Política de Guarda e Proteção de Chaves Privadas

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Sumário

1. Objetivo 2
2. Abrangência 2
3. Termos e Definições 3
4. Diretrizes Gerais 4
    4.1. Princípios 4
    4.2. Controle da Companhia e apoio de prestadores 5
5. Arquitetura e Guarda dos Instrumentos de Controle 6
    5.1. Arquitetura de carteiras e distribuição dos ativos 6
    5.2. Geração de chaves e cerimônias 7
    5.3. Módulos de segurança e técnicas criptográficas 7
    5.4. Armazenamento, fragmentação e redundância 8
6. Acessos e Autorização de Transações 9
    6.1. Concessão, alçadas e desativação de acessos 9
    6.2. Autorização e assinatura de transações 9
7. Ciclo de Vida, Conciliação e Ordens de Autoridades 10
    7.1. Rotação, reemissão e destruição 10
    7.2. Conciliação e demonstração de controle 10
    7.3. Ordens judiciais e medidas de indisponibilidade 10
8. Monitoramento, Incidentes e Pessoas 11
    8.1. Monitoramento, registros e testes 11
    8.2. Resposta a comprometimentos e continuidade 11
    8.3. Pessoas, treinamento e confidencialidade 12
    8.4. Vedações 12
9. Revisão 13
10. Normas de Referência 13
11. Vigência 14
12. Controle e Histórico de Versões 14

1. Objetivo

Esta Política estabelece as diretrizes da Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (a "Companhia") para a guarda e a proteção das chaves privadas e dos demais instrumentos de controle dos ativos virtuais de seus clientes e usuários, em cumprimento aos arts. 43, inciso VI, e 49 da Resolução BCB nº 520, de 10 de novembro de 2025, com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade desses instrumentos e, por consequência, a preservação dos ativos virtuais custodiados e o exercício dos direitos de seus titulares.

A Companhia é a custodiante dos ativos virtuais de seus clientes, e as disposições desta Política relativas à custódia, inclusive as que remetem aos arts. 9º e 73 a 84 da Resolução BCB nº 520/2025, aplicam-se integralmente. A tecnologia de apoio à custódia é contratada de provedor de serviço de tecnologia, na forma do art. 9º, §§ 6º e 7º, da mesma Resolução, sem transferência da custódia.

A guarda e o controle dos instrumentos que afetam o exercício dos direitos relacionados ao ativo virtual, a exemplo das chaves privadas, constituem o núcleo da atividade de custódia, na forma do art. 9º, inciso I, da Resolução BCB nº 520/2025. Por isso, esta Política parte de uma premissa: a Companhia deve ser capaz de, a qualquer tempo, assegurar que somente o titular, ou quem ele autorize, disponha dos ativos, executar tempestivamente as instruções recebidas e impedir qualquer movimentação não autorizada, inclusive quando se valer de tecnologia ou de apoio operacional de terceiros ou de integrantes do seu grupo econômico.

Esta Política é compatível com a Política de Segurança Cibernética da Companhia e a ela se integra, na forma do art. 49, § 4º, da Resolução BCB nº 520/2025, compondo o conjunto de documentos com que a Companhia comprova o atendimento das normas de segurança cibernética exigido pelo art. 88, inciso II, alínea "b", da mesma Resolução.

Esta Política estabelece o quê e o porquê. As especificações técnicas, os prazos de recuperação, os roteiros de cerimônia e os fluxos operacionais são estabelecidos no Procedimento de Custódia e Gestão de Chaves Privadas, que a detalha e a ela se subordina.

2. Abrangência

Aplica-se a todas as chaves privadas e aos demais instrumentos de controle, em qualquer formato, inclusive chaves integrais, fragmentos, frases-semente, credenciais de plataformas de custódia, dispositivos de assinatura e papéis administrativos de contratos inteligentes, relativos às

carteiras sob responsabilidade direta ou indireta da Companhia, em todas as redes e em todos os ativos virtuais que ela custodie ou opere.

Por força do art. 49, § 1º, da Resolução BCB nº 520/2025, a Política alcança obrigatoriamente as chaves privadas dos ativos virtuais mantidos em favor de clientes e usuários. Por decisão da Companhia, alcança também, com o mesmo padrão mínimo de proteção, as chaves das carteiras próprias e de tesouraria e as utilizadas no provimento de liquidez, observada a segregação entre ativos próprios e de clientes.

Aplica-se aos administradores, colaboradores, guardiões e prestadores de serviço, inclusive os integrantes do grupo econômico, que gerem, guardem, acessem, operem ou apoiem sistemas que interajam com esses instrumentos, bem como aos ambientes físicos e lógicos em que eles são gerados, armazenados ou utilizados.

3. Termos e Definições

Termo	Definição
Chave privada	Dado criptográfico secreto que permite assinar transações e, assim, dispor dos ativos virtuais associados a um endereço em rede baseada em registro distribuído.
Instrumentos de controle	Chaves privadas e quaisquer outros meios que afetem o exercício dos direitos relacionados ao ativo virtual, tais como fragmentos de chave, frases-semente, credenciais e dispositivos de assinatura, regras de aprovação configuradas em plataforma de custódia, delegações de código de carteiras, a exemplo do padrão EIP-7702, e papéis administrativos de contratos inteligentes.
Carteira quente	Carteira de ativos virtuais mantida constantemente conectada à rede mundial de computadores, nos termos do art. 2º, inciso VI, da Resolução BCB nº 520/2025.
Carteira morna	Carteira de ativos virtuais de categoria intermediária entre as carteiras fria e quente, mantida conectada à rede mundial de computadores com acréscimo de camadas de segurança, nos termos do art. 2º, inciso VII, da Resolução BCB nº 520/2025.
Carteira fria	Carteira de ativos virtuais que não está constantemente conectada à rede mundial de computadores (internet), nos termos do art. 2º, inciso V, da Resolução BCB nº 520/2025.

Termo	Definição
Módulo de segurança	Dispositivo ou ambiente computacional protegido, como o módulo de segurança de hardware (HSM) ou o enclave seguro, projetado para gerar, armazenar e utilizar chaves sem expô-las em texto claro.
Computação multipartidária (MPC)	Técnica criptográfica em que a chave é gerada e utilizada de forma distribuída entre múltiplas partes, sem que a chave integral exista, em qualquer momento, em um único local.
Assinatura múltipla (multisig)	Configuração em que a movimentação exige as assinaturas de um número mínimo de chaves independentes, verificado pela própria rede ou por contrato inteligente.
Compartilhamento de segredo	Técnica, como o esquema de Shamir, que divide um segredo em fragmentos, de modo que apenas um número mínimo deles permite reconstituí-lo.
Quórum (m-de-n)	Número mínimo de aprovações, assinaturas ou fragmentos (m), dentre o total existente (n), exigido para autorizar uma operação ou reconstituir um instrumento de controle.
Guardião	Pessoa formalmente designada para custodiar fragmento, dispositivo ou credencial e para participar de aprovações ou de cerimônias de chaves.
Cerimônia de chaves	Procedimento formal, roteirizado, testemunhado e registrado para a geração, o backup, a recuperação, a rotação ou a destruição de instrumentos de controle.
Comprometimento	Perda, divulgação ou acesso não autorizado a instrumento de controle, suspeita fundada de qualquer desses eventos, ou falha que impeça a sua utilização legítima.
Varredura (sweep)	Transferência dos ativos de um endereço existente para um endereço novo, sob controle da Companhia, como medida de rotação ou de contenção de comprometimento.

4. Diretrizes Gerais

4.1. Princípios

A guarda e a proteção dos instrumentos de controle observam os princípios abaixo, que orientam a interpretação desta Política e do Procedimento:

- **Controle pela Companhia:** a Companhia mantém, de forma permanente e demonstrável, a capacidade de autorizar, executar e impedir movimentações dos ativos custodiados.
- **Ausência de ponto único de falha:** nenhuma pessoa, dispositivo, local ou prestador é, isoladamente, suficiente para movimentar ativos de clientes fora das regras de assinatura aprovadas, ou para alterar essas regras, e a perda de qualquer deles não impede a recuperação dos ativos.
- **Segregação de funções e controle duplo:** quem solicita não aprova, quem aprova não executa isoladamente e quem opera não audita.
- **Menor privilégio:** os acessos são concedidos na estrita medida da necessidade funcional, por prazo determinado quando possível, e revistos periodicamente.
- **Minimização da exposição:** os saldos próprios e de tesouraria mantidos em ambiente conectado são os menores compatíveis com a liquidez necessária à operação.
- **Segregação patrimonial:** as carteiras de clientes são segregadas das carteiras próprias e de tesouraria, e os instrumentos de controle das carteiras próprias são incapazes de produzir qualquer efeito sobre as carteiras de clientes, na forma dos arts. 29, 30 e 78 da Resolução BCB nº 520/2025.
- **Rastreabilidade:** todo acesso, aprovação, assinatura e cerimônia é registrado de forma íntegra e auditável.

4.2. Controle da Companhia e apoio de prestadores

A Companhia pode utilizar tecnologia de custódia, módulos de segurança, plataformas de computação multipartidária e serviços operacionais contratados de terceiros ou de integrantes do seu grupo econômico, observado o Procedimento de Gestão de Fornecedores (KYP). A contratação de mecanismo ou de serviço tecnológico para a custódia só é admitida se o ofertante atestar, em documento específico, que o mecanismo ou serviço não lhe permite afetar, de qualquer maneira, a guarda e o controle dos instrumentos de controle, a descrição e a conciliação das posições, o atendimento das instruções de movimentação e o tratamento dos eventos incidentes sobre os ativos, nem o exercício dos direitos a eles relacionados, na forma do art. 9º, § 6º, da Resolução BCB nº 520/2025. A declaração abrange os contratos inteligentes fornecidos pelo ofertante aos quais as carteiras de clientes deleguem código.

Esses mecanismos e serviços são considerados relevantes para fins da Resolução BCB nº 520/2025 e sujeitam-se à regulamentação sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, na forma do art. 9º, § 7º, da mesma Resolução. Os contratos asseguram à Companhia acesso integral e tempestivo aos dados, registros e evidências necessários à conciliação, à auditoria, à supervisão e ao cumprimento de

ordens judiciais, bem como plano de saída que permita a migração dos instrumentos de controle sem interrupção da custódia, inclusive mediante a recuperação dos fragmentos a partir de backups sob controle da Companhia.

O apoio contratado é auxiliar. A configuração dos quóruns assegura que toda movimentação dependa da aprovação de pessoa autorizada da Companhia. As decisões sobre movimentações, parâmetros, exceções e resposta a comprometimentos permanecem com a Companhia.

Caso a Companhia contrate outra entidade, inclusive integrante do grupo ou constituída no exterior, para prestar o próprio serviço de custódia, e não apenas tecnologia de apoio, observa adicionalmente os arts. 74, 75, 83 e 84 da Resolução BCB nº 520/2025. Nessa hipótese, a Companhia avalia e monitora continuamente a política de custódia do custodiante, que deve ser compatível com esta Política e com a política de segurança cibernética da Companhia e mantida em língua portuguesa à disposição do Banco Central do Brasil; recebe e avalia seus testes de estresse e seus planos de segurança e de PLD/FT; verifica as condições do parágrafo único do art. 83, inclusive a autorização e a supervisão no país de constituição, o representante legal no Brasil e as garantias; e assegura cláusulas de monitoramento das posições, de acesso do Banco Central do Brasil, de segregação com eficácia jurídica plena e de carteiras específicas para os clientes do Brasil. A Companhia responde perante os clientes nos mesmos termos do custodiante contratado, na forma dos arts. 73, § 6º, inciso III, e 81, parágrafo único, da mesma Resolução.

5. Arquitetura e Guarda dos Instrumentos de Controle

5.1. Arquitetura de carteiras e distribuição dos ativos

Cada conta de cliente possui carteira própria associada, sem utilização de carteira coletiva (omnibus). As carteiras de clientes são operadas por computação multipartidária em ambiente conectado e classificam-se como carteiras quentes, nos termos do art. 2º, inciso VI, da Resolução BCB nº 520/2025. A Companhia não mantém, nesta data, carteiras mornas ou frias. A eventual distribuição dos ativos entre carteiras quentes, mornas e frias, de que trata o art. 49, inciso II, da mesma Resolução, depende de aprovação da Diretoria e de revisão desta Política e do contrato de custódia. O saldo das carteiras próprias e de tesouraria mantidas em ambiente conectado observa o limite. A Companhia não mantém ativos virtuais de sua titularidade nas carteiras de clientes, ressalvados os depósitos mínimos exigidos pela rede para a existência de contas de tokens, que observam o art. 30, §§ 2º a 4º, da Resolução BCB nº 520/2025. As taxas de rede das movimentações de clientes são pagas por carteira patrocinadora de taxas, de titularidade da Companhia, segregada das carteiras de clientes e sujeita aos limites e quóruns aplicáveis às carteiras de tesouraria e a limites de consumo monitorados.

As movimentações de carteiras próprias e de tesouraria dependem de aprovação em quórum e somente se destinam a endereços previamente cadastrados e controlados pela Companhia. As carteiras quentes contam com monitoramento contínuo e com bloqueio automático diante de padrões anômalos de movimentação.

A descrição das carteiras, dos métodos de guarda e da distribuição dos ativos entre elas integra o contrato de custódia e os termos de uso oferecidos aos clientes, na forma do art. 73, incisos III e V, da Resolução BCB nº 520/2025, em termos compatíveis com esta Política. Esses documentos informam os riscos de cada método de guarda e de cada estratégia de distribuição e colhem, de forma documentada, a decisão ou a concordância do cliente, na forma do § 1º do mesmo artigo.

A admissão de novo ativo virtual ou de nova rede depende de avaliação prévia, pela Custódia e pela Segurança da Informação, da capacidade de guarda segura dos respectivos instrumentos de controle, no âmbito da Política de Elegibilidade de Ativos Virtuais.

5.2. Geração de chaves e cerimônias

Os instrumentos de controle são gerados exclusivamente em módulo de segurança ou em protocolo de computação multipartidária aprovado, em ambiente controlado, com fonte de entropia validada e sem exposição da chave integral em texto claro fora do ambiente seguro. É vedada a geração em dispositivos pessoais, em ambientes não homologados ou por ferramentas não aprovadas.

A geração dos instrumentos de controle das carteiras próprias e de tesouraria, bem como os respectivos backups, recuperações, rotações e destruições, ocorre em cerimônia de chaves, conduzida segundo roteiro aprovado, com a presença de ao menos dois participantes autorizados e de testemunha independente da operação, registrada em ata e, quando cabível, em gravação, com validação dos endereços públicos resultantes antes de sua utilização. As carteiras de clientes são geradas pela plataforma de custódia, por meio de interface de programação, segundo regras aprovadas e com registro de cada geração.

5.3. Módulos de segurança e técnicas criptográficas

A Companhia utiliza técnicas criptográficas compatíveis com o valor custodiado e com o estado da técnica, documentados no Procedimento, na forma do art. 49, inciso III, da Resolução BCB nº 520/2025. A guarda dos instrumentos de controle é realizada por computação multipartidária (MPC), sem uso de módulo de segurança de hardware (HSM). Caso a Companhia venha a adotar HSM, os módulos possuem validação vigente segundo a norma FIPS 140-3, nível 3 ou superior, ou certificação reconhecida equivalente. Módulos cuja validação FIPS 140-2 tenha sido transferida

para a lista histórica não são adotados em novas contratações e contam com plano de substituição.

A solução de computação multipartidária adotada, e eventual solução de assinatura múltipla, devem oferecer garantia de segurança ao menos equivalente à desse padrão, com protocolo e implementação avaliados por terceiro independente. As atualizações de firmware, de software e de configuração dos módulos seguem o processo de gestão de mudanças, com aprovação e testes prévios.

5.4. Armazenamento, fragmentação e redundância

Os instrumentos de controle são armazenados segundo protocolos documentados de acesso, armazenamento e proteção, com uso de criptografia e de outras técnicas de segurança da informação, na forma do art. 49, § 2º, da Resolução BCB nº 520/2025.

Chaves múltiplas ou fragmentadas são armazenadas em locais diferentes, na forma do art. 49, § 3º, da Resolução BCB nº 520/2025, em quantidade e distribuição que assegurem, ao mesmo tempo, que nenhum local ou guardião permita, isoladamente, a movimentação dos ativos e que a perda de um local ou de um guardião não impeça a sua recuperação. Os backups dos fragmentos são criptografados com chave sob controle exclusivo da Companhia e mantidos em ao menos dois locais geograficamente distintos, de modo a permitir a recuperação dos instrumentos de controle independentemente do prestador.

A Companhia mantém, ainda, o mecanismo de redundância previsto no art. 76, inciso XII e § 1º, da Resolução BCB nº 520/2025, que contém todos os dados e informações dos clientes e os instrumentos de controle sobre os ativos virtuais, acompanhado de procedimentos de recuperação. O mecanismo é submetido às leis brasileiras, administrado por instituição ou entidade constituída no Brasil, ou por repositório tecnológico da própria Companhia, uma vez autorizada, na forma do § 2º do mesmo artigo, acessível ao Banco Central do Brasil e compatível com a política de segurança cibernética, inclusive quando a infraestrutura principal de custódia for operada por prestador no exterior. A entidade que o administrar é considerada contratação relevante, na forma do § 3º do mesmo artigo. Quando hospedado em nuvem no exterior, o mecanismo observa as condições da Resolução BCB nº 85/2021 para processamento e armazenamento de dados no exterior. O procedimento de recuperação é testado semestralmente.

Frases-semente, fragmentos e credenciais não são registrados em correio eletrônico, aplicativos de mensagem, armazenamento em nuvem de uso geral, fotografias ou qualquer outro meio não homologado. A Custódia mantém inventário atualizado dos instrumentos de controle, com sua localização, seus guardiões e as redes e carteiras a que se referem.

6. Acessos e Autorização de Transações

6.1. Concessão, alçadas e desativação de acessos

O acesso aos instrumentos de controle e aos sistemas de custódia é concedido formalmente, segundo regras e alçadas compatíveis com o grau de acesso e com os limites de responsabilidade de cada função, na forma do art. 49, incisos IV e VI, e do art. 48, incisos I e IV, da Resolução BCB nº 520/2025. O acesso exige autenticação multifator com dispositivo físico e é precedido, para os guardiões e para as funções com acesso a instrumentos de controle, de verificação de antecedentes justificada pela natureza da função, com base no art. 7º, inciso IX, da Lei nº 13.709/2018, segundo critérios definidos no Procedimento de Conheça seu Colaborador (KYE), e da assinatura de termo de confidencialidade específico.

Os acessos são revistos semestralmente, por área distinta da concedente, e revogados imediatamente em caso de desligamento, de mudança de função ou de suspeita de comprometimento. O desligamento ou a substituição de guardião enseja a reemissão ou a redistribuição dos fragmentos sob sua guarda ou, quando o guardião detiver apenas credenciais de aprovação, a revogação dessas credenciais, de modo que o antigo guardião não conserve qualquer capacidade de contribuir para o quórum.

6.2. Autorização e assinatura de transações

Toda movimentação de ativos de clientes ocorre somente mediante instrução do titular, ou de quem ele autorize, ou, independentemente de instrução, nas hipóteses de movimentação entre carteiras controladas pela Companhia sem alteração da titularidade dos ativos, de cumprimento de ordem judicial ou de demanda de autoridade competente e de transferência prevista na política de segregação patrimonial para os casos de interrupção ou descontinuidade dos serviços, e é autorizada segundo regras de assinatura configuradas no sistema de custódia, que aplicam limites, alçadas, quóruns, janelas de execução e listas de endereços. As movimentações de carteiras próprias e de tesouraria e as alterações de regras de assinatura, permissões e listas de endereços na plataforma de custódia exigem a aprovação de ao menos duas pessoas autorizadas, distintas do solicitante. A delegação de código em carteiras de clientes, a exemplo do padrão EIP-7702, restringe-se a contratos previamente aprovados pela Custódia e pela Segurança da Informação, e sua alteração depende do quórum.

O sistema de assinatura é integrado aos controles de PLD/FT, de sanções e de prevenção a fraudes. Nenhuma transação é assinada antes da triagem dos endereços de origem e de destino, na forma da Política de Sanções e Indisponibilidade de Ativos, e da aplicação dos limites e bloqueios temporários de que trata o art. 43, § 2º, inciso VI, da Resolução BCB nº 520/2025 e, a

partir de 1º de janeiro de 2027, da retenção cautelar prevista na Resolução BCB nº 584/2026. As transferências de ou para carteiras autocustodiadas que atinjam o valor de comunicação ao Coaf previsto no art. 49 da Circular BCB nº 3.978/2020, com a redação dada pela Resolução BCB nº 591/2026, são identificadas no fluxo de assinatura e encaminhadas à função de PLD/FTP, e as informações de originador e de beneficiário são tratadas na forma da regulamentação aplicável.

7. Ciclo de Vida, Conciliação e Ordens de Autoridades

7.1. Rotação, reemissão e destruição

As credenciais de acesso à plataforma de custódia e as chaves de contas de serviço têm períodos de validade definidos com base nas recomendações da publicação NIST SP 800-57. Os instrumentos de controle gerados por computação multipartidária não têm prazo fixo de validade e são rotacionados, com varredura dos ativos para novos endereços, na suspeita de comprometimento, no desligamento de guardião cuja participação não possa ser neutralizada por redistribuição, na substituição de módulo de segurança ou de prestador e sempre que a avaliação de risco o recomendar.

A destruição de instrumentos de controle ocorre somente após a confirmação de saldo nulo e da inexistência de operações pendentes nos endereços associados, em cerimônia, por método que impeça a sua recuperação, com registro em ata.

7.2. Conciliação e demonstração de controle

A Companhia concilia, diariamente e por área distinta da que executa as movimentações, as posições registradas de cada cliente com os saldos dos endereços nas respectivas redes, obtidos de fonte independente do prestador de tecnologia de custódia, na forma do art. 9º, inciso II, e do art. 76, inciso III, da Resolução BCB nº 520/2025, e trata as divergências como incidentes. A Custódia mantém a capacidade de demonstrar, por meios criptográficos verificáveis, o controle dos endereços que a Companhia declara deter, para fins de auditoria, de prova de reservas, segundo os métodos definidos na política de segregação patrimonial de que trata o art. 30, inciso II, da mesma Resolução, e de prestação de informações ao Banco Central do Brasil, inclusive as previstas no art. 88, inciso III, da Resolução BCB nº 520/2025, com a redação dada pela Resolução BCB nº 589/2026, e, quando aplicável, na Instrução Normativa BCB nº 713/2026.

7.3. Ordens judiciais e medidas de indisponibilidade

A Companhia não adota instrumentos de controle ou mecanismos de guarda que imponham obstáculos ao exercício de seus deveres nos termos do contrato de custódia ou ao imediato

atendimento de ordens judiciais ou de demandas de autoridades competentes aplicáveis aos ativos custodiados, na forma do art. 73, § 3º, da Resolução BCB nº 520/2025, nem ao cumprimento imediato de medidas de indisponibilidade de ativos. O Procedimento prevê rito específico para a execução de bloqueios e de transferências determinados por autoridade competente, com quóruns e guardiões disponíveis em prazo compatível com o fixado na ordem, observada a Política de Sanções e Indisponibilidade de Ativos.

8. Monitoramento, Incidentes e Pessoas

8.1. Monitoramento, registros e testes

A Companhia mantém monitoramento contínuo da segurança dos ambientes de custódia e de avaliação de riscos, com detecção e resposta a ameaças, na forma dos arts. 48, inciso II, e 50 da Resolução BCB nº 520/2025. Os registros de geração, acesso, aprovação, assinatura, cerimônia e alteração de configuração são imutáveis, sincronizados em horário e mantidos por, no mínimo, cinco anos, ou pelo prazo maior exigido pela regulamentação de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

Os sistemas, programas e contratos inteligentes utilizados na custódia são submetidos a análises de vulnerabilidades, a revisão por analistas independentes e a testes de robustez e de segurança, na forma do art. 48, inciso VIII, da Resolução BCB nº 520/2025, inclusive teste de intrusão anual. Os procedimentos de backup e de recuperação são testados semestralmente, com verificação da integridade dos fragmentos, e os resultados são reportados à Diretoria.

A Companhia realiza, ao menos anualmente, testes de estresse para avaliar a capacidade de seus sistemas de garantir a segurança dos ativos custodiados, com método e resultados documentados e arquivados por, no mínimo, cinco anos, na forma do art. 82 da Resolução BCB nº 520/2025, podendo contratar entidade de reconhecida capacidade técnica para esse fim.

8.2. Resposta a comprometimentos e continuidade

A Companhia mantém plano de resposta a comprometimento de instrumentos de controle, integrado ao Plano de Ação e de Resposta a Incidentes previsto na Política de Segurança Cibernética, na forma do art. 49, inciso V, da Resolução BCB nº 520/2025. Diante de comprometimento ou de sua suspeita fundada, a Companhia suspende imediatamente a utilização dos instrumentos afetados, avalia a exposição e, quando necessário, executa a varredura emergencial dos ativos para carteiras não afetadas.

O plano de continuidade de negócios, em conjunto com o Plano de Recuperação de Posições e de Controle de Ativos Virtuais e de Recursos de Clientes, fixa os prazos estimados para o reinício e a

recuperação da custódia e para as ações de comunicação, na forma do art. 43, § 4º, da Resolução BCB nº 520/2025. Os incidentes são registrados e comunicados ao Banco Central do Brasil, aos clientes afetados e às demais autoridades competentes na forma da regulamentação de segurança cibernética e de proteção de dados pessoais, e ao Coaf quando houver indício de lavagem de dinheiro ou de financiamento do terrorismo ou da proliferação.

8.3. Pessoas, treinamento e confidencialidade

Os colaboradores e guardiões com acesso a instrumentos de controle recebem treinamento específico, ao menos anual, no âmbito do programa de treinamento do Procedimento de Conheça seu Colaborador (KYE), na forma do art. 43, § 2º, inciso II, e do art. 48, incisos V e VII, da Resolução BCB nº 520/2025, firmam termo de confidencialidade específico e são submetidos a verificação de antecedentes na admissão e periodicamente, nos termos do item 6.1 e do Procedimento de Conheça seu Colaborador (KYE). As funções críticas são distribuídas de modo a evitar conflito de interesses e concentração de conhecimento, com substitutos designados e treinados.

8.4. Vedações

- Gerar, armazenar ou utilizar instrumento de controle fora de ambiente e de ferramenta homologados.
- Registrar frase-semente, fragmento ou credencial em meio não homologado, inclusive correio eletrônico, aplicativo de mensagem, armazenamento em nuvem de uso geral ou fotografia.
- Permitir que uma única pessoa, local, dispositivo ou prestador seja suficiente para movimentar ativos de clientes fora das regras de assinatura aprovadas, ou para alterar essas regras.
- Permitir que prestador, ainda que do grupo, atinja o quórum de movimentação ou altere regras de assinatura e de autenticação sem a aprovação de pessoa autorizada da Companhia.
- Compartilhar credenciais ou dispositivos de autenticação, ou concentrar na mesma pessoa as funções de solicitar, aprovar e executar movimentação.
- Assinar transação antes da conclusão da triagem e dos demais controles de PLD/FT, de sanções e de prevenção a fraudes aplicáveis.
- Manter saldo em carteira própria ou de tesouraria acima do limite aprovado, salvo exceção documentada e temporária.

- Manter mecanismo de guarda ou de controle que impeça ou retarde o cumprimento de ordem judicial autêntica, de demanda de autoridade competente ou de medida de indisponibilidade.
- Contratar, adotar ou utilizar mecanismo que dificulte a atuação das autoridades ou a detecção de crimes, a exemplo de misturadores ou embaralhadores, na forma do art. 90 da Resolução BCB nº 520/2025.
- Destruir instrumento de controle sem a confirmação de saldo nulo e sem cerimônia registrada.

9. Revisão

Esta Política é revista anualmente, e de forma extraordinária diante de alterações relevantes na regulamentação do Banco Central do Brasil, na arquitetura de custódia, nos módulos de segurança ou nos prestadores contratados, nas redes e nos ativos custodiados, após incidente de comprometimento ou diante de apontamento de auditoria ou da supervisão, com aprovação da Diretoria, formalizada em ata, após deliberação prévia do Comitê de Compliance.

10. Normas de Referência

- Lei nº 14.478, de 21 de dezembro de 2022, e Decreto nº 11.563, de 13 de junho de 2023.
- Resolução BCB nº 520, de 10 de novembro de 2025, em especial os arts. 9º, 29, 30, 43, 48 a 50, 73 a 84 e 90, e o art. 88, com as alterações da Resolução BCB nº 589/2026.
- Resolução BCB nº 85, de 8 de abril de 2021 (segurança cibernética e contratação de serviços de processamento e armazenamento de dados e de computação em nuvem), Resolução BCB nº 260/2022 (controles internos) e Resolução BCB nº 93/2021 (auditoria interna), aplicáveis por força da Resolução BCB nº 552/2026.
- Circular BCB nº 3.978, de 23 de janeiro de 2020, com a redação dada pela Resolução BCB nº 591/2026, e Resolução BCB nº 584/2026 (prevenção a fraudes).
- Lei nº 13.810, de 8 de março de 2019 (cumprimento de sanções do Conselho de Segurança das Nações Unidas e indisponibilidade de ativos).
- Resolução BCB nº 44, de 24 de novembro de 2020 (procedimentos para a execução, pelas instituições autorizadas a funcionar pelo Banco Central do Brasil, das medidas determinadas pela Lei nº 13.810/2019).

- Instrução Normativa BCB nº 713/2026, quando aplicável.
- Resolução CMN nº 5.280/2026 (sigilo bancário) e Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

11. Vigência

Esta Política tem caráter permanente e entra em vigor na data de sua aprovação pela Diretoria, com formalização em ata, após deliberação prévia do Comitê de Compliance. O conteúdo poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os colaboradores da Companhia e seus prestadores de serviço deverão consultar sempre a última versão disponível.

12. Controle e Histórico de Versões

Versão	Data	Histórico de Alterações/Inclusões	Resp. Aprovação
1.0	15/10/2026	Emissão inicial	Diretoria, após deliberação do Comitê de Compliance