainda não conta com disciplina legal específica nem com consolidação jurisprudencial.

P42: A PSAV Custodiante deve manter plano de continuidade de negócios e plano de contingência?

R: Sim. A custodiante deve manter planos de continuidade e contingência compatíveis com a criticidade da custódia, visando preservar acesso, integridade, movimentação e recuperação dos ativos.

P43: Quais elementos mínimos devem constar do plano de continuidade e contingência?

R: O plano deve contemplar, no mínimo: (i) identificação de sistemas, processos e prestadores críticos; (ii) procedimentos de recuperação e restabelecimento das operações; (iii) mecanismos de transferência para custodiante substituto ou devolução direta dos ativos; (iv) definição de responsáveis e fluxos de comunicação; (v) procedimentos para substituição de prestadores tecnológicos críticos; e (vi) realização periódica de testes, revisão e atualização dos planos. Sempre que ocorrer mudança material envolvendo prestadores críticos ou infraestrutura relevante, os planos deverão ser revisados e atualizados.

P44: Como devem ser definidos os prazos e procedimentos para devolução de ativos virtuais?

R: O contrato de custódia deve prever, de forma clara e acessível, os prazos, condições e procedimentos para devolução dos ativos virtuais ou sua transferência a custodiante substituto, observada a regulamentação aplicável. Os prazos devem ser compatíveis com o modelo operacional adotado e considerar as características dos ativos custodiados, observando transparência e previsibilidade para os clientes.

7. Salvaguarda dos Ativos Virtuais e Segregação Patrimonial

P45: O que é segregação patrimonial e como ela deve ser implementada na custódia de ativos virtuais?

R: A segregação patrimonial consiste na separação dos ativos virtuais de clientes dos ativos próprios da instituição, por meio de registros contábeis e operacionais que permitam sua individualização, rastreabilidade e proteção patrimonial. Trata-se de exigência da Resolução BCB nº 520/25, cujo detalhamento operacional é objeto das melhores práticas do Regime. A PSAV Custodiante deve manter controles que assegurem a identificação dos direitos de cada cliente, a adequada conciliação dos registros e a preservação dos ativos em situações de insolvência, liquidação ou descontinuidade operacional. A efetividade da segregação patrimonial em cenários concursais depende, contudo, de construção legal e jurisprudencial ainda em consolidação, razão pela qual os controles exigidos configuram obrigação de meios voltada a maximizar a proteção dos clientes.

P46: O que é pooling de ativos virtuais e quando ele pode ser utilizado?

R: Pooling é o arranjo operacional pelo qual ativos virtuais de diferentes clientes são mantidos coletivamente em uma mesma carteira, endereço ou estrutura operacional. Sua utilização é permitida desde que a instituição mantenha registros individualizados, conciliação periódica, rastreabilidade dos direitos de cada cliente e controles que assegurem a integridade e a proteção dos ativos custodiados.

P47: É permitida a manutenção conjunta de ativos próprios e de clientes?

R: Como regra, não. A segregação patrimonial exige a separação entre ativos próprios da instituição e ativos de clientes. Qualquer exceção admitida pela regulamentação deve observar estritamente os limites, condições e controles previstos na norma aplicável, incluindo identificação adequada dos ativos, inexistência de ônus para os clientes e finalidade operacional legítima.

P48: Podem existir estruturas operacionais destinadas ao pagamento de taxas de rede ou validação de transações?

R: Sim. Estruturas operacionais destinadas ao pagamento de taxas de rede ou à participação em mecanismos de validação podem ser utilizadas, desde que observem segregação contábil adequada, mecanismos de conciliação, controles de risco, preservação da identificação dos ativos dos clientes e não comprometam a capacidade de individualização e devolução dos ativos quando necessária.

P49: Como a PSAV Custodiante deve validar a efetividade da segregação patrimonial?

R: A instituição deve realizar conciliações periódicas, observada a frequência mínima exigida pela regulamentação entre seus registros internos e os ativos efetivamente custodiados, bem como submeter seus controles de segregação patrimonial a auditorias independentes e testes periódicos de efetividade. Os procedimentos adotados devem ser capazes de demonstrar a identificação individualizada dos clientes, a suficiência dos controles operacionais e a capacidade de devolução ou transferência dos ativos em cenários adversos. Os testes devem considerar, entre outros cenários, falhas operacionais, indisponibilidade de prestadores críticos, liquidação da instituição e devolução em massa de ativos virtuais.

8. Prova de Reservas

P50: O que é a Prova de Reservas (PoR) e qual é seu objetivo?

R: A Prova de Reservas (PoR) é um mecanismo destinado a verificar, em data-base específica, a correspondência entre os ativos virtuais sob custodia e os saldos registrados em favor dos clientes. Seu objetivo é promover transparência e confiança quanto à existência dos ativos custodiados, sem substituir auditorias financeiras, avaliações de solvência, verificação de passivos ou outros procedimentos independentes de asseguração.

P51: Quais requisitos devem ser observados na realização da Prova de Reservas?

R: A Prova de Reservas deve ser realizada com base em metodologia formal, documentada, auditável e compatível com a estrutura operacional da instituição. A instituição deve assegurar a integridade das informações utilizadas, a rastreabilidade dos procedimentos adotados, a preservação da confidencialidade dos clientes e a realização de verificações independentes compatíveis com a metodologia empregada. A periodicidade da realização da PoR deve estar prevista na política da instituição e ser compatível com os riscos e características das atividades exercidas. São admitidas metodologias reconhecidas de mercado — como provas baseadas em árvores de Merkle com verificação independente —, desde que atendidos os requisitos de documentação, integridade e auditabilidade referidos nesta resposta.

P52: Como os resultados da Prova de Reservas devem ser divulgados?

R: Os resultados da Prova de Reservas devem ser divulgados aos clientes de forma clara, transparente e compatível com a metodologia adotada, preservando a confidencialidade das informações individuais. A divulgação deve apresentar informações suficientes para a compreensão da metodologia utilizada, das premissas relevantes consideradas, das limitações do mecanismo e dos principais resultados obtidos. Não é necessária a divulgação integral dos dados utilizados na apuração nem de informações que possam comprometer a segurança operacional da instituição ou a privacidade dos clientes.

P53: Como a Prova de Reservas deve ser realizada quando a custódia ocorre por meio de arranjo omnibus ou em nome de PSAV Contratante?

R: Nos arranjos omnibus ou em estruturas nas quais a PSAV Custodiante mantém os ativos em nome de outra instituição responsável pelo relacionamento com o cliente final, devem ser mantidos mecanismos que permitam a reconciliação entre os saldos consolidados dos ativos custodiados e os registros individualizados dos clientes finais. A estrutura deve assegurar rastreabilidade auditável, preservação da confidencialidade dos clientes e acesso às informações necessárias para verificação independente da consistência dos saldos.

P54: Quais elementos devem constar da metodologia de Prova de Reservas?

R: A metodologia deve ser formalmente documentada e contemplar, no mínimo, o escopo da verificação realizada, os critérios de identificação e reconciliação dos ativos abrangidos, os procedimentos de coleta, validação e tratamento das informações, os mecanismos de verificação utilizados, as medidas de proteção da privacidade dos clientes, o tratamento de estruturas de pooling, omnibus ou subcustódia e as limitações e premissas relevantes do processo adotado.

9. Auditoria

P55: O que deve constar dos relatórios de auditoria?

R: Os relatórios de auditoria devem descrever o escopo e a metodologia utilizados, os controles avaliados, os principais achados identificados, a classificação de criticidade dos achados, os riscos ou fragilidades constatadas, as recomendações de melhoria e os respectivos planos de ação, quando aplicáveis. Os relatórios devem ser suficientemente detalhados para permitir a compreensão das conclusões alcançadas e o acompanhamento das medidas corretivas.

P56: Quais auditorias são exigidas para a atividade de custódia de ativos virtuais?

R: A PSAV Custodiante deve manter estrutura de auditoria compatível com os riscos de suas atividades, contemplando auditoria interna periódica e auditoria independente, esta realizada, no mínimo, anualmente, nos termos da Resolução BCB nº 520/25. Ambas têm por objetivo avaliar a efetividade dos controles relacionados à atividade de custódia e apoiar a estrutura de governança, gestão de riscos e controles internos da instituição.

P57: Qual a diferença entre a auditoria interna e a auditoria independente?

R: A auditoria interna integra a terceira linha de defesa da instituição e tem como objetivo avaliar continuamente a efetividade dos controles internos e dos mecanismos de gestão de riscos. A auditoria independente é realizada por entidade externa sem vínculo com a instituição e tem por objetivo fornecer avaliação imparcial dos principais controles relacionados à atividade de custódia. As duas funções são complementares e não se substituem. A auditoria interna atua de forma contínua na terceira linha de defesa, enquanto a auditoria independente fornece asseguração externa, com periodicidade mínima anual, sobre aspectos críticos da operação.

P58: Os relatórios de auditoria devem ser aprovados e mantidos pela instituição?

R: Sim. Os relatórios de auditoria devem ser formalmente analisados pela estrutura de governança da instituição, acompanhados dos planos de ação eventualmente necessários e mantidos em arquivo pelo prazo previsto na regulamentação e na autorregulação aplicáveis.

P59: Quais temas devem ser abrangidos pelas auditorias da atividade de custódia?

R: As auditorias devem abranger, conforme aplicável, os controles de segregação patrimonial, reconciliação de posições, gerenciamento de chaves privadas, segurança cibernética, continuidade de negócios, contratação de terceiros, Prova de Reservas, transparência e demais controles relevantes para a atividade de custódia.

10. Segurança e Resiliência Operacional

P60: Quais requisitos de segurança cibernética devem ser observados?

R: O Regime exige: autenticação multifator e segregação de perfis; criptografia forte e controles de integridade; monitoramento contínuo de vulnerabilidades e tentativas de intrusão; planos de resposta a incidentes; registro e guarda de logs por no mínimo 5 anos; e reporte tempestivo aos clientes. As políticas devem ser revisadas no mínimo a cada 24 meses.

P61: Qual a periodicidade de revisão das políticas de segurança?

R: Políticas e controles de segurança da informação e cibersegurança devem ser revisados no mínimo a cada 24 meses, ou sempre que houver mudança relevante na infraestrutura tecnológica, modelo operacional ou perfil de risco.

P62: Quais frameworks podem ser usados na auditoria de segurança?

R: A instituição pode utilizar frameworks reconhecidos, como NIST, ISO 27001, CIS Controls, SOC ou equivalentes, desde que adequados ao escopo e aplicados por profissionais independentes e qualificados. A menção não representa homologação ou certificação pela ANBIMA. Relatório deve conter escopo, metodologia, normas adotadas, principais achados, planos de ação corretiva, assinatura do auditor e da alta administração, com guarda por 5 anos.

P63: Que monitoramento de segurança é obrigatório?

R: Monitoramento contínuo de vulnerabilidades, tentativas de intrusão, acessos às chaves privadas, alterações em sistemas críticos, e transações suspeitas. Logs devem ser mantidos por no mínimo 5 anos com controles de integridade e proteção contra adulteração.

P64: A instituição deve contratar seguro ou garantia financeira? / São necessárias garantias financeiras para riscos operacionais?

R: A PSAV deve avaliar periodicamente, no âmbito de gestão de riscos, a necessidade e suficiência de adoção de garantias financeiras ou mecanismos equivalentes para mitigação de perdas decorrentes de incidentes operacionais ou falhas de segurança. Avaliação deve considerar perfil de risco, complexidade operacional, volume sob custódia, grau de terceirização e histórico de incidentes.

11. Governança, Compliance e Controles Internos

P65: Qual estrutura mínima de governança a PSAV Custodiante deve manter?

R: A PSAV Custodiante deve manter estrutura de governança compatível com a natureza, porte, complexidade e perfil de risco de suas atividades, incluindo mecanismos de supervisão, gestão de riscos, compliance, segurança cibernética e controles internos. A estrutura deve assegurar definição clara de responsabilidades, reporte à alta administração e documentação

das decisões relevantes. A estrutura pode contemplar comitês ou instâncias responsáveis por temas como riscos, compliance e segurança cibernética, observada a proporcionalidade em relação ao porte e à complexidade das atividades da instituição.

P66: Quais são as responsabilidades da alta administração?

R: A alta administração é responsável pela efetividade da estrutura de governança, gestão de riscos, compliance e controles internos da instituição, bem como por promover a cultura de integridade, gestão de riscos e conformidade. Deve aprovar políticas relevantes, supervisionar a implementação dos controles, acompanhar a correção de deficiências identificadas, deliberar sobre mudanças materiais e assegurar recursos adequados para a atividade de custódia.

P67: O que é o modelo das três linhas de defesa?

R: O modelo das três linhas de defesa organiza as responsabilidades de controle na instituição em: (i) primeira linha, composta pelas áreas de negócio e operação, responsáveis pela execução dos controles e gestão dos riscos; (ii) segunda linha, composta pelas funções de risco e compliance, responsáveis pelo monitoramento e supervisão; e (iii) terceira linha, composta pela auditoria interna, responsável pela avaliação independente da efetividade do sistema de controles internos.

P68: Quais requisitos de qualificação se aplicam aos administradores e responsáveis técnicos?

R: Os administradores e responsáveis técnicos devem possuir qualificação compatível com as funções exercidas, experiência adequada em temas relacionados à custódia de ativos virtuais, gestão de riscos, segurança da informação, compliance ou atividades correlatas. Devem ainda apresentar reputação ilibada, idoneidade moral e profissional compatíveis com suas atribuições e participar de programas periódicos de capacitação e atualização, observando a evolução tecnológica, regulatória e operacional aplicável à atividade de custódia de ativos virtuais.

P69: O que caracteriza uma mudança material e como ela deve ser tratada?

R: Considera-se mudança material qualquer alteração capaz de afetar de forma relevante a estrutura de custódia, a infraestrutura tecnológica crítica, os mecanismos de gerenciamento de chaves, a segregação patrimonial, a Prova de Reservas ou outros controles essenciais da atividade. Essas mudanças devem ser avaliadas previamente, documentadas, submetidas à governança competente e aprovadas antes de sua implementação. São exemplos de mudanças materiais a substituição de subcustodiante, alterações relevantes nos mecanismos de gestão de chaves privadas ou mudanças significativas na metodologia de Prova de Reservas.

P70: Como devem ser tratados e comunicados incidentes relevantes?

R: A PSAV Custodiante deve manter política formal para registro, classificação, tratamento e comunicação de incidentes relevantes. A política deve definir critérios de materialidade,

responsabilidades internas, fluxos de comunicação, medidas corretivas, procedimentos de análise de causa raiz e critérios de reporte à alta administração e às instâncias de governança competentes. Os registros e evidências relacionados aos incidentes devem ser mantidos pelo prazo regulamentar aplicável.

P71: Quais requisitos mínimos devem compor a estrutura de compliance e controles internos?

R: A estrutura de compliance e controles internos deve ser proporcional aos riscos da atividade, contemplar monitoramento contínuo dos controles, avaliação da conformidade regulatória, reporte à governança competente, gestão de conflitos de interesse, mecanismos de reporte às instâncias de governança e procedimentos para identificação, registro e tratamento de falhas de controle.

12. Transparência e Comunicação com clientes

P72: Quais requisitos de transparência e comunicação com clientes devem ser observados?

R: A PSAV Custodiante deve manter política formal de transparência e comunicação com clientes, aprovada e supervisionada pela alta administração. A política deve estabelecer responsabilidades, canais de comunicação, periodicidade de divulgação das informações, procedimentos para tratamento de incidentes e critérios para assegurar que as informações prestadas sejam claras, corretas, atualizadas e compatíveis com o perfil dos clientes atendidos. A alta administração deve supervisionar periodicamente a efetividade desses mecanismos de comunicação e transparência.

P73: Como as informações sobre a custódia devem ser comunicadas aos clientes?

R: As informações relacionadas aos serviços de custódia devem ser apresentadas em linguagem clara, objetiva e compatível com o perfil do público destinatário. As comunicações devem permitir a adequada compreensão dos serviços prestados, dos riscos envolvidos, das responsabilidades da instituição e dos direitos dos clientes, evitando jargões técnicos desnecessários ou informações potencialmente enganosas.

P74: Quais informações e riscos devem ser divulgados aos clientes?

R: A instituição deve divulgar informações claras e tempestivas sobre os serviços prestados, incluindo os modelos de custódia utilizados, a utilização de terceiros relevantes, as condições de acesso e devolução dos ativos, bem como os riscos associados aos ativos virtuais e à prestação do serviço. Devem ser informados, quando aplicáveis, riscos operacionais, tecnológicos, de liquidez, de subcustódia, de segurança cibernética e relacionados a eventos on-chain. As informações divulgadas devem permanecer consistentes com a documentação contratual e com as demais comunicações realizadas pela instituição.

P75: Quais canais de atendimento devem ser disponibilizados aos clientes?

R: A instituição deve disponibilizar canais adequados de atendimento aos clientes, compatíveis com os serviços prestados e capazes de receber dúvidas, solicitações, reclamações e comunicações relacionadas aos ativos custodiados. As informações sobre os canais disponíveis devem constar da documentação contratual e dos materiais de comunicação com clientes.

P76: Os clientes devem ser informados sobre a utilização de subcustodiantes ou terceiros relevantes?

R: Sim. Os clientes devem receber informações adequadas sobre a utilização de subcustodiantes ou prestadores relevantes relacionados à atividade de custódia, de forma compatível com o dever de transparência e observadas as limitações decorrentes de sigilo comercial ou segurança operacional. A instituição deve ser capaz de explicar aos clientes o papel desses terceiros na prestação do serviço de custódia, quando aplicável.

P77: Por quanto tempo devem ser arquivados os relatórios e comunicações enviados aos clientes?

R: Os relatórios, comunicações e notificações enviados aos clientes devem ser arquivados pelo prazo mínimo previsto na regulamentação e na autorregulação aplicáveis, de forma a permitir sua recuperação, verificação de autenticidade e utilização como evidência do cumprimento das obrigações de transparência e comunicação. A instituição deve assegurar a integridade, rastreabilidade e acessibilidade dessas informações durante todo o período de guarda.

13. Contratação de Terceiros

P78: Quais atividades relacionadas à custódia podem ser executadas por terceiros?

R: A PSAV Custodiante pode contratar terceiros para a execução de atividades relacionadas à custódia de ativos virtuais, incluindo serviços tecnológicos, subcustódia e outras atividades de suporte, desde que sejam observados os requisitos de governança, due diligence, monitoramento e controles previstos na regulamentação e na autorregulação aplicáveis.

P79: Quais requisitos mínimos devem constar dos contratos celebrados com terceiros?

R: Os contratos com terceiros devem definir claramente o escopo dos serviços contratados, as responsabilidades das partes, regras de reporte e conciliação, requisitos de continuidade de negócios, mecanismos de auditoria, proteção de dados, confidencialidade, acesso a registros e condições para substituição ou encerramento da relação contratual. Devem também assegurar compatibilidade com as exigências regulatórias e de autorregulação aplicáveis.

P80: Quais procedimentos de due diligence devem ser adotados na contratação de terceiros e subcustodiantes?

R: Antes da contratação, a instituição deve realizar due diligence proporcional aos riscos da atividade exercida, abrangendo aspectos jurídicos, regulatórios, prudenciais, tecnológicos, cibernéticos, operacionais e reputacionais. Nos casos de subcustodiantes localizados no exterior, a avaliação deve considerar também a equivalência regulatória da jurisdição, a efetividade da segregação patrimonial, a existência de supervisão competente e a capacidade de acesso a informações e registros necessários ao exercício da supervisão e da auditoria.

P81: Como devem ser realizadas as conciliações com subcustodiantes?

R: A PSAV Custodiante deve adotar procedimentos de conciliação compatíveis com os riscos e características da atividade terceirizada, assegurando a identificação tempestiva de divergências e a adoção de medidas corretivas quando necessário. A responsabilidade final pela efetividade dessas conciliações permanece com a instituição contratante.

P82: Quando há uma PSAV Intermediária, como devem ser distribuídas as responsabilidades relacionadas ao cliente?

R: Quando uma instituição responsável pelo relacionamento com o cliente contrata ou utiliza uma custodiante, o contrato deve alocar responsabilidades por cadastro, PLD/FT, Travel Rule, ordens, atendimento, proteção de dados, comunicação de incidentes e tratamento de reclamações. A alocação contratual não pode afastar deveres legais próprios de cada participante.

P83: Existem requisitos específicos para a contratação de prestadores tecnológicos críticos?

R: Sim. A contratação de prestadores tecnológicos críticos exige avaliação prévia proporcional aos riscos da atividade, monitoramento contínuo da prestação dos serviços e documentação dos controles adotados. A instituição deve ser capaz de demonstrar que o prestador possui capacidade técnica compatível com a criticidade das funções desempenhadas e que os riscos envolvidos foram adequadamente avaliados e mitigados. Quando aplicável, poderá ser utilizado o Questionário ANBIMA de Due Diligence Tecnológica ou mecanismo equivalente.