

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Política de Segurança Cibernética

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Sumário

1. Objetivo	2
2. Abrangência	2
3. Termos e Definições	3
4. Objetivos de Segurança Cibernética	4
5. Procedimentos e Controles Mínimos	4
6. Medidas de Segurança Próprias da Atividade	8
7. Classificação de Dados e Relevância de Incidentes	9
8. Plano de Ação e de Resposta a Incidentes	10
9. Contratação de Serviços de Processamento, Armazenamento de Dados e de Computação em Nuvem	10
10. Serviços Relevantes	11
11. Procedimentos Prévios à Contratação	13
12. Contratação no Exterior	14
13. Cláusulas Contratuais Obrigatórias	15
14. Comunicação ao Banco Central do Brasil	17
15. Subcontratação	17
16. Monitoramento, Continuidade e Extinção	17
17. Recuperação de Posições e Rede do Sistema Financeiro Nacional	18
18. Vedações	19
19. Continuidade de Negócios na Interface Cibernética	19
20. Divulgação e Cultura de Segurança	20
21. Acompanhamento, Efetividade e Relatório Anual	21
22. Revisão	22
23. Normas de Referência	22
24. Vigência	22
25. Controle e Histórico de Versões	22

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

1. Objetivo

Esta Política estabelece os princípios, as diretrizes, os procedimentos e os controles de segurança cibernética da Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (sociedade PSAV), referida neste documento como Organização, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados na prestação de serviços de ativos virtuais.

A Organização presta serviços que envolvem a custódia e a movimentação de instrumentos de controle de ativos virtuais de terceiros, por meio de infraestrutura de carteiras contratada de prestador especializado, sob sua responsabilidade e governança. Nesse contexto, o comprometimento de um único mecanismo de assinatura criptográfica produz perda direta, imediata e, em regra, irreversível para o cliente. A segurança cibernética não é, aqui, função de suporte: é condição de exercício da atividade.

Fundamenta-se na Resolução BCB nº 85, de 8 de abril de 2021, cujo âmbito de aplicação foi estendido às sociedades prestadoras de serviços de ativos virtuais pela Resolução BCB nº 552, de 3 de março de 2026, e nos arts. 14, 32 a 43, 45, 48, 49, 50 e 51 da Resolução BCB nº 520, de 10 de novembro de 2025.

Esta Política incorpora, nas Seções 9 a 18 (o “Capítulo de Nuvem”), a política de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem exigida pelo Capítulo III da Resolução BCB nº 85/2021, anteriormente tratada em documento próprio, de modo que um único instrumento responde pelas duas exigências regulatórias.

2. Abrangência

Esta Política aplica-se a todos os dados, sistemas de informação, ativos de tecnologia, redes, ambientes de nuvem e instrumentos criptográficos sob responsabilidade da Organização, próprios ou operados por terceiros em seu nome, e a todos os administradores, funcionários, estagiários, prestadores de serviços e demais partes relacionadas que os acessem.

Aplica-se igualmente aos serviços relevantes contratados de terceiros, na forma do art. 33 da Resolução BCB nº 520/2025, hipótese em que a responsabilidade pela observância desta Política permanece integralmente com a Organização, nos termos dos arts. 36 e 51 da mesma Resolução.

A Organização não integra conglomerado prudencial. Não lhe é aplicável, por isso, a faculdade de adoção de política única de segurança cibernética prevista no art. 2º, § 2º, da Resolução BCB nº 85/2021. Padrões técnicos de outras sociedades do grupo podem ser adotados como referência,

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

mas não substituem esta Política nem a sua aprovação pelo órgão de administração da Organização.

3. Termos e Definições

Termo	Definição
Alta Direção	Diretoria da Organização.
Incidente	Evento que comprometa ou possa comprometer a confidencialidade, a integridade ou a disponibilidade dos dados ou dos sistemas de informação da Organização.
Incidente relevante	Incidente que atenda a pelo menos um dos parâmetros da Seção 7.2, ensejando registro, análise de causa e impacto, controle dos efeitos e as comunicações cabíveis.
Informação sensível	Dado ou informação classificado como Restrito ou Confidencial na forma da Seção 7.1, inclusive dado pessoal, informação sujeita a sigilo e instrumento de controle de ativo virtual.
Instrumento de controle de ativo virtual	Mecanismo de assinatura criptográfica que autentica transações com ativos virtuais, notadamente a chave privada, na forma do art. 2º, VIII, da Resolução BCB nº 520/2025.
Serviço relevante	Serviço cuja falha afeta o desempenho das atividades da Organização ou o pleno exercício dos direitos de cliente ou usuário, na forma do art. 33 da Resolução BCB nº 520/2025, incluídos os serviços de tecnologia relacionados à prestação de serviços de ativos virtuais.
Computação em nuvem	Disponibilidade à Organização, sob demanda e de maneira virtual, de recursos computacionais para implantação ou execução de softwares; de recursos para execução de aplicativos próprios; ou de aplicativos do próprio prestador executados por meio da internet, na forma do art. 13 da Resolução BCB nº 85/2021.
Convênio	Acordo para troca de informações entre o Banco Central do Brasil e a autoridade supervisora do país onde o serviço é prestado, exigido pelo art. 16, I, da Resolução BCB nº 85/2021.
Dossiê de contratação	Conjunto documental que reúne a diligência prévia, o contrato, as comunicações ao Banco Central do Brasil e os registros de monitoramento de cada prestador de serviço relevante.
Prestador	Instituição ou entidade contratada para a prestação de serviço relevante, no país ou no exterior.
Subcontratação	Contratação, pelo prestador, de terceiro para a execução de parte do serviço relevante prestado à Organização.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Termo	Definição
Situação de crise	Incidente relevante ou interrupção de serviço relevante que atenda aos critérios da Seção 19.3, ensejando comunicação tempestiva ao Banco Central do Brasil.
Teste de intrusão	Exercício controlado de exploração de vulnerabilidades, realizado com independência e imparcialidade, na forma do art. 22-A da Resolução BCB nº 85/2021.

4. Objetivos de Segurança Cibernética

São objetivos de segurança cibernética da Organização, na forma do art. 3º, I e § 1º, da Resolução BCB nº 85/2021:

- prevenir a ocorrência de incidentes, por meio de controles proporcionais ao porte, ao perfil de risco e ao modelo de negócio da Organização, à natureza das suas atividades e à sensibilidade dos dados sob sua responsabilidade;
- detectar tempestivamente incidentes e comportamentos atípicos, mediante monitoramento contínuo e rastreabilidade do processamento;
- reduzir a vulnerabilidade da Organização a incidentes relacionados com o ambiente cibernético, por meio de programa permanente de avaliação e correção de vulnerabilidades;
- responder a incidentes de forma estruturada, preservando a integridade dos ativos virtuais e dos recursos financeiros de clientes e usuários e a continuidade dos processos críticos de negócio; e
- assegurar que o comprometimento de qualquer componente isolado não seja suficiente para permitir a movimentação não autorizada de ativos virtuais de clientes e usuários.

O último objetivo é específico da atividade da Organização e prevalece, em caso de conflito de prioridades na resposta a incidente, sobre objetivos de disponibilidade.

5. Procedimentos e Controles Mínimos

Os procedimentos e controles adotados para reduzir a vulnerabilidade da Organização a incidentes abrangem, no mínimo, as famílias enumeradas no art. 3º, § 2º, da Resolução BCB nº 85/2021, detalhadas nesta Seção. Aplicam-se, inclusive, ao desenvolvimento de sistemas de informação seguros e à adoção de novas tecnologias, na forma do art. 3º, § 3º, e alcançam, no

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

que couber, os sistemas adquiridos ou desenvolvidos por terceiros e executados com recursos computacionais da Organização.

5.1. Autenticação e controles de acesso

O acesso à rede corporativa é limitado a usuários credenciados e a dispositivos autorizados. O acesso a partir de ambientes externos à Organização exige múltiplos fatores de autenticação, sem exceção.

As permissões de acesso são revistas periodicamente e de forma tempestiva, com atenção específica aos colaboradores terceirizados que acessem recursos computacionais da Organização. A revisão observa periodicidade mínima semestral para acessos privilegiados e sistemas críticos e anual para os demais, conforme a Norma de Gestão de Acessos, e é registrada com data, responsável e resultado.

A concessão de autorizações, a criação de senhas e os controles de acesso observam alçadas compatíveis com as responsabilidades de cada função, e estão sujeitos a mecanismo de desativação preventiva em situações suspeitas, na forma do art. 48, IV, da Resolução BCB nº 520/2025.

5.2. Criptografia, certificados e chaves

A Organização emprega criptografia na transmissão e no armazenamento de informações sensíveis, conforme os algoritmos e os parâmetros definidos na Política de Criptografia e Gestão de Chaves e no Padrão Técnico de Criptografia.

A gestão de certificados digitais compreende o monitoramento do uso de certificados e de assinaturas digitais com os mecanismos de rastreabilidade da Seção 5.5; os procedimentos de guarda, com controle de acesso físico e lógico às chaves privadas sob responsabilidade da Organização; as medidas destinadas a evitar o compartilhamento indevido dessas chaves; e a validação tempestiva de certificados revogados perante as autoridades certificadoras.

As chaves privadas de ativos virtuais de clientes e usuários observam, adicionalmente e com prevalência, o regime da Seção 6.2.

5.3. Proteção da rede e configuração segura

A rede é segmentada de modo a resguardar o ambiente de produção e os recursos computacionais que suportam processos críticos de negócio. São mantidos regras de firewall e monitoramento de conexões, critérios definidos para o estabelecimento e o monitoramento de conexões com ambientes externos, com atenção reforçada em horário noturno e em dias não

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

úteis, e medidas para identificar e prevenir conexões indevidas originadas de recursos tecnológicos da Organização, na forma da Norma de Configuração Segura e Segurança de Redes.

São mantidos processos e ferramentas para identificação, análise, tratamento e controle de eventos atípicos no ambiente de produção, abrangendo o estabelecimento de redes privadas virtuais e as tentativas de acesso privilegiado.

Os ativos de tecnologia observam perfis de configuração segura, definidos na Norma de Configuração Segura e Segurança de Redes, que preveem a gestão do ciclo de vida dos recursos computacionais, a aplicação regular de correções de segurança, a configuração adequada dos serviços suportados e a alteração de senhas e de outros padrões de fábrica.

5.4. Prevenção e detecção de intrusão, de software malicioso e de vazamento

A Organização mantém mecanismos de prevenção e detecção de intrusão, de proteção contra softwares maliciosos e de prevenção de vazamento de informações, com cobertura dos ambientes de produção, dos ambientes de nuvem e das estações de trabalho corporativas, e com tratamento registrado dos eventos identificados, na forma da Norma de Registro e Monitoramento de Eventos.

5.5. Rastreabilidade

A rastreabilidade abrange transações e operações e contempla, no mínimo, trilhas de auditoria do processamento fim a fim dos dados e das informações, incluída a definição e a geração de registros que possibilitem identificar falhas de processamento ou comportamentos atípicos e subsidiar análises; a definição de tempo de retenção conforme o tipo de processamento realizado; e a retenção segura das trilhas de auditoria, conforme a Norma de Registro e Monitoramento de Eventos.

A trilha de movimentação de ativos virtuais de clientes e usuários é retida por prazo não inferior a cinco anos, em observância ao art. 45, II, da Resolução BCB nº 520/2025.

5.6. Cópias de segurança

As cópias de segurança dos dados e das informações observam periodicidade, retenção e local de guarda definidos na Política de Backup e no Processo de Teste de Restauração de Backup, e são submetidas a testes de restauração com periodicidade mínima semestral. O resultado de cada teste é registrado, e a falha de restauração é tratada como incidente relevante.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.7. Gestão de vulnerabilidades e testes de intrusão

O programa de gestão de vulnerabilidades compreende testes e análises periódicos para detecção de vulnerabilidades em sistemas de informação; varreduras periódicas dos recursos tecnológicos com o objetivo de identificar dispositivos indevidamente conectados à rede corporativa; análises periódicas dos recursos tecnológicos; testes de intrusão; e a correção tempestiva das vulnerabilidades identificadas.

Os testes de intrusão têm periodicidade mínima anual e são realizados com independência e imparcialidade por pessoa natural ou empresa especializada contratada especificamente para essa finalidade, sem prejuízo da realização de testes por equipes da própria Organização. Os resultados são documentados, com identificação das vulnerabilidades e dos planos de ação estabelecidos para a sua correção.

Vedação de acumulação. O prestador contratado para desenhar ou implantar os controles desta Política não pode ser o mesmo contratado para a execução do teste de intrusão do caput, sob pena de comprometimento da independência e da imparcialidade exigidas pelo art. 22-A da Resolução BCB nº 85/2021.

5.8. Segurança no desenvolvimento e na adoção de novas tecnologias

O ciclo de desenvolvimento de sistemas contempla etapas de verificação de segurança anteriores à promoção ao ambiente de produção. A adoção de nova tecnologia é precedida de avaliação de segurança documentada, e a mesma verificação se aplica, no que couber, a sistemas adquiridos ou desenvolvidos por terceiros e executados com recursos computacionais da Organização.

Os contratos inteligentes que afetem o desempenho das atividades da Organização submetem-se a análise de vulnerabilidade, a revisão de desempenho por analistas independentes e a testes de robustez e de segurança, na forma do art. 48, VIII, da Resolução BCB nº 520/2025, previamente à sua utilização e a cada alteração relevante.

5.9. Integração por interfaces eletrônicas

A integração de sistemas de informação por meio de interfaces eletrônicas observa requisitos de segurança definidos na Norma de Configuração Segura e Segurança de Redes, aplicáveis a autenticação, autorização, limitação de requisições, registro e tratamento de erros. É mantido inventário das integrações, com indicação dos controles aplicados a cada interface.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.10. Inteligência no ambiente cibernético

A Organização mantém ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de seu interesse na internet, na Deep Web e na Dark Web e em grupos privados de comunicação, com atenção específica à exposição de credenciais, de endereços de carteiras e da marca da Organização. Os achados são tratados e, quando cabível, tipificados como incidente na forma da Seção 7.2.

6. Medidas de Segurança Próprias da Atividade

6.1. Ambiente computacional

As medidas e os procedimentos destinados a garantir a segurança, a resiliência e o adequado funcionamento do ambiente computacional que suporta a prestação de serviços de ativos virtuais, exigidos pelo art. 48 da Resolução BCB nº 520/2025, integram esta Política e observam as Seções 5.1 a 5.10.

São adotadas medidas preventivas específicas para a mitigação de incidentes cibernéticos nas operações que envolvam operadores do segmento de finanças descentralizadas, incluída a avaliação prévia do protocolo, dos contratos inteligentes envolvidos e do histórico de comprometimento da rede.

6.2. Guarda e proteção dos instrumentos de controle dos ativos virtuais

A geração, a custódia e o gerenciamento dos instrumentos de controle dos ativos virtuais de clientes e usuários observam procedimentos documentados, com especificação dos métodos e das técnicas empregados na execução das transações, na forma do art. 49 da Resolução BCB nº 520/2025.

A infraestrutura de geração, guarda e uso das chaves de ativos virtuais de clientes e usuários é contratada de prestador de serviço relevante especializado, sujeito ao Capítulo de Nuvem (Seções 9 a 18). As políticas de assinatura, as alçadas, o quórum e a concessão e a desativação dos instrumentos de controle permanecem sob definição e governança da Organização, e a responsabilidade perante clientes, usuários e o Banco Central do Brasil não se transfere ao prestador.

Os ativos virtuais de clientes e usuários são mantidos em carteiras segregadas dos ativos próprios da Organização, com identificação individualizada e conciliação periódica entre os registros internos e os saldos verificados em cadeia, na forma da Resolução BCB nº 520/2025.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Os procedimentos de geração, guarda, acesso, autorização de transações, rotação e destruição dos instrumentos de controle, a arquitetura de carteiras e a distribuição dos ativos entre elas, os quóruns e as medidas de mitigação de comprometimento constam da Política de Guarda e Proteção de Chaves Privadas, que se integra a esta Política na forma do art. 49, § 4º, da Resolução BCB nº 520/2025.

Adotadas chaves privadas múltiplas ou segmentadas, os fragmentos são armazenados em locais diferentes. Nenhum indivíduo, isoladamente, detém capacidade de movimentar ativos virtuais de clientes e usuários.

Cada exercício do poder de assinatura é registrado com data, hora, motivo, detentores participantes e quórum observado, e a trilha correspondente é retida na forma da Seção 5.5.

6.3. Segurança institucional

A Organização mantém mecanismos de monitoramento contínuo da segurança institucional e de avaliação de riscos, com o objetivo de detectar, prevenir e responder a ameaças e incidentes, na forma do art. 50 da Resolução BCB nº 520/2025. A segurança institucional compreende, além do ambiente cibernético, a segurança física das instalações e do pessoal, e é objeto de política própria à qual esta se articula (Política de Segurança Física).

7. Classificação de Dados e Relevância de Incidentes

7.1. Classificação dos dados e das informações

Os dados e as informações são classificados quanto à relevância nas categorias Público, Uso Interno, Confidencial e Restrito, na forma da Norma de Gestão da Informação. A classificação determina os controles de acesso, de transmissão, de armazenamento e de descarte aplicáveis, e orienta a avaliação de relevância dos serviços a serem contratados, na forma do art. 12, § 1º, da Resolução BCB nº 85/2021.

Instrumentos de controle de ativos virtuais são classificados, em qualquer hipótese, como Restrito; dados sujeitos a sigilo são classificados, no mínimo, como Confidencial, na forma da Norma de Gestão da Informação.

7.2. Parâmetros de relevância do incidente

É relevante o incidente que atenda a pelo menos um dos seguintes parâmetros:

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

- comprometimento, efetivo ou potencial, de instrumento de controle de ativo virtual, independentemente do valor envolvido;
- acesso não autorizado, exfiltração ou alteração de informação classificada como Restrito ou Confidencial;
- **indisponibilidade de processo crítico de negócio por período superior ao prazo estipulado para o seu reinício (RTO), aprovado na forma da Política de Continuidade de Negócios;**
- movimentação de ativo virtual ou de recurso financeiro de cliente ou usuário sem instrução válida;
- comprometimento de prestador de serviço relevante com reflexo sobre dados, ativos ou serviços da Organização; e
- qualquer evento que enseje comunicação a autoridade, a cliente ou a usuário por força de lei ou de regulamento.

O incidente relevante é registrado, tem a sua causa e o seu impacto analisados e os seus efeitos controlados, abrangendo inclusive as informações recebidas de empresas prestadoras de serviços a terceiros, na forma do art. 3º, IV e § 4º, da Resolução BCB nº 85/2021.

8. Plano de Ação e de Resposta a Incidentes

A implementação desta Política é operacionalizada pelo Plano de Ação e de Resposta a Incidentes, documento apartado, aprovado pela Diretoria, com formalização em ata, após deliberação prévia do Comitê de Compliance, que abrange, no mínimo, as ações destinadas a adequar as estruturas organizacional e operacional da Organização aos princípios e às diretrizes desta Política; as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes; e a área responsável pelo registro e pelo controle dos efeitos de incidentes relevantes.

O Plano contempla roteiros de resposta por tipo de incidente e é compatível com os planos de recuperação das posições e de controle dos ativos virtuais e dos recursos financeiros de clientes e usuários exigidos pelo art. 34, II, da Resolução BCB nº 520/2025.

9. Contratação de Serviços de Processamento, Armazenamento de Dados e de Computação em Nuvem

As empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das atividades operacionais da Organização,

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

observam procedimentos e controles de prevenção e tratamento de incidentes em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria Organização.

As Seções 9 a 18 estabelecem os critérios, os procedimentos e as condições contratuais que a Organização observa na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, com fundamento no Capítulo III e no art. 22-B da Resolução BCB nº 85/2021 e nos arts. 32 a 42 e 51 da Resolução BCB nº 520/2025.

A Organização opera sobre infraestrutura de terceiros. A consequência regulatória disso é que parte substancial dos seus controles é exercida por meio de contrato, e não de configuração própria. Cláusula ausente ou mal redigida é, aqui, deficiência de controle, e não questão comercial.

A responsabilidade da Organização pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo dos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação, não se transfere ao contratado em nenhuma hipótese.

O Capítulo de Nuvem aplica-se à contratação, à alteração, ao monitoramento e à extinção de contratos de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, celebrados no país ou no exterior, com prestadores integrantes ou não do grupo econômico da Organização.

A contratação de serviço relevante junto a sociedade integrante do grupo não afasta nenhuma exigência deste Capítulo. O contrato intragrupo observa as mesmas cláusulas obrigatórias da Seção 13 e a mesma diligência prévia da Seção 11.

O Capítulo não se aplica à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado, na forma do art. 18 da Resolução BCB nº 85/2021.

Os fornecedores que não se enquadrem como prestadores de serviços relevantes observam a Norma de Segurança em Fornecedores.

10. Serviços Relevantes

10.1. Critério de relevância

É relevante o serviço que afeta o desempenho das atividades da Organização ou que afeta, ou pode afetar, o pleno exercício dos direitos de cliente ou usuário. Na avaliação da relevância, consideram-se a criticidade do serviço e a sensibilidade dos dados e das informações a serem

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

processados, armazenados e gerenciados pelo contratado, levada em conta a classificação de dados da Seção 7.1 desta Política.

São relevantes, entre outros, os serviços de infraestrutura de carteiras e de custódia de ativos virtuais; de provimento de liquidez para as operações no mercado de ativos virtuais; de formação de mercado; de emissão de moeda eletrônica e de oferta de conta de pagamento ou de depósito; e os serviços de tecnologia especificamente relacionados à prestação de serviços de ativos virtuais.

Os serviços de tecnologia referidos acima são considerados relevantes também para fins de aplicação da regulamentação sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, na forma do art. 33, § 2º, da Resolução BCB nº 520/2025. A qualificação não é discricionária: verificado o enquadramento, o serviço submete-se integralmente a esta Política.

10.2. Rol de serviços relevantes

A Organização mantém rol nominal e versionado dos contratos qualificados como relevantes, com indicação do prestador, do objeto, da hipótese de computação em nuvem aplicável nos termos da Seção 10.3, dos países e regiões de processamento e armazenamento, da data da comunicação ao Banco Central do Brasil e da existência de subcontratação notificada.

O rol vigente é mantido como registro desta Política, no índice de evidências regulatórias da Compliance, e não integra o texto desta Política.

O rol é mantido pela Compliance, com apoio da Segurança da Informação e da Tecnologia, e atualizado a cada contratação, alteração ou extinção. A operação de serviço relevante ausente do rol é evento reportável.

10.3. Hipóteses de computação em nuvem

Cada contrato é classificado em uma das seguintes hipóteses: disponibilização de processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à Organização implantar ou executar softwares; implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Organização com recursos computacionais do prestador; ou execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador com recursos computacionais dele próprio.

Na terceira hipótese, a Organização assegura que o prestador adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

11. Procedimentos Prévios à Contratação

11.1. Governança proporcional

A contratação de serviço relevante é precedida da adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que a Organização esteja exposta. Os critérios de decisão quanto à terceirização integram as políticas, estratégias e estruturas de gerenciamento de riscos da Organização e alcançam expressamente a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país e no exterior.

11.2. Verificação da capacidade do prestador

Previamente à contratação, a Organização verifica a capacidade do potencial prestador de assegurar:

- o cumprimento da legislação e da regulamentação em vigor;
- o acesso da Organização aos dados e às informações a serem processados ou armazenados;
- a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados;
- a sua aderência às certificações exigidas pela Organização para a prestação do serviço;
- o acesso da Organização aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e controles utilizados na prestação dos serviços;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços;
- a identificação e a segregação dos dados dos clientes e dos usuários finais da Organização por meio de controles físicos ou lógicos; e
- a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes e dos usuários finais.

A verificação abrange, adicionalmente, a capacidade técnica e operacional do prestador e o seu histórico de cumprimento normativo, na forma do art. 34, I, da Resolução BCB nº 520/2025, e o estabelecimento, em conjunto com o prestador, de controles internos que permitam o monitoramento e a identificação de listas de sanções e de endereços de carteiras de ativos virtuais sancionadas, no país ou no exterior.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

11.3. Documentação

Os procedimentos desta Seção, inclusive as informações relativas à verificação da Seção 11.2, são documentados e reunidos no dossiê de contratação do prestador, que permanece à disposição do Banco Central do Brasil.

11.4. Competências internas

A Organização mantém recursos e competências necessários à adequada gestão dos serviços contratados, inclusive para a análise das informações e o uso dos recursos de monitoramento providos pelo prestador. A ausência de competência interna para interpretar os relatórios e os recursos de gestão disponibilizados equivale, para os fins desta Política, à ausência de monitoramento.

12. Contratação no Exterior

12.1. Requisitos

A contratação de serviços relevantes prestados no exterior observa a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados; a garantia de que a prestação não causará prejuízo ao regular funcionamento da Organização nem embaraço à atuação do Banco Central do Brasil; a definição prévia dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e a previsão de alternativas para a continuidade dos negócios no caso de impossibilidade de manutenção ou de extinção do contrato.

A Organização assegura que a legislação e a regulamentação dos países e das regiões indicados não restringem nem impedem o acesso da Organização e do Banco Central do Brasil aos dados e às informações. A comprovação do atendimento a estes requisitos é documentada.

A existência de convênio e o atendimento aos demais requisitos desta Seção para cada jurisdição constante do rol de serviços relevantes são verificados e documentados no dossiê de contratação de cada prestador, antes do protocolo do pedido de autorização e a cada alteração de prestador, de serviço ou de região.

12.2. Ausência de convênio

Inexistindo convênio, a contratação depende de autorização prévia do Banco Central do Brasil, solicitada com antecedência mínima de sessenta dias em relação à data pretendida para a

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

contratação. O mesmo prazo mínimo aplica-se às alterações contratuais que impliquem modificação da denominação do contratado, dos serviços relevantes contratados ou dos países e regiões indicados.

Efeito sobre o cronograma. O prazo de sessenta dias é anterior à contratação, e não posterior. Toda contratação relevante em jurisdição sem convênio, inclusive a migração de contrato já vigente para nova região, deve ser identificada no planejamento com antecedência suficiente. O mapeamento de jurisdições da Seção 10.2 é, por isso, condição de exequibilidade desta Política, e não documento acessório.

12.3. Alteração de países e regiões

A alteração dos países ou das regiões de processamento, armazenamento e gerenciamento de dados, ainda que promovida unilateralmente pelo prestador, sujeita-se aos requisitos desta Seção. O contrato prevê a obrigação de notificação prévia da alteração pelo prestador, em prazo compatível com o cumprimento das exigências regulatórias pela Organização.

13. Cláusulas Contratuais Obrigatórias

13.1. Cláusulas gerais

Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem contêm cláusulas dispondo sobre:

- a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- a adoção de medidas de segurança para a transmissão e o armazenamento desses dados;
- a manutenção, enquanto vigente o contrato, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes e dos usuários finais;
- a obrigatoriedade, em caso de extinção do contrato, de transferência dos dados ao novo prestador ou à Organização e de exclusão dos dados pela contratada substituída, após a transferência e a confirmação da integridade e da disponibilidade dos dados recebidos;
- o acesso da Organização às informações fornecidas pelo prestador para verificar o cumprimento dos itens anteriores, às informações relativas às certificações e aos relatórios de auditoria especializada, e às informações e recursos de gestão adequados ao monitoramento dos serviços;

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

- a obrigação de o prestador notificar a Organização sobre a subcontratação de serviços relevantes;
- a permissão de acesso do Banco Central do Brasil aos contratos e acordos firmados, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações e aos códigos de acesso;
- a adoção de medidas pela Organização em decorrência de determinação do Banco Central do Brasil; e
- a obrigação de o prestador manter a Organização permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Os contratos preveem, ainda, que o prestador atua por conta e sob as diretrizes da Organização, e que a Organização permanece responsável pelos serviços prestados aos clientes, usuários e demais instituições do mercado de ativos virtuais por meio da entidade contratada.

13.2. Regime de resolução

Para a hipótese de decretação de regime de resolução da Organização pelo Banco Central do Brasil, os contratos preveem a obrigação de o prestador conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança e aos códigos de acesso que estejam em seu poder.

Preveem, igualmente, a obrigação de notificação prévia ao responsável pelo regime de resolução sobre a intenção de interromper a prestação de serviços, com pelo menos trinta dias de antecedência, obrigando-se o prestador a aceitar eventual pedido de prazo adicional de trinta dias formulado pelo responsável, inclusive quando a interrupção for motivada por inadimplência da Organização.

13.3. Acesso do supervisor e informação a clientes

Os contratos de prestação de serviços relevantes preveem que o prestador forneça as informações e os documentos necessários ao desempenho das atribuições de supervisão do Banco Central do Brasil e permita o acesso da autarquia à documentação, às informações referentes aos produtos e serviços fornecidos e às suas dependências, na forma do art. 40 da Resolução BCB nº 520/2025.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

A Organização oferece a clientes, usuários e demais contrapartes negociais informações claras e transparentes sobre o envolvimento de outras instituições ou entidades contratadas na prestação dos serviços relevantes, destacando as contratações que possam representar riscos e indicando as formas de mitigação, resguardados o sigilo das informações confidenciais e os dados comercialmente sensíveis.

14. Comunicação ao Banco Central do Brasil

A contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem é comunicada ao Banco Central do Brasil em até dez dias após a contratação, com indicação da denominação da empresa contratada, dos serviços relevantes contratados e, no caso de contratação no exterior, dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados armazenados, processados e gerenciados.

As alterações contratuais que impliquem modificação dessas informações são comunicadas em até dez dias após a alteração contratual.

A Compliance mantém controle de prazos das comunicações desta Seção. O descumprimento do prazo é evento reportável à Diretoria, independentemente de o serviço permanecer em operação regular.

15. Subcontratação

A notificação de subcontratação de serviços relevantes recebida do prestador é registrada no dossiê de contratação e considerada na definição dos mecanismos de acompanhamento e de controle da Organização.

A subcontratação não altera a responsabilidade do prestador perante a Organização nem a responsabilidade da Organização perante os seus clientes, usuários e o Banco Central do Brasil. Verificado que a subcontratação implica processamento ou armazenamento de dados em país ou região não indicados no contrato, aplica-se a Seção 12.3.

16. Monitoramento, Continuidade e Extinção

16.1. Monitoramento contínuo

A Organização averigua continuamente as capacidades técnica e operacional do prestador e monitora, de forma contínua, o seu desempenho, com base nas informações e nos recursos de

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

gestão disponibilizados, nos relatórios de auditoria especializada independente e nas certificações mantidas.

O monitoramento observa periodicidade mínima anual e, para os prestadores que suportam a custódia de ativos virtuais ou o ambiente de produção, semestral, e é registrado com data, responsável, informações analisadas e conclusão.

16.2. Continuidade e substituição

Para cada serviço relevante, a Organização mantém alternativa de continuidade que contemple a substituição do prestador e o restabelecimento da operação normal, com prazo estimado de reinício compatível com os prazos definidos na Análise de Impacto no Negócio (BIA), na forma da Política de Continuidade de Negócios e da Seção 19 desta Política.

A interrupção de serviço relevante é tratada como incidente e, atendidos os critérios aplicáveis, como situação de crise, com comunicação tempestiva ao Banco Central do Brasil.

16.3. Extinção e devolução de dados

Na extinção do contrato, a Organização assegura a transferência dos dados ao novo prestador ou a si própria e a exclusão dos dados pela contratada substituída, após a transferência e a confirmação da integridade e da disponibilidade dos dados recebidos. A confirmação é documentada e integra o dossiê de contratação.

17. Recuperação de Posições e Rede do Sistema Financeiro Nacional

A Organização elabora e mantém atualizados planos robustos de recuperação das posições e de controle dos ativos virtuais e dos recursos financeiros dos clientes e usuários, aplicáveis a incidentes que afetem esses ativos e recursos e que envolvam a instituição ou entidade contratada.

Esses planos são compatíveis com o Plano de Ação e de Resposta a Incidentes e com as demais Seções desta Política, e são submetidos a teste que contemple cenário de indisponibilidade de prestador de serviço relevante.

O serviço prestado para a comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional, quando aplicável à Organização, é considerado relevante para fins desta Política, independentemente da forma de conexão, inclusive nos casos em que o prestador forneça serviço de processamento de mensagens no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

18. Vedações

É vedado à Organização:

- **iniciar a operação de serviço relevante antes de concluída a diligência prévia da Seção 11 e formalizado o contrato com as cláusulas da Seção 13;**
- **contratar serviço relevante prestado no exterior em jurisdição sem convênio sem a autorização prévia da Seção 12.2;**
- celebrar contrato de serviço relevante que não contenha cláusula vedando à instituição ou entidade contratada a cobrança dos clientes e usuários da Organização, sob a forma de tarifas, comissões ou valores de ressarcimento, por serviços prestados no fornecimento de produtos ou serviços de responsabilidade da própria contratada, na forma do art. 37 da Resolução BCB nº 520/2025;
- aceitar cláusula que restrinja o acesso da Organização ou do Banco Central do Brasil aos dados, às informações, às cópias de segurança ou aos códigos de acesso; e
- **manter contrato relevante cuja extinção não assegure a transferência e a subsequente exclusão dos dados na forma da Seção 16.3.**

19. Continuidade de Negócios na Interface Cibernética

19.1. Diretrizes

A Política de Continuidade de Negócios estabelece o método, as alçadas, os cenários mínimos e o programa de testes de continuidade. A Política de Gestão de Riscos dispõe, quanto à continuidade dos negócios e na forma dos arts. 19 e 20 da Resolução BCB nº 85/2021, sobre o tratamento dos incidentes relevantes; sobre os procedimentos a serem seguidos em caso de interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o restabelecimento da operação normal; e sobre os cenários de incidente considerados nos testes de continuidade.

19.2. Prazos

A Política de Gestão de Riscos e seus procedimentos especificam o tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção de serviços relevantes, e o prazo estipulado para o reinício ou a normalização das atividades ou dos serviços interrompidos, observado o art. 43, § 4º, da Resolução BCB nº 520/2025, que alcança também as ações de

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

comunicação interna e externa necessárias à orientação sobre o restabelecimento das atividades. Os prazos por processo crítico constam da Análise de Impacto no Negócio (BIA), anexo da Política de Continuidade de Negócios.

19.3. Situação de crise e comunicação ao Banco Central do Brasil

Configura situação de crise o incidente relevante ou a interrupção de serviço relevante que atenda a pelo menos um dos seguintes critérios: indisponibilidade de processo crítico de negócio por período superior ao período máximo tolerável de interrupção (MTPD) definido na Análise de Impacto no Negócio; comprometimento de instrumento de controle de ativo virtual de cliente ou usuário; ou impossibilidade de restabelecimento por meio dos procedimentos ordinários previstos no Plano de Ação e de Resposta a Incidentes.

A Organização comunica tempestivamente ao Banco Central do Brasil a ocorrência de incidentes relevantes e as interrupções de serviços relevantes que configurem situação de crise, bem como as providências adotadas para o reinício das atividades, na forma e pelos canais definidos na regulamentação. A decisão de comunicar, ou de não comunicar, é fundamentada pelo Diretor responsável e registrada, na forma do Plano de Ação e de Resposta a Incidentes.

20. Divulgação e Cultura de Segurança

Esta Política é divulgada aos funcionários da Organização e às empresas prestadoras de serviços a terceiros, mediante linguagem clara e acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. Resumo contendo as suas linhas gerais é divulgado ao público no sítio eletrônico da Organização.

A disseminação da cultura de segurança cibernética compreende programas de capacitação e de avaliação periódica de pessoal; a prestação de informações a clientes e usuários finais sobre precauções na utilização dos produtos e serviços oferecidos, incluídas as medidas de segurança recomendadas e os riscos da autocustódia; e o comprometimento da Alta Direção com a melhoria contínua dos procedimentos.

A Organização desenvolve iniciativas de compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Banco Central do Brasil, sem prejuízo do dever de sigilo e da livre concorrência, abrangendo as informações recebidas de prestadores de serviços e mantendo-as disponíveis ao Banco Central do Brasil.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

21. Acompanhamento, Efetividade e Relatório Anual

21.1. Mecanismos

A Organização institui mecanismos de acompanhamento e de controle destinados a assegurar a implementação e a efetividade desta Política, do Plano de Ação e de Resposta a Incidentes e dos requisitos de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo a definição de processos, testes e trilhas de auditoria; a definição de métricas e indicadores adequados; e a identificação e a correção de eventuais deficiências. As notificações recebidas sobre subcontratação de serviços relevantes são consideradas na definição desses mecanismos.

21.2. Auditoria interna

Os mecanismos da Seção 21.1 são submetidos a testes anuais pela auditoria interna, exercida por empresa independente contratada, no programa de auditoria interna do SGSI, com apoio da Compliance quando necessário, com relato ao Comitê de Compliance.

21.3. Relatório anual

É elaborado relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, com data-base de 31 de dezembro, abordando, no mínimo, a efetividade da implementação das ações de adequação; o resumo dos resultados obtidos na implementação das rotinas, procedimentos, controles e tecnologias de prevenção e resposta; os incidentes relevantes ocorridos no período; os resultados dos testes de continuidade de negócios, considerados cenários de indisponibilidade ocasionada por incidentes; e os resultados dos testes de intrusão e das varreduras e análises periódicas para detecção de vulnerabilidades, com os planos de ação estabelecidos para as suas correções.

O relatório é submetido ao Comitê de Compliance e apresentado à Diretoria até 31 de março do ano seguinte ao da data-base.

21.4. Exceções

As exceções a esta Política são registradas, avaliadas quanto ao risco residual pela Segurança da Informação e aprovadas conforme a alçada única de exceções da Política de Segurança da Informação, com prazo, controles compensatórios e responsável definidos. Não são admitidas exceções aos controles da Seção 6.2 nem à exigência de múltiplos fatores de autenticação para acesso a partir de ambientes externos.

	Política de Segurança Cibernética	SEG-POL-009-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

22. Revisão

Esta Política e o Plano de Ação e de Resposta a Incidentes são documentados e revistos no mínimo anualmente, e de forma extraordinária diante de alteração normativa, de incidente relevante, inclusive envolvendo prestador, de contratação ou extinção de serviço relevante, de alteração de jurisdição de processamento ou armazenamento, de mudança material na arquitetura tecnológica ou no perímetro de serviços, de resultado de teste de intrusão que evidencie deficiência estrutural, ou de apontamento de auditoria ou da supervisão.

23. Normas de Referência

- Resolução BCB nº 85, de 8 de abril de 2021, na redação vigente, em especial o Capítulo III e os arts. 21, 22-A, 22-B e 23.
- Resolução BCB nº 552, de 3 de março de 2026, que estendeu o âmbito de aplicação da Resolução BCB nº 85/2021 às sociedades prestadoras de serviços de ativos virtuais.
- Resolução BCB nº 519 e nº 520, de 10 de novembro de 2025, em especial os arts. 14, 32 a 43, 45, 48, 49, 50 e 51 da Resolução nº 520.
- Lei nº 14.478, de 21 de dezembro de 2022.
- Lei nº 13.709, de 14 de agosto de 2018, quanto à proteção de dados pessoais.

24. Vigência

Esta Política entra em vigor na data de sua publicação, após aprovação pela Diretoria da Organização, com formalização em ata, após deliberação prévia do Comitê de Compliance, e permanece vigente até a sua revisão ou revogação expressa. A aprovação desta Política e do Plano de Ação e de Resposta a Incidentes pela Diretoria atende ao art. 9º da Resolução BCB nº 85/2021, aplicável à Organização por força da Resolução BCB nº 552/2026; na ausência de conselho de administração, a aprovação cabe à Diretoria e não é suprida por ratificação de deliberação de comitê.

25. 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