

AUDITORIA · GUIA TÉCNICO · SÉRIE ATIVOS VIRTUAIS

Proof of reserves na *prática*

Existência, titularidade e completude dos ativos sob custódia: o que a prova de reservas demonstra, onde ela falha e como transformá-la em evidência de exame independente.

NORMA BASE

NBC TO 3000 · IN BCB 739 ·
Res. BCB 520

PÚBLICO

CFO, riscos, tecnologia e
auditoria interna

EDIÇÃO

Guia técnico MERC · Série
Ativos Virtuais

DATA

Agosto de 2026

Índice

Guia em quatro partes. Parte I: o conceito e as três asserções. Parte II: a mecânica, da árvore de Merkle à completude dos passivos. Parte III: a prova como evidência e suas limitações. Parte IV: implantação, perguntas frequentes e checklist.

PARTE I · CONCEITO

- 01** O que a prova prova · e o que ela não prova
- 02** As três asserções · existência, titularidade, completude
- 03** Prova, auditoria e asseguração · três trabalhos, três normas

PARTE II · MECÂNICA

- 04** Árvore de Merkle na prática · inclusão verificável sem expor saldos
- 05** Titularidade de endereços · quem tem a chave tem o ativo
- 06** Completude dos passivos · o elo fraco da prova
- 07** Janela temporal e ativos móveis · a foto e o instante

PARTE III · EVIDÊNCIA

- 08** Evidência on-chain · do registro em cadeia ao papel de trabalho
- 09** Cotação, conversão e agregação · da quantidade ao valor
- 10** Limitações e formas de burlar · o que a prova não alcança
- 11** Prova de reservas sob NBC TO 3000 · nível de segurança e relatório

PARTE IV · PRÁTICA

- 12** Estruturar uma prova auditável · preparação, papéis e rotina
- 13** Perguntas frequentes
- 14** Checklist · implantação e exame
- 15** Próximos passos com a MERC

PARTE I

I

O que a prova *prova.*

As três asserções que dão sentido técnico à prova de reservas e a diferença entre demonstração pública e asseguração.

01 O que a prova prova

02 As três asserções

03 Prova, auditoria e asseguração

O que a prova de reservas de fato *prova*



Provar que uma PSAV tem reservas parece o fim da história. É o começo. Uma plataforma pode exibir carteiras que somam um valor expressivo e, ainda assim, dever aos clientes mais do que guarda. Reserva sem passivo é meia prova. O regime brasileiro de ativos virtuais entendeu isso e não trata proof of reserves como número de vitrine: trata como controle formal, auditável e público, que precisa cobrir os dois lados da conta. O que se tem e o que se deve.

Comece pela definição. Prova de reservas é a demonstração de que a prestadora controla ativos on-chain cujos saldos somam determinado valor. O controle se prova de forma criptográfica: quem detém a chave privada de um endereço consegue assinar uma mensagem que qualquer terceiro verifica, ou movimentar um valor pequeno e previamente combinado a partir daquele endereço. Somados os saldos dos endereços comprovadamente controlados, tem-se o total das reservas. Até aqui, a prova fala apenas do ativo.

O que ela não prova, sozinha, é o outro lado. A **prova de passivos** soma o que a plataforma deve aos clientes, cliente a cliente, a partir do razão interno de obrigações. Sem ela, uma reserva aparentemente robusta pode esconder insolvência: mostra-se o ativo e cala-se o passivo. Foi a violação dessa lógica que produziu os maiores colapsos do mercado de cripto no mundo. A prova só fecha quando reserva e obrigação são demonstradas juntas e a primeira cobre a segunda, ativo por ativo.

ASPECTO	PROVA DE RESERVAS (ATIVOS)	PROVA DE PASSIVOS (OBRIGAÇÕES)	ÁRVORE DE MERKLE
O que demonstra	Que a PSAV controla ativos on-chain que somam X	Quanto a PSAV deve, no total, aos clientes	Que o saldo de cada cliente está incluído no total de passivos
Como se prova	Assinatura de mensagem com a chave privada ou movimentação-teste	Soma das obrigações do razão interno por cliente	Cada cliente confere o seu ramo até a raiz publicada
Risco se isolado	Esconder passivos maiores que a reserva	Não ter lastro on-chain que cubra o devido	Passivos omitidos ficam fora da árvore
Resultado esperado	Total custodiado verificável	Total devido verificável	Reserva maior ou igual ao passivo, cliente a cliente

O que a Resolução 520 *exige*

O marco parte da Lei 14.478/2022 e do Decreto 11.563/2023, que atribuiu ao Banco Central a competência sobre o setor. Sobre essa base, as Resoluções BCB 519, 520 e 521 estruturam o regime das prestadoras. Elas entraram em vigor em 2 de fevereiro de 2026, e as prestadoras em atividade têm 270 dias, contados da vigência, para protocolar o pedido de autorização. O prazo final é 30/10/2026.

02/02/2026

VIGÊNCIA

Início de vigência das Resoluções BCB 519, 520 e 521, o núcleo do regime das PSAVs.

270 dias

JANELA DE PROTOCOLO

Prazo, contado da vigência, para a prestadora em atividade pedir autorização ao Banco Central.

30/10/2026

PRAZO FINAL

Data limite, improrrogável, para o protocolo do pedido de autorização.

A Resolução 520 coloca a prova de reservas dentro da política formal de segregação patrimonial e determina auditoria independente bienal, com asseguração razoável sobre os ativos próprios e sobre os ativos de clientes, com relatório divulgado publicamente. São três decisões de peso. Primeira: a prova deixa de ser gesto voluntário de marketing e vira componente obrigatório de uma política formal. Segunda: o nível de asseguração exigido é o razoável, o mais alto. Terceira: o resultado é público, e a evidência precisa resistir à leitura de qualquer interessado, não só do regulador.

A REGRA DE OURO

Reserva sem passivo é meia prova. Uma prova de reservas que mostra apenas o total custodiado, sem conciliar com as obrigações e sem sustentar a titularidade das carteiras, não prova o que se propõe. A prova completa demonstra que os ativos existem, que são da prestadora e que cobrem o que ela deve, cliente a cliente.

Este guia percorre o caminho completo: as três asserções que organizam o exame, a mecânica da árvore de Merkle e da prova de titularidade, o elo fraco da completude, a janela temporal, a conversão em valor, as limitações conhecidas, a norma de asseguração e o desenho de implantação. Ao final, perguntas frequentes, checklist e os próximos passos com a MERC.

Existência, titularidade, *completude*.

Diante de uma prova de reservas, o exame independente se organiza em torno de três asserções. Existência: os ativos declarados de fato existem e estão on-chain no momento do corte. Titularidade: os endereços que compõem a reserva são realmente controlados pela PSAV, e não emprestados de terceiros para inflar a foto. Completude: o total de passivos contempla todas as obrigações com clientes, sem omissões que reduzam artificialmente o devido. Quem domina as três palavras domina o assunto.

Existência é o atributo mais direto. O saldo de um endereço é registro público em cadeia: qualquer pessoa consulta e confere. O que a existência exige do exame é um corte temporal bem definido, com bloco de referência registrado, porque saldo posterior à foto não prova nada sobre a data da prova. A consulta se faz diretamente na cadeia, sem depender de relatório da administração, e é complementada por confirmação independente do custodiante para os ativos mantidos em custódia qualificada.

Titularidade exige prova ativa, endereço a endereço. Saldo sem prova de controle não é reserva da instituição. A demonstração usual é a assinatura de mensagem com a chave privada ou a movimentação-teste previamente combinada. A armadilha correspondente é o endereço emprestado: ativos de terceiros exibidos como próprios apenas no instante da verificação. A Parte II detalha os métodos e os seus limites.

Completude é a asserção mais difícil, porque provar que nada foi omitido é sempre mais trabalhoso do que provar que algo está presente. O dado não está on-chain: está no razão interno da plataforma. Um cliente deixado fora da soma reduz o passivo total e faz a reserva parecer suficiente. O antídoto é o teste de completude no sentido clássico da auditoria, cruzando o razão de clientes com fontes independentes do universo real de obrigações.

ASSERÇÃO	O QUE O EXAME BUSCA	PROCEDIMENTO TÍPICO	ARMADILHA
Existência	Que os ativos existem on-chain no corte	Consulta aos saldos on-chain na data do snapshot, com bloco de referência	Snapshot mal definido ou saldo posterior à foto
Titularidade	Que os endereços são controlados pela PSAV	Assinatura de mensagem ou movimentação-teste por endereço	Endereços emprestados ou tomados no momento da foto
Completude	Que todos os passivos com clientes entraram na conta	Conciliação da árvore de Merkle com o razão e teste de completude	Clientes deixados fora da árvore para reduzir o passivo

A equação que *fecha*

As três asserções convergem para uma comparação simples. As reservas comprovadas de cada ativo são a soma do saldo on-chain nas carteiras próprias controladas com os ativos mantidos em custódia qualificada e confirmados de forma independente. As obrigações com clientes são a soma do que a instituição deve, cliente a cliente, por ativo. A cobertura é a divisão de um pelo outro, e a meta é cobertura de pelo menos 100 por cento em cada ativo, não apenas no consolidado.

$$\text{cobertura por ativo} = \text{reservas comprovadas} \div \text{obrigações com clientes}$$

A leitura por ativo importa porque a agregação esconde. Uma cobertura consolidada aparentemente confortável pode conviver com um ativo descoberto, e é exatamente no ativo descoberto que o cliente daquele ativo tem o seu risco. Por isso o exame conclui ativo por ativo, e a Parte III mostra, com um exemplo numérico ilustrativo, como uma falta localizada aparece na conciliação e no relatório.

HIERARQUIA DE DIFICULDADE

Existência é verificável por qualquer um: o saldo está em cadeia. Titularidade exige demonstração criptográfica ativa. Completude exige procedimento de auditoria sobre registros internos. A parte mais fácil de comprovar é a reserva; a parte mais fácil de manipular é a obrigação. O desenho da prova precisa investir esforço na proporção inversa da facilidade: mais horas de exame sobre o razão de obrigações do que sobre os saldos em cadeia, e mais ceticismo sobre o que a plataforma mostra do que sobre o que o registro público confirma.

Prova, auditoria e *asseguração*.

A prestadora que entra no regime do Banco Central precisa de dois trabalhos independentes de terceiros, não de um. O primeiro é a auditoria das demonstrações financeiras. O segundo é a *asseguração* da prova de reservas e dos controles de custódia. São trabalhos de natureza distinta, com normas distintas, objetos distintos e relatórios distintos. Confundir os dois é a origem da maior parte dos atrasos e das ressalvas evitáveis na travessia para o novo regime.

A auditoria das demonstrações segue as NBC TA e olha para dentro do balanço: patrimônio, resultado, fluxos de caixa e notas explicativas. Em uma prestadora, o ponto de julgamento mais sensível é a fronteira entre ativo próprio e ativo de cliente. Ativos virtuais próprios mantidos para uso ou investimento tendem a se enquadrar como intangível, na linha do CPC 04, e ativos mantidos para venda no curso normal do negócio podem se enquadrar como estoque, na linha do CPC 16. Ativos de clientes sob custódia, quando a prestadora não detém o controle no sentido contábil, ficam fora do balanço, com a obrigação de guarda divulgada e sustentada justamente pela prova de reservas.

A *asseguração* da prova de reservas segue a NBC TO 3000 e a correspondente internacional ISAE 3000, normas de trabalhos de *asseguração* que não são auditoria de demonstrações. O objeto é a afirmação da administração de que os ativos custodiados existem e correspondem às obrigações com clientes. Há ainda um terceiro instrumento: o relatório sobre controles de custódia e segregação, sob NBC TO 3402 e ISAE 3402, que conclui sobre o desenho e, conforme o tipo, sobre a operação dos controles ao longo de um período.

TRABALHO	OBJETO	NORMA ÂNCORA	PRODUTO
Auditoria das demonstrações	Demonstrações financeiras da prestadora	NBC TA	Opinião de auditoria
Asseguração da prova de reservas	Existência e correspondência dos ativos de clientes	NBC TO 3000 e ISAE 3000	Conclusão de <i>asseguração</i>
Relatório de controles	Desenho e operação dos controles de custódia e segregação	NBC TO 3402 e ISAE 3402	Relatório de controles

A LINHA QUE SEPARA

A auditoria das demonstrações responde se o balanço da prestadora está correto. A *asseguração* da prova de reservas responde se os ativos que não estão no balanço, porque são de clientes, existem e batem com o que a instituição deve a esses clientes. Uma opinião limpa de auditoria não diz nada sobre a prova de reservas. Uma conclusão limpa de *asseguração* não diz nada sobre o balanço. A prestadora precisa das duas.

A separação importa para a decisão de contratação. Escopo, norma, tipo de conclusão, periodicidade e exigência de divulgação são diferentes. A auditoria das demonstrações segue o ciclo anual. A *asseguração* da prova de reservas tem periodicidade bienal e divulgação pública específica. E, no processo de autorização, a IN BCB 739 tornou o relatório de *asseguração* razoável, emitido por auditor registrado na CVM, parte da documentação exigida da prestadora: o trabalho independente deixou de ser diferencial e virou condição de entrada.

ARMADILHA COMUM

Contratar apenas a auditoria das demonstrações e presumir que ela cobre a prova de reservas. Não cobre. A prova de reservas é objeto próprio, com norma própria de *asseguração*. A instituição que descobre isso perto do protocolo perde a janela de reconciliar carteira a carteira com calma.

Um teste de coerência encerra a seção. O relatório sobre demonstrações cita NBC TA; se citar NBC TO 3000, está trocado. O relatório sobre prova de reservas cita NBC TO 3000 e ISAE 3000; se prometer opinião sobre o balanço, extrapola o objeto. O relatório sobre controles cita NBC TO 3402; se concluir sobre saldos, saiu do escopo. Regra prática de contratação: peça, no

escopo, o nome da norma e o objeto exato. Contrato que diz apenas asseguração, sem dizer sobre o quê e sob qual norma, deixa margem para entregar menos do que a regulação exige.

PART E II

II

A mecânica, sem *mistério*.

Árvore de Merkle, prova de titularidade, completude dos passivos e a janela temporal que muda tudo.

04 Árvore de Merkle na prática

05 Titularidade de endereços

06 Completude dos passivos

07 Janela temporal e ativos móveis

A árvore de *Merkle* na prática.



A árvore de Merkle é a peça que costura reserva e passivo do lado do cliente. Ela resolve um problema real: como permitir que cada cliente verifique que o seu saldo entrou no total de obrigações, sem que a plataforma exponha os saldos de todos os demais. A resposta é uma estrutura de hashes encadeados que publica um único resumo, a raiz, e entrega a cada cliente apenas o caminho que liga o seu saldo a esse resumo.

A mecânica é direta. Cada saldo de cliente vira uma folha da árvore: um hash calculado sobre o identificador e o valor devido. As folhas são combinadas em pares, e cada par é resumido por um novo hash. Os resultados são combinados de novo, em camadas sucessivas, até restar um único hash: a raiz. Qualquer alteração em qualquer folha, por menor que seja, muda a raiz. É essa propriedade que dá à estrutura o seu valor probatório: a raiz publicada é um compromisso matemático com o conjunto exato de saldos que a gerou.

A verificação individual funciona assim: o cliente recebe o seu par de identificador e saldo, mais a sequência de hashes dos ramos vizinhos ao longo do caminho até a raiz. Com isso, ele recalcula os hashes camada a camada e confere se o resultado final coincide com a raiz publicada. Se coincide, o saldo dele estava na árvore no momento em que a raiz foi gerada. Ele não vê nenhum saldo alheio, e ninguém vê o dele.

Uma implantação bem feita cuida de detalhes que decidem o valor probatório do mecanismo. A árvore é construída por ativo, para que a verificação e a conciliação respeitem a regra de cobertura ativo por ativo. As folhas protegem a identidade do cliente, usando identificadores derivados que não expõem dados cadastrais a quem observa a estrutura. A raiz é publicada junto com a identificação do corte a que se refere, para que ninguém compare uma árvore de uma data com saldos de outra. E as instruções de verificação são simples o bastante para que um cliente sem formação técnica consiga executá-las, porque um mecanismo que só especialistas usam não cumpre a função de transparência que justificou a sua existência.

CAMADA	O QUE CONTÉM	QUEM VERIFICA
Folhas	Hash do identificador e do saldo de cada cliente, por ativo	Cada cliente confere a própria folha
Ramos intermediários	Hashes de pares combinados, camada a camada	O cliente recalcula com os hashes vizinhos recebidos
Raiz	Resumo único de todos os saldos incluídos	Publicada; qualquer interessado compara
Soma das folhas	Total de obrigações incluídas na árvore	O exame independente concilia com o razão contábil

O que a árvore *não* prova

Aqui mora a distinção que organiza todo o resto do guia. A árvore de Merkle prova inclusão, não completude. Ela garante que quem confere está dentro da árvore; não garante que a árvore contém todos os clientes. Uma plataforma poderia gerar uma árvore impecável com apenas parte da base, publicar a raiz e entregar caminhos válidos a todos os incluídos. Cada verificação

individual daria certo, e o total continuaria errado. O cliente omitido não recebe caminho nenhum, e clientes que não verificam não denunciam nada.

INCLUSÃO NÃO É COMPLETUDE

A árvore de Merkle garante que quem está nela foi incluído. Não garante que todos estão nela. Essa distinção é o coração do trabalho do auditor: a completude do conjunto de folhas precisa ser testada por procedimento próprio, contra o razão contábil e contra fontes independentes do universo de clientes.

Por isso a árvore vale como componente de um desenho maior, nunca como prova autossuficiente. No desenho auditável, a soma das folhas precisa ser conciliada com o total de passivos do razão contábil, e o razão precisa estar sujeito a teste de completude. A raiz precisa estar vinculada ao mesmo corte temporal dos saldos on-chain, com bloco de referência registrado, para que ativo e passivo sejam fotografados no mesmo instante. E a ferramenta de verificação precisa estar acessível aos clientes, porque um mecanismo de inclusão verificável que ninguém consegue usar é apenas decoração criptográfica sobre um número da administração.

A prova de titularidade dos endereços.

Comprovar que um endereço tem saldo é trivial: está registrado em cadeia. Comprovar que a instituição controla aquele endereço é o trabalho de verdade. Em ativos virtuais, quem detém a chave privada detém o ativo. A titularidade, portanto, não se prova com contrato nem com declaração: prova-se demonstrando controle da chave, endereço a endereço, e provando que esse controle é exclusivo e persistente.

O método usual é a **assinatura de mensagem**. Quem detém a chave privada assina um texto arbitrário, e qualquer pessoa verifica que a assinatura corresponde àquele endereço, sem que a chave seja exposta. Para ter valor de evidência, a mensagem precisa ser específica do exercício: um texto definido no momento do corte, que não possa ter sido assinado em outra ocasião e reaproveitado. A alternativa é a **movimentação-teste**: transfere-se um valor pequeno e previamente combinado a partir do endereço, evidenciando controle pela própria transação registrada em cadeia. Nos dois casos, a evidência precisa ser arquivada com o texto ou a transação de referência, a data, o endereço e o método de verificação, porque a prova que não deixa registro reconstruível não serve ao exame posterior.

MÉTODO	COMO FUNCIONA	LIMITE
Assinatura de mensagem	Texto de referência assinado com a chave privada; verificação pública contra o endereço	Prova o controle no instante da assinatura, não a persistência nem a origem do ativo
Movimentação-teste	Transferência de valor pequeno e combinado a partir do endereço	Custa taxa de rede e também é pontual; exige combinação prévia para valer como teste
Confirmação de custodiante	Custodiante qualificado confirma, por escrito e de forma independente, os ativos mantidos	Depende da qualidade e da independência do custodiante; exige extrato conciliável

Cada método prova o controle em um instante. Nenhum prova, sozinho, que o controle é exclusivo. Chave compartilhada com terceiro, ou endereço de custodiante sem confirmação independente, cria o risco de contar como reserva o que não está sob controle da instituição. A regra do exame é dura: endereço cujo controle não pode ser provado de forma exclusiva não deve ser contado como reserva.

O RISCO DA CHAVE COMPARTILHADA

Saldo sem prova de controle não é reserva da instituição. E prova de controle sem exclusividade vale pouco: se um terceiro também detém a chave, o ativo pode sair sem autorização da prestadora. A prova de controle da chave é tão importante quanto o saldo, e a exclusividade é tão importante quanto o controle.

Titularidade nasce da governança

A prova de titularidade sustentável no tempo depende da governança de chaves e carteiras. Uma custódia madura separa carteiras conectadas à rede, para a liquidez do dia, de carteiras isoladas, para a guarda do volume. Um desenho ilustrativo com números redondos ajuda a fixar a proporção: com uma obrigação de 46 unidades de um ativo com clientes, a política mantém 42,5 na carteira fria e 3,5 na carteira quente, o que põe 92,4 por cento do volume fora da rede e deixa 7,6 por cento disponível para saques. A conciliação prova que a soma das duas carteiras iguala a obrigação registrada.

Os controles mínimos de chave completam o quadro: segregação de funções entre quem gera, quem aprova e quem movimenta; assinatura múltipla ou esquema equivalente para valores acima do limite; backup de recuperação guardado fora do mesmo ambiente físico; registro imutável de cada acesso e de cada movimentação; e nenhuma chave crítica sob controle de uma só pessoa. Quando a custódia técnica é delegada a custodiante, inclusive estrangeiro admitido sob condições, a responsabilidade pela guarda e pela segregação permanece com a prestadora autorizada no Brasil, e a titularidade se sustenta por confirmação independente e por direito contratual de acesso a registros. Sem essa camada de governança, a assinatura de mensagem prova um instante; com ela, prova um regime.

Completude: o elo *fraco*.

A parte mais fácil de comprovar em uma prova de reservas é o lado dos ativos, porque o saldo on-chain é público e verificável. A parte mais fácil de manipular é o lado das obrigações, porque depende dos registros internos. Um número de obrigações incompleto infla artificialmente a cobertura sem tocar em nenhuma carteira. Por isso a completude dos passivos é o elo fraco da prova e o centro de gravidade do exame independente.

O mecanismo da fraude é simples de descrever. As obrigações com clientes vivem no razão interno da plataforma: o sistema que registra quanto cada cliente tem a receber, por ativo. Quem controla esse sistema controla o denominador da cobertura. Deixar um conjunto de clientes fora da soma reduz o passivo total, e a mesma reserva passa a parecer suficiente. A árvore de Merkle, como visto, não denuncia a omissão: quem ficou de fora não recebe caminho de verificação e, se não reclamar, não aparece.

O antídoto é o teste de completude no sentido clássico da auditoria: partir do registro contábil e de fontes independentes do universo de clientes e verificar se a soma das obrigações reconhecidas corresponde ao universo real. Na prática, o exame cruza pontas que não deveriam divergir: o razão de obrigações por cliente, o sistema operacional de saldos que alimenta a plataforma, a soma das folhas da árvore de Merkle e o total de passivos do razão contábil. Se as pontas batem, e se o próprio razão está sujeito a teste de completude contra movimentações de entrada e saída, a omissão de clientes fica difícil de sustentar.

PONTA DA CONCILIAÇÃO	FONTE	O QUE PRECISA FECHAR
Razão de obrigações por cliente	Registro auxiliar individualizado da plataforma	Soma igual ao passivo de custódia do razão contábil
Sistema operacional de saldos	Base que sustenta a operação diária e os saques	Conciliado ao razão, com diferenças tratadas
Soma das folhas da árvore de Merkle	Estrutura publicada no corte	Igual ao total de obrigações do razão no mesmo corte
Resultado	Três pontas independentes	Mesmo total devido, no mesmo instante, com diferença zero

Individualização é *pré-condição*

O teste de completude só funciona sobre uma base individualizada. Os recursos financeiros de clientes precisam estar em contas individualizadas e segregadas dos recursos próprios, e os ativos virtuais de clientes em carteiras distintas das carteiras da casa. O teste central é implacável: a soma das contas individualizadas tem de igualar a obrigação total de custódia, e o saldo segregado tem de bater com essa soma. Se as pontas não fecham, há mistura, erro de registro ou indisponibilidade, e a prova de reservas perde a base.

CONTA POOL NÃO É SEGREGAÇÃO

Manter todos os recursos de clientes em uma conta coletiva, sem controle individualizado por cliente, não cumpre a exigência de contas individualizadas. A individualização precisa ser demonstrável cliente a cliente, ainda que a conta bancária seja consolidada, por meio de registro auxiliar conciliado. Sem esse registro, a asseguaração encontra ressalva e o teste de completude não tem contra o que rodar.

DE ONDE VEM A EVIDÊNCIA INDEPENDENTE

O universo de clientes não se testa apenas com o que a plataforma mostra. O exame usa fontes que a administração não controla no momento do teste: movimentações de entrada e saída registradas em cadeia e no sistema bancário, histórico de cadastros, reclamações e circularização de uma amostra de clientes. Obrigação omitida costuma deixar rastro em alguma dessas pontas.

Uma consequência prática merece registro. A completude não se prova na véspera: ela depende de o registro individualizado existir e ser conciliado ao longo do período. A prestadora que descobre no exame que a individualização não existe não tem como reconstruí-la retroativamente com valor probatório. É o tipo de lacuna que não se conserta com esforço de última hora, apenas com desenho antecipado.

A janela *temporal* e os ativos móveis.

Prova de reservas é uma fotografia em um instante, e o instante importa tanto quanto a imagem. Um corte temporal mal definido invalida a existência. Um corte previsível convida à preparação. E ativos que se movem ao redor da data do corte podem transformar uma prova formalmente correta em uma foto posada. Esta seção trata do tempo: o corte, os empréstimos de ocasião e a leitura de representatividade.

Primeiro, o corte. A prova precisa de um momento de referência definido com rigor: em cadeias de blocos, o natural é ancorar o corte em um bloco específico, registrado na documentação, de modo que os saldos lidos sejam os daquele bloco e não de um momento vago. Ativo e passivo precisam ser fotografados no mesmo instante: saldos on-chain no bloco de referência e razão de obrigações no mesmo corte, com a raiz da árvore de Merkle gerada sobre essa mesma base. Uma prova com ativo de um momento e passivo de outro compara grandezas de datas diferentes e não conclui nada.

Segundo, o endereço emprestado. Como a titularidade se prova demonstrando controle em um instante, uma plataforma sem reserva suficiente pode, em tese, tomar ativos emprestados de um terceiro no momento do snapshot, provar controle sobre aqueles endereços e devolvê-los depois. A foto fica bonita, a substância não. O exame combate isso olhando o filme ao redor da foto: a persistência do controle antes e depois do corte, a origem dos ativos, movimentações atípicas próximas da data e a coerência entre os endereços apresentados e a operação real da plataforma.

ARMADILHA TEMPORAL	SINAL TÍPICO	RESPOSTA DO EXAME
Corte previsível	Reserva reforçada às vésperas da data conhecida	Corte definido com rigor e sem antecedência que permita preparação
Endereço emprestado	Entradas relevantes pouco antes do corte e saídas logo depois	Análise de movimentação ao redor da data, origem dos ativos e persistência do controle
Foto não representativa	Posição do corte destoa da posição média do período	Leitura do período, não só do instante; verificações intermediárias
Ativo e passivo em datas diferentes	Raiz de Merkle gerada em corte distinto do bloco de referência	Amarração de todas as pontas ao mesmo corte documentado

A FOTO POSADA

Reserva que aparece dias antes do corte e desaparece dias depois não é reserva: é figurino. O valor probatório da prova depende de o exame alcançar a vizinhança temporal do corte, porque é nela que o empréstimo de ocasião deixa rastro. A movimentação on-chain é pública e permanente: quem posa para a foto assina o próprio ensaio.

Um refinamento operacional completa o quadro do corte: os itens em trânsito. No instante da foto, sempre haverá depósitos confirmando em cadeia mas ainda não creditados ao cliente, e saques debitados do cliente mas ainda não liquidados on-chain. Esses itens não invalidam a prova; invalidam a prova mal documentada. O desenho correto define, por escrito, como cada categoria em trânsito é tratada na conciliação, aplica o critério de forma uniforme e registra os itens do corte com o seu desfecho. Diferença explicada e documentada é conciliação; diferença ignorada é lacuna.

Da foto ao *filme*

Terceiro, a representatividade. Ainda que o corte seja íntegro, uma única foto diz pouco sobre o regime. A pergunta que interessa ao cliente não é se a reserva cobria as obrigações em uma data, mas se cobre sempre. Por isso o desenho maduro combina a prova datada com a conciliação contemporânea: a comparação diária entre ativos custodiados e obrigações registradas, guardada de forma íntegra, que transforma a prova bienal em consequência natural da rotina. É também a ponte para o relatório de controles sob NBC TO 3402, que conclui sobre o funcionamento dos controles ao longo do período, e não apenas sobre uma data.

O resumo da seção cabe em três exigências. Corte ancorado em bloco de referência, documentado, aplicado igualmente a ativos e passivos. Vizinhança temporal examinada, para expor reforços de ocasião. E rotina de conciliação que dê ao instante da prova o contexto do período. Sem as três, a janela temporal é a porta pela qual uma prova tecnicamente elegante deixa de provar qualquer coisa.

PARTE III

III

Da demonstração à *evidência*.

O que o exame independente aproveita, o que descarta e onde a prova pode ser burlada.

08 Evidência on-chain

09 Cotação, conversão e agregação

10 Limitações e formas de burlar

11 Prova de reservas sob NBC TO 3000

Evidência *on-chain* como evidência de exame.



A prova de reservas é assegurável porque parte da evidência é criptográfica e verificável de forma independente. Isso muda a natureza do teste em relação a uma auditoria tradicional: o examinador não depende de um extrato emitido pela administração para conhecer o saldo, porque consegue ler a cadeia diretamente. Mas não elimina o julgamento. Evidência on-chain responde o que existe; não responde de quem é, nem se o conjunto está completo.

O valor da evidência on-chain vem de três propriedades. É **independente**: o registro em cadeia não é produzido nem alterável pela entidade examinada, o que o coloca entre as fontes de maior confiabilidade que um examinador pode ter. É **permanente**: a movimentação histórica fica registrada, o que permite examinar a vizinhança temporal do corte e a persistência do controle. E é **reexecutável**: qualquer verificação pode ser refeita por terceiros, o que serve tanto ao assegurado quanto ao público que lerá o relatório divulgado.

Essas propriedades não dispensam disciplina de documentação. A leitura da cadeia precisa virar papel de trabalho: quais endereços foram consultados, em qual bloco de referência, com qual resultado, por qual ferramenta. A assinatura de mensagem precisa ser arquivada com o texto assinado, a data e o método de verificação. A confirmação do custodiante precisa ser obtida diretamente pelo examinador, não repassada pela administração. Evidência que não deixa trilha reconstruível não sustenta conclusão, por mais elegante que seja a criptografia por trás dela.

ELEMENTO DE EVIDÊNCIA	FONTE	O QUE O EXAMINADOR FAZ
Saldos on-chain	Registro público em cadeia, no bloco de referência	Consulta direta e independente; registro do bloco e da ferramenta
Prova de controle da chave	Assinatura de mensagem ou movimentação-teste	Verifica a assinatura contra o endereço; arquiva texto, data e método
Confirmação de custodiante	Custodiante qualificado, de forma independente	Obtém e avalia diretamente; concilia o extrato com a obrigação
Razão de obrigações	Registro auxiliar individualizado da prestadora	Concilia ao contábil e testa a completude contra fontes independentes
Reconciliação final	Todas as pontas, no mesmo corte	Reexecuta a comparação por ativo e documenta o tratamento das diferenças

A trilha que sustenta a *conclusão*

Organizada, a trilha de evidência de uma prova de reservas tem cinco elos. Primeiro, a lista de endereços próprios, fechada para o corte, com prova de controle de chave para cada um. Segundo, a extração on-chain dos saldos no corte definido, com registro do bloco de referência. Terceiro, as confirmações independentes dos custodiantes para os ativos em custódia qualificada. Quarto, o

razão de obrigações com clientes conciliado ao sistema de saldos, com teste de completude. Quinto, a reconciliação final por ativo, ligando reservas comprovadas a obrigações, com a cobertura resultante e o tratamento documentado de cada diferença.

CONTEMPORÂNEA VALE. RECONSTRUÍDA NÃO CONVENCE

Registro feito no momento do fato tem força probatória. Planilha montada na véspera do exame, para explicar o que teria acontecido meses antes, não tem. A trilha precisa nascer com a operação: conciliação diária guardada de forma íntegra, log imutável de acesso às chaves, decisão registrada no instante em que foi tomada. Reconstrução tardia é a origem mais comum de ressalva.

O fecho da seção é uma inversão útil. Em vez de perguntar que evidência a prova de reservas produz, pergunte que conclusão cada evidência sustenta. O saldo on-chain sustenta existência. A assinatura sustenta titularidade em um instante. A confirmação do custodiante sustenta a parcela delegada. O razão testado sustenta completude. Nenhuma peça sustenta a prova inteira: é o conjunto, amarrado no mesmo corte e documentado elo a elo, que transforma demonstração pública em evidência de exame.

Cotação, conversão e agregação.

A prova de reservas se comprova em quantidade e se comunica em valor. A conciliação técnica compara unidades do mesmo ativo: tanto devido, tanto custodiado. A leitura executiva e o relatório público, porém, precisam de uma moeda comum, e é na conversão e na agregação que se escondem dois riscos: a cotação mal escolhida e o consolidado que disfarça a falta localizada. Um exemplo numérico ilustrativo, com valores calculados apenas para demonstrar a mecânica, organiza a discussão.

Considere uma prestadora que custodia quatro ativos, identificados como Ativo A, B, C e D. Para cada um, comparam-se as obrigações com clientes e as reservas comprovadas, estas somando o saldo on-chain nas carteiras próprias controladas e os ativos em custódia qualificada. Primeiro, o quadro em quantidades.

ATIVO	OBRIGAÇÕES (QTD)	ON-CHAIN (QTD)	CUSTÓDIA (QTD)	RESERVA (QTD)	COBERTURA
Ativo A	1.250,00	900,00	350,00	1.250,00	100%
Ativo B	18.000,00	12.000,00	6.000,00	18.000,00	100%
Ativo C	42.000.000,00	30.000.000,00	12.000.000,00	42.000.000,00	100%
Ativo D	260.000,00	150.000,00	110.000,00	260.000,00	100%

Convertido a um preço de referência ilustrativo por ativo, o total das reservas soma R\$ 1.192.300.000,00 e iguala o total das obrigações, com cobertura consolidada de 100 por cento e diferença zero. É a fotografia íntegra que a prestadora quer levar à divulgação. A cotação usada na conversão precisa ser definida por critério documentado: fonte, horário compatível com o corte e tratamento uniforme entre ativos. Cotação escolhida a dedo, ou colhida em horário diferente do corte, introduz na prova um erro que nenhuma criptografia detecta.

Agora o cenário com falta. Suponha que, na verificação, a custódia comprovada do Ativo B seja de 5.100 unidades em vez de 6.000. A reserva do Ativo B cai de 18.000 para 17.100 unidades: uma falta de 900 unidades.

ATIVO	OBRIGAÇÕES (R\$)	RESERVA (R\$)	DIFERENÇA (R\$)	COBERTURA
Ativo A	425.000.000,00	425.000.000,00	0,00	100,00%
Ativo B	333.000.000,00	316.350.000,00	menos 16.650.000,00	95,00%
Ativo C	228.900.000,00	228.900.000,00	0,00	100,00%
Ativo D	205.400.000,00	205.400.000,00	0,00	100,00%
Total	1.192.300.000,00	1.175.650.000,00	menos 16.650.000,00	98,60%

cobertura consolidada = soma das reservas em valor ÷ soma das obrigações em valor

A conciliação técnica, note-se, acontece em quantidade: tanto devido, tanto custodiado, no mesmo ativo. A conversão em valor serve à leitura agregada e à comunicação, nunca substitui o teste por unidade. Essa ordem importa porque o preço flutua e a quantidade não: uma cobertura em valor pode melhorar de um dia para o outro sem que uma única unidade tenha entrado na carteira, apenas porque a cotação subiu. O critério de conversão documentado, com fonte definida, horário amarrado ao corte e tratamento uniforme entre ativos, impede que a variação de preço vire maquiagem de cobertura.

Diante da diferença, o assegurado isola o ativo e quantifica a falta em unidades e em valor. Rastreia a origem: chave não incluída, endereço não comprovado, custódia não confirmada pelo custodiante ou obrigação registrada a maior. Dá à

administração a oportunidade de corrigir: incluir a carteira faltante, obter a confirmação ou ajustar o registro. E reavalia. Se a diferença persiste, ela impacta a conclusão, que passa a apontar a exceção em vez de concluir por correspondência integral.

A DIFERENÇA NÃO SE ESCONDE NO TOTAL

Uma cobertura consolidada de 98,60 por cento pode parecer confortável, mas esconde um ativo a 95,00 por cento. O cliente do Ativo B não é protegido pela sobra dos demais: cada obrigação é devida no seu próprio ativo. Por isso a asseguração conclui ativo por ativo, além do consolidado. A régua é a correspondência em cada ativo.

Limitações e formas de *burlar*.

Uma prova de reservas bem construída é um controle poderoso. Uma prova de reservas mal lida é um instrumento de falsa segurança. Esta seção junta as duas pontas: o que a prova, por natureza, não alcança, e as formas conhecidas de burlá-la. Quem desenha a prova precisa fechar as brechas; quem lê o relatório precisa conhecer os limites do que está escrito.

Primeiro, os limites de natureza. A prova de reservas não é declaração de solvência da prestadora: ela trata da correspondência entre ativos custodiados e obrigações com clientes, e não das demais dívidas da instituição com terceiros, que vivem no balanço e são objeto da auditoria das demonstrações. É datada: vale para o corte examinado, não para o dia em que alguém a lê. E é limitada ao perímetro declarado: obrigações registradas fora do sistema que alimenta a prova, se existirem, escapam ao seu alcance e só são capturadas pelo teste de completude.

Segundo, as formas de burlar, que este guia examinou uma a uma e aqui organiza em quadro único, com a consequência e a defesa correspondente.

FORMA DE BURLAR OU ERRO	CONSEQUÊNCIA	DEFESA
Endereço emprestado no corte	Reserva inflada com ativo de terceiro	Persistência do controle, origem dos ativos e movimentação ao redor da data
Passivo omitido da árvore	Cobertura inflada pela redução do devido	Teste de completude do razão contra fontes independentes
Corte previsível ou reforçado	Foto não representativa do regime	Corte rigoroso, vizinhança examinada, conciliação contemporânea
Saldo sem prova de controle	Endereço de terceiro contado como reserva	Prova criptográfica de controle exclusivo para cada endereço
Cotação conveniente na conversão	Cobertura distorcida em valor	Critério documentado de fonte e horário, uniforme entre ativos
Conclusão só no consolidado	Falta localizada escondida no total	Cobertura calculada e concluída ativo por ativo
Ativo e passivo em cortes distintos	Comparação de datas diferentes, sem valor	Amarração de todas as pontas ao mesmo bloco de referência

O LIMITE DA LEITURA

Prova de reservas não é opinião sobre o balanço, não é garantia de que a custódia é inviolável e não é promessa sobre o futuro. É a demonstração, datada e delimitada, de que os ativos custodiados existiam, eram da prestadora e cobriam as obrigações com clientes no corte examinado. Ler mais do que isso no relatório é erro de quem lê; permitir que se leia mais é erro de quem escreve.

Autodeclaração não é *asseguração*

Resta a limitação mais comum na prática do mercado: a prova publicada sem exame independente. Uma página que exhibe endereços e uma raiz de Merkle, mantida pela própria plataforma, prova apenas o que a plataforma escolheu mostrar, na forma que escolheu mostrar. Sem terceiro que teste titularidade, complete o exame dos passivos e amarre o corte, a autodeclaração tem o valor de qualquer autodeclaração. O regime brasileiro fechou essa porta ao exigir asseguarção razoável com relatório público: o número da vitrine passou a precisar de um exame por trás.

Há, por fim, o limite do escopo temporal. A prova, mesmo assegurada, não conclui sobre os controles que mantêm a correspondência entre uma verificação e a seguinte: governança de chaves, alçadas de movimentação, limites de carteira conectada, conciliação diária. Esse é o objeto do relatório de controles sob NBC TO 3402, que olha o filme onde a prova olha a foto. A leitura completa do risco de custódia exige os dois documentos lado a lado: a prova dizendo que a cobertura existia no corte, o relatório de controles dizendo que os mecanismos que a preservam operaram no período.

A leitura construtiva das limitações é o mapa de desenho. Cada brecha conhecida corresponde a um controle que a fecha, e a Parte IV converte esse mapa em plano de implantação. Antes, porém, falta o instrumento que dá forma ao exame: a NBC TO 3000, o nível de segurança e a estrutura do relatório. É o assunto da próxima seção.

A prova sob a NBC TO 3000.

A NBC TO 3000, com a correspondente internacional ISAE 3000, é a norma que transforma a prova de reservas em trabalho de asseguaração: critérios definidos, evidência suficiente, procedimentos documentados e uma conclusão com nível de segurança declarado. Conhecer a norma serve a quem contrata, a quem prepara e a quem lê. E a primeira decisão que ela impõe é a escolha do nível: razoável ou limitada.

Na **segurança razoável**, o trabalho reúne evidência suficiente para reduzir o risco a um nível aceitavelmente baixo e permite conclusão em forma positiva: em nossa opinião, a prova de reservas está adequadamente apresentada. Exige mais procedimentos, mais teste de controles e mais evidência. Na **segurança limitada**, a evidência sustenta apenas conclusão em forma negativa: nada chegou ao nosso conhecimento que nos leve a crer que a prova não esteja adequadamente apresentada. Menos procedimentos, ênfase em indagação e análise, conforto menor.

DIMENSÃO	SEGURANÇA RAZOÁVEL	SEGURANÇA LIMITADA
Nível de conforto	Alto	Moderado
Forma da conclusão	Positiva	Negativa
Extensão dos procedimentos	Ampla, com teste de controles e de detalhe	Reduzida, com ênfase em indagação e análise
Risco de asseguaração	Reduzido a nível aceitavelmente baixo	Reduzido a nível aceitável, porém maior
Custo e prazo relativos	Maiores	Menores
Quando faz sentido	Divulgação pública de alto impacto, exposição relevante	Ciclos intermediários, conforto de gestão

Para a prova de reservas da PSAV, a escolha regulatória já está feita: a Resolução 520 exige asseguaração razoável, e a IN BCB 739 levou a mesma régua ao processo de autorização, exigindo relatório de asseguaração razoável emitido por auditor registrado na CVM. A régua sobe de forma concreta. Não basta receber os endereços da administração e checar saldos: o examinador testa a titularidade de forma independente, avalia a completude com procedimentos próprios, examina os controles que produzem a prova ao longo do período e documenta tudo em nível que sustente opinião positiva. Segurança limitada segue útil como verificação intermediária de gestão entre os ciclos, mas não substitui o trabalho exigido.

NÃO CONFUNDA OS TEXTOS

A conclusão de segurança limitada é redigida na forma negativa e não pode ser lida como se fosse uma opinião de segurança razoável. Tratar uma conclusão limitada como razoável superestima o conforto obtido. O relatório declara o nível de forma explícita exatamente por essa razão.

A estrutura do relatório

O relatório de asseguaração tem blocos definidos pela norma: título e destinatário, deixando claro que é relatório de asseguaração independente; identificação do objeto, a prova de reservas em uma data ou período e a afirmação da administração sobre a correspondência; os critérios contra os quais a prova é avaliada, incluindo a definição de reservas comprovadas e de obrigações com clientes; as responsabilidades de cada parte; o nível de segurança, declarado de forma inequívoca; o resumo do trabalho executado; e a conclusão, positiva na razoável, negativa na limitada. A conclusão pode ser sem exceção, quando a correspondência se comprova em cada ativo, ou com exceção, quando uma diferença como a do Ativo B do exemplo persiste após a oportunidade de correção.

Dois atributos completam o regime. A periodicidade da auditoria independente da prova de reservas é bienal, em calendário próprio, distinto do fechamento anual das demonstrações. E o relatório é divulgado publicamente: diferente de uma opinião

dirigida a sócios e administração, a conclusão alcança clientes e mercado, o que eleva a exigência de qualidade e de tempestividade da evidência.

COMO LER A CONCLUSÃO EM UM MINUTO

Identifique o nível: razoável dá opinião positiva, limitada dá conclusão negativa. Verifique se a conclusão alcança cada ativo, e não só o consolidado. Procure exceções nomeadas: um total alto não anula uma exceção localizada. E confira a data ou o período de referência, porque a prova de reservas é sempre datada.

PARTE IV

IV

Estruturar, responder e *implantar*.

O desenho auditável, as dúvidas mais comuns e o checklist de implantação.

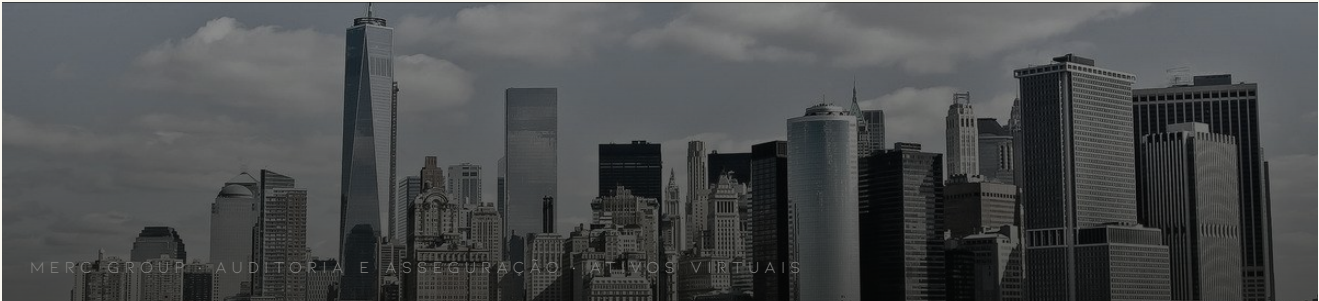
12 Estruturar uma prova auditável

13 Perguntas frequentes

14 Checklist

15 Próximos passos com a MERC

Estruturar uma prova *auditável*.



A qualidade da conclusão depende da qualidade da preparação. A administração é responsável pela prova de reservas e pelos controles; o assegurado conclui sobre o que a administração afirma. A prestadora que chega ao exame com a trilha pronta recebe um trabalho rápido e uma conclusão limpa. A que deixa para a véspera recebe pedidos que não consegue atender e exceções que não consegue corrigir. Esta seção organiza a preparação: papéis, sequência e rotina.

Primeiro, os papéis. Cada entregável da prova tem um dono e um circuito de aprovação, e quem executa não aprova a própria execução.

ENTREGÁVEL	ADMINISTRAÇÃO	CONTROLLER	ÁREA TÉCNICA	ASSEGURADOR
Afirmção sobre a prova de reservas	Responsável	Apoia	Apoia	Avalia
Lista de endereços próprios	Aprova	Revisa	Prepara	Testa
Prova de controle das chaves	Aprova	Revisa	Executa	Testa
Razão de obrigações com clientes	Aprova	Prepara	Apoia	Testa completude
Confirmações de custodiantes	Aprova	Solicita	Apoia	Obtém e avalia
Reconciliação por ativo	Aprova	Prepara	Apoia	Reexecuta
Documentação dos controles	Responsável	Prepara	Apoia	Avalia

Segundo, a sequência. Fechar a lista de endereços próprios e provar o controle de cada chave. Extrair os saldos on-chain no corte definido, com bloco de referência. Obter as confirmações dos custodiantes. Conciliar o razão de obrigações e testar a sua completude. Montar a reconciliação por ativo e calcular a cobertura. Só então o assegurado reexecuta e conclui. Inverter a ordem custa caro: reconciliar antes de fechar a lista de endereços, por exemplo, produz um número que muda no dia seguinte.

O QUE ATRASA O TRABALHO

Lista de endereços incompleta, chave sem prova de controle, confirmação de custodiante pendente e razão de obrigações sem teste de completude são as quatro pendências que mais atrasam a asseguuração. Todas são preparáveis com antecedência. Nenhuma se resolve na véspera da divulgação.

A prova vive na *rotina*

Terceiro, a rotina. O relatório é bienal, mas a evidência é diária. A prova de reservas testável é subproduto de uma conciliação contemporânea bem guardada: registro individualizado de obrigações por cliente conciliado diariamente, saldo de cada carteira verificável de forma independente, extrato de custodiante integrado à conciliação, diferenças tratadas com responsável e prazo, e

histórico guardado de forma íntegra para o ciclo. A instituição que só pensa na prova quando o examinador chega descobre, tarde, que faltam extratos, que a individualização não existe e que a diferença histórica nunca foi conciliada.

O calendário fecha a preparação. O ciclo bienal da prova de reservas convive com o fechamento anual das demonstrações e, quando contratado, com o período de cobertura do relatório de controles sob NBC TO 3402. Tratar os três como um cronograma único, com marcos compartilhados, evita o desgaste de produzir a mesma evidência três vezes em formatos diferentes: a conciliação diária que sustenta a prova é a mesma que alimenta o relatório de controles e a mesma que suporta a divulgação da obrigação de guarda nas notas explicativas. Evidência desenhada uma vez, usada três vezes.

Por fim, a sala de dados. Antecipe o pedido do examinador, que é previsível: inventário de carteiras com prova de controle, extrações on-chain com bloco de referência, confirmações de custodiantes, razão individualizado com teste de completude, conciliações do período, políticas aprovadas com data e atas do comitê. Sala de dados montada por frente, com evidência nomeada e organizada, encurta o campo do exame e reduz o custo do trabalho. Em agosto de 2026, com o protocolo de autorização correndo até 30/10/2026, essa antecipação deixou de ser boa prática e virou gestão de prazo.

Perguntas *frequentes.*

Respostas curtas às dúvidas que mais aparecem na decisão do CFO, no desenho da área técnica e na leitura do relatório. Cada resposta remete aos conceitos detalhados ao longo do guia.

Provar que a PSAV tem reservas é suficiente?

Não. Prova de reservas mostra apenas o lado do ativo. Sem prova de passivos, uma reserva de valor elevado pode ainda assim ser menor do que o total devido aos clientes, escondendo insolvência. A prova só fecha quando reserva e passivo são demonstrados juntos e a primeira cobre o segundo, ativo por ativo.

Como se prova a titularidade de um endereço on-chain?

Demonstrando controle sobre a chave privada. O método usual é a assinatura de mensagem: assina-se um texto de referência com a chave e verifica-se que a assinatura corresponde ao endereço, sem expor a chave. A alternativa é a movimentação-teste de valor combinado. A armadilha é o endereço emprestado apenas no momento do corte, que o exame combate analisando a persistência do controle e a movimentação ao redor da data.

Para que serve a árvore de Merkle na prova de passivos?

Ela permite que cada cliente verifique que o seu saldo foi incluído no total de obrigações, conferindo o caminho do seu valor até a raiz publicada, sem ver os saldos dos demais. Prova inclusão de quem confere, mas não prova que todos os clientes estão na árvore. A completude depende de teste adicional sobre o razão.

Por que a exigência é de asseguarção razoável, e não limitada?

Porque o regime quer opinião positiva, e não apenas ausência de indícios de erro. Asseguarção razoável obriga o examinador a obter evidência suficiente para reduzir o risco a nível baixo e afirmar que a informação está adequada em todos os aspectos relevantes. Combinada com a divulgação pública do relatório, eleva a régua da prova de reservas.

A auditoria das demonstrações cobre a prova de reservas?

Não. São trabalhos distintos, com objetos e normas distintos. A auditoria das demonstrações segue as NBC TA e trata do balanço da prestadora. A prova de reservas segue a NBC TO 3000 e trata dos ativos de clientes que estão fora do balanço. A prestadora precisa dos dois.

Com que frequência a prova de reservas é auditada, e o relatório é público?

A auditoria independente da prova de reservas tem periodicidade bienal, e o relatório é divulgado publicamente. Verificações intermediárias de gestão, inclusive com segurança limitada, podem ocorrer à parte, mas não substituem o ciclo exigido.

O que acontece se faltar reserva em um ativo?

O segurador isola o ativo, quantifica a diferença em unidades e em valor, rastreia a origem e dá à administração a oportunidade de corrigir. Se a diferença persiste, a conclusão aponta a exceção, como no exemplo ilustrativo do Ativo B, com cobertura de 95,00 por cento apesar de um consolidado de 98,60 por cento.

Custódia por terceiro tira a responsabilidade da prestadora?

Não. A responsabilidade pela guarda e pela segregação permanece com a prestadora autorizada no Brasil, mesmo quando a custódia técnica é delegada a custodiante, inclusive estrangeiro admitido sob condições. Os ativos delegados entram na prova por confirmação independente do custodiante, com extrato conciliável.

Uma prova publicada pela própria plataforma, sem exame, vale alguma coisa?

Vale como transparência voluntária, não como asseguração. Sem terceiro independente que teste titularidade, completude e corte, a autodeclaração prova o que a plataforma escolheu mostrar. O regime brasileiro exige o exame independente exatamente para fechar essa lacuna.

Quando começar a preparação?

Antes do protocolo e antes da data de referência da prova. Em agosto de 2026, o prazo final para protocolar o pedido de autorização é 30/10/2026, e a trilha de evidência não se reconstrói em semanas: individualização, conciliação diária e prova de controle de chaves são controles que precisam operar antes de serem examinados.

Checklist de *implantação.*

Lista de verificação para o CFO, o controller, a área de riscos e a área técnica, antes do desenho da prova e antes de cada ciclo de asseguarção. Marque cada item com evidência, não com intenção: item marcado sem documento que o comprove é um item aberto disfarçado de fechado.

DESENHO DA PROVA

- ✓ A prova de reservas está formalizada dentro da política de segregação patrimonial, com método descrito.
- ✓ A prova cobre os dois lados: reservas comprovadas e obrigações com clientes, ativo por ativo.
- ✓ O corte temporal é definido com rigor e ancorado em bloco de referência documentado.
- ✓ Ativo, passivo e raiz da árvore de Merkle são gerados sobre o mesmo corte.
- ✓ O critério de cotação para conversão em valor está documentado: fonte, horário e uniformidade.

TITULARIDADE E ENDEREÇOS

- ✓ A lista de endereços próprios está completa e fechada para o corte.
- ✓ Cada endereço tem prova criptográfica de controle: assinatura de mensagem ou movimentação-teste arquivada.
- ✓ Nenhum endereço com controle compartilhado ou não exclusivo é contado como reserva.
- ✓ As carteiras de clientes são distintas das carteiras próprias, com política de segregação demonstrável.
- ✓ A governança de chaves opera com segregação de funções, alçadas, assinatura múltipla e log imutável.
- ✓ O custodiante contratado tem confirmação independente, extrato conciliável e direito de acesso a registros.

PASSIVOS E COMPLETUDE

- ✓ O registro de obrigações é individualizado por cliente e por ativo, conciliado diariamente.
- ✓ A soma das contas individualizadas iguala a obrigação total de custódia e o saldo segregado.
- ✓ O razão de obrigações foi conciliado ao sistema operacional de saldos, com diferenças tratadas.
- ✓ A completude do razão foi testada contra fontes independentes do universo de clientes.
- ✓ A soma das folhas da árvore de Merkle bate com o total de obrigações do razão no corte.
- ✓ Os clientes têm acesso a ferramenta funcional de verificação do próprio saldo na árvore.

EVIDÊNCIA E CONCILIAÇÃO

- ✓ As extrações on-chain registram endereços, saldos, bloco de referência e ferramenta utilizada.
- ✓ A reconciliação por ativo está montada, com cobertura calculada ativo por ativo e no consolidado.
- ✓ Diferenças foram isoladas, quantificadas e endereçadas antes da data de referência.
- ✓ A movimentação ao redor do corte foi analisada em busca de reforços atípicos de reserva.
- ✓ O histórico de conciliações do período está guardado de forma íntegra e reconstruível.

RELATÓRIO E ASSEGUARÇÃO

- ✓ O escopo contratado nomeia o objeto e a norma: prova de reservas sob NBC TO 3000 e ISAE 3000.
- ✓ O nível de segurança está definido, com asseguarção razoável para o ciclo exigido.
- ✓ O relatório de controles sob NBC TO 3402 cobre o período e a interface com custodiantes.

- ✓ O calendário reserva o ciclo bienal da prova, distinto do fechamento anual das demonstrações.
- ✓ A trilha de evidência está pronta para divulgação pública, não apenas para uso interno.

Próximos passos com a *MERC*.

A MERC apoia PSAVs a transformar proof of reserves de exercício de vitrine em controle auditável. Como auditoria especializada no mercado financeiro brasileiro, aplicamos ao lastro on-chain o mesmo rigor de conciliação que aplicamos à custódia de recursos em instituições reguladas. O objetivo é simples: que a prestadora consiga demonstrar, a qualquer momento e a qualquer interessado, que as reservas existem, são suas e cobrem o que ela deve.

O trabalho se organiza em quatro frentes, na sequência em que a necessidade aparece.

- **Diagnóstico.** Avaliamos o desenho atual da prova: cobertura dos dois lados da conta, corte temporal, prova de titularidade, individualização das obrigações e trilha de evidência. O resultado é um mapa de lacunas priorizado contra as exigências da Resolução 520 e da IN BCB 739.
- **Prontidão.** Ajudamos a fechar as lacunas antes do exame: estruturação da prova de ativos por assinatura de mensagem ou movimentação-teste, prova de passivos a partir de um razão conciliável, árvore de Merkle com verificação acessível ao cliente, teste de completude e rotina de conciliação contemporânea.
- **Asseguração.** Conduzimos o trabalho de asseguração sob a NBC TO 3000, no nível razoável que a regulação exige, com a disciplina de evidência que a conclusão positiva requer e com a consciência de que o relatório será público.
- **Auditoria.** Executamos a auditoria das demonstrações financeiras da prestadora sob as NBC TA, com atenção à fronteira entre ativo próprio e ativo de cliente, em coordenação com o ciclo da prova de reservas.

POR QUE AGORA

O regime está em vigor desde 02/02/2026 e o prazo de protocolo corre até 30/10/2026. Individualização, conciliação diária e prova de controle de chaves não se reconstróem retroativamente: precisam operar antes de serem examinadas. Quanto antes o diagnóstico, maior a janela para corrigir com calma o que o exame encontraria tarde demais.

Se a prova de reservas da sua operação precisa virar evidência com valor de asseguração, comece por uma conversa técnica com os sócios da MERC. A conversa inicial mapeia o estágio da sua prova contra as quatro frentes acima e devolve uma visão objetiva de esforço e sequência: o que já sustenta exame, o que precisa de desenho e o que precisa apenas de disciplina de guarda. Este guia integra a Série Ativos Virtuais da MERC, que cobre o marco regulatório, a autorização, as demonstrações financeiras, a asseguração e os controles de custódia da prestadora. Fale conosco em www.mercgroup.com.br/contato ou por contato@mercgroup.com.br. Conteúdo técnico da Série Ativos Virtuais em www.mercgroup.com.br/insights.

Prova boa é a que resiste ao *exame*.

Quando a prova de reservas precisa virar evidência com valor de asseguarção, os sócios da MERC desenham o procedimento, testam a completude e conduzem o exame sob a NBC TO 3000.

CONTATO

contato@mercgroup.com.br

TELEFONE E WHATSAPP

+55 11 98196 1447

CONTEÚDO TÉCNICO

www.mercgroup.com.br/insights

ENDEREÇO

Av. Adolfo Pinheiro, 1001 · Alto da Boa Vista · São Paulo SP