

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Política de Continuidade de Negócios

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Sumário

1. Objetivo	1
2. Abrangência	2
3. Termos e Definições	3
4. Princípios	4
5. Estrutura do Programa de Continuidade	4
6. Criticidade e Prazos de Recuperação	5
7. Cenários de Interrupção	6
8. Gestão de Crise	7
9. Comunicação	8
10. Prestadores de Serviços e Nuvem	8
11. Programa de Testes	8
12. Revisão	9
13. Normas de Referência	9
14. Vigência	10
15. Controle e Histórico de Versões	10

1. Objetivo

Esta Política estabelece os princípios, as diretrizes, os papéis e as alçadas da gestão de continuidade de negócios da Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (sociedade PSAV), referida neste documento como Organização, com o objetivo de assegurar que os processos críticos da prestação de serviços de ativos virtuais sejam mantidos ou restabelecidos em prazos definidos, e que os instrumentos de controle de ativos virtuais e os recursos financeiros de clientes e usuários permaneçam sob controle da Organização durante qualquer interrupção.

A continuidade, para a Organização, não é um tema de disponibilidade de sistemas. Uma interrupção que preserve a custódia mas suspenda a operação é um evento grave; uma interrupção que comprometa a custódia é um evento irreversível. Esta Política ordena as

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

prioridades nessa sequência: primeiro a integridade dos instrumentos de controle e dos recursos de clientes, depois a capacidade de operar, depois a conveniência.

Fundamenta-se no art. 43, IV e § 4º, da Resolução BCB nº 520, de 10 de novembro de 2025, e no art. 3º, V, “a”, nos arts. 19 e 20 e no Capítulo III da 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. Alinha-se à ISO 22301:2019 e aos controles 5.29 e 5.30 da ISO/IEC 27001:2022.

Esta Política estabelece o método e as alçadas. Os prazos de recuperação de cada processo decorrem da Análise de Impacto no Negócio (BIA) e constam do Plano de Continuidade de Negócios, na forma da Seção 6. Os requisitos operacionais são detalhados na Norma de Gestão de Continuidade de Negócios, que esta Política fundamenta.

2. Abrangência

Esta Política aplica-se aos processos, sistemas, dados, instalações, pessoas e prestadores de serviços que suportam a prestação de serviços de ativos virtuais pela Organização, inclusive a infraestrutura tecnológica compartilhada com as demais sociedades do Trace Finance Group, que, para os fins desta Política, é tratada como recurso da Organização e submete-se integralmente aos seus requisitos.

Aplica-se, ainda, aos prestadores de serviços relevantes, na forma do Capítulo de Nuvem da Política de Segurança Cibernética, e aos demais fornecedores que suportem processos críticos, na forma da Norma de Segurança em Fornecedores.

A estrutura de gestão de continuidade é única para o grupo e é regida pela Norma de Gestão de Continuidade de Negócios. Esta Política acrescenta as exigências próprias da sociedade PSAV e prevalece, quanto a ela, em caso de divergência.

3. Termos e Definições

Termo	Definição
Processo crítico	Processo cuja interrupção afeta a custódia ou a movimentação de ativos virtuais ou de recursos financeiros de clientes e usuários, o cumprimento de obrigação regulatória com prazo, ou o pleno exercício dos direitos de cliente ou usuário.

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Termo	Definição
Análise de Impacto no Negócio (BIA)	Avaliação, conduzida com os gestores dos processos, dos impactos da interrupção ao longo do tempo, da qual decorrem a categoria de criticidade, o MTPD, o RTO, o RPO e o nível mínimo aceitável de operação de cada processo.
MTPD	Período máximo tolerável de interrupção, após o qual o impacto se torna inaceitável para a Organização, para os clientes ou para a regulação.
RTO	Tempo objetivo de recuperação: prazo estipulado para o reinício ou a normalização do processo ou serviço interrompido, na forma do art. 43, § 4º, da Resolução BCB nº 520/2025. É sempre inferior ao MTPD.
RPO	Ponto objetivo de recuperação: perda máxima de dados admitida, medida como o intervalo entre o último ponto de recuperação disponível e a interrupção.
Plano de Continuidade de Negócios (PCN)	Documento que consolida, por processo crítico, os prazos aprovados, as estratégias de continuidade, os critérios de acionamento, os responsáveis e os roteiros de comunicação.
Plano de Recuperação de Desastres (PRD)	Documento técnico, mantido por Tecnologia, com os procedimentos de recuperação dos sistemas, dados e infraestrutura que suportam os processos críticos.
Situação de crise	Incidente relevante ou interrupção de serviço relevante que atenda aos critérios da Seção 19.3 da Política de Segurança Cibernética, ensejando a ativação da Mesa de Crise e a comunicação tempestiva ao Banco Central do Brasil.
Mesa de Crise	Estrutura de coordenação ativada em situação de crise, na forma da Seção 8.
Teste de continuidade	Exercício planejado que verifica a capacidade de execução das estratégias e dos planos, nas modalidades da Seção 11.

4. Princípios

A gestão de continuidade observa os seguintes princípios, que orientam toda decisão de desenho, de investimento e de resposta:

- Custódia antes de operação. Nenhuma estratégia de continuidade admite a perda, a exposição ou a transferência não autorizada de instrumentos de controle de ativos virtuais. Em caso de conflito entre restabelecer o serviço e preservar a custódia, prevalece a custódia.

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

- Fundamentação na BIA. Nenhum prazo de recuperação é fixado por conveniência técnica ou por categoria de infraestrutura. Os prazos decorrem do impacto avaliado com o gestor do processo e são aprovados pelo Comitê de Compliance.
- Proporcionalidade. As estratégias são compatíveis com o porte da Organização e com a criticidade de cada processo. Redundância sem fundamento na BIA é custo; ausência de redundância em processo crítico é risco aceito formalmente, nunca omissão.
- Segurança preservada na contingência. Os controles de segurança da informação permanecem aplicáveis durante a interrupção e a recuperação. A redução temporária de controle é autorizada, registrada e limitada no tempo, na forma da Norma de Gestão de Continuidade de Negócios.
- Capacidade demonstrada, não presumida. Um plano só é considerado efetivo após teste compatível com o seu escopo. Prazo não testado é hipótese, e é apresentado como tal em qualquer documento, inclusive ao supervisor.
- Dependência conhecida. Todo processo crítico tem mapeadas as suas dependências de pessoas, sistemas, dados, instalações e prestadores, inclusive as concentrações em um único provedor ou região.

5. Estrutura do Programa de Continuidade

O programa de continuidade é composto pelos documentos a seguir, em ordem de precedência. Cada um deriva do anterior e nenhum é considerado em vigor sem o que o fundamenta.

Documento	Conteúdo
Esta Política	Princípios, método, papéis, alçadas, cenários mínimos e programa de testes
Norma de Gestão de Continuidade de Negócios	Requisitos operacionais da BIA, das estratégias, dos planos, da gestão de crise, da comunicação, dos fornecedores, dos testes e da melhoria
Análise de Impacto no Negócio (BIA)	Processos críticos, impactos no tempo, categoria de criticidade, MTPD, RTO, RPO, nível mínimo de operação e dependências
Plano de Continuidade de Negócios (PCN)	Por processo crítico: prazos aprovados, estratégias, acionamento, responsáveis e substitutos, procedimentos alternativos e roteiros de comunicação

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Documento	Conteúdo
Plano de Recuperação de Desastres (PRD)	Procedimentos técnicos de recuperação de sistemas, dados e infraestrutura, com ordem de recuperação e critérios de verificação
Programa anual de testes e relatórios	Calendário, cenários, resultados, desvios e ações; inclui os testes de restauração do Processo de Teste de Restauração de Backup

A BIA é anexo desta Política, aprovada pelo Comitê de Compliance e atualizável sem alteração da versão maior, desde que não modifique os princípios, os papéis ou as alçadas aqui fixados. O PCN e o PRD são documentos próprios, na forma da Norma de Gestão Documental. A alteração de categoria ou de prazo de recuperação de processo crítico é sempre feita por revisão da BIA, submetida ao Comitê de Compliance.

6. Criticidade e Prazos de Recuperação

6.1. Categorias de criticidade

A BIA classifica cada processo em uma das categorias a seguir, definidas pelo período máximo tolerável de interrupção. A categoria determina a prioridade de recuperação, o rigor das estratégias e a frequência mínima de teste.

Categoria	MTPD	Processos típicos	Exigência mínima
Crítico	Até 4 horas	Custódia e movimentação de ativos virtuais; autenticação de clientes; liquidação de operações; monitoramento PLD	Estratégia de recuperação automatizada; teste técnico anual; cenário em teste integrado anual
Alto	Até 24 horas	Atendimento a clientes; conciliação; comunicações regulatórias com prazo	Procedimento alternativo documentado; teste anual
Médio	Até 72 horas	Processos de suporte com impacto financeiro ou contratual diferido	Procedimento alternativo documentado; teste a cada dois anos
Baixo	Superior a 72 horas	Processos administrativos sem impacto em clientes ou em obrigações com prazo	Registro na BIA; sem plano específico

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

A atribuição de categoria é feita pelo impacto, e não pelo sistema que suporta o processo. Os processos típicos indicados são orientativos; a classificação vinculante é a da BIA aprovada.

6.2. Regras para os prazos

O RTO de cada processo é inferior ao seu MTPD e é fixado com margem para a decisão de acionamento, a execução da recuperação e a verificação de segurança antes do retorno. O RPO é fixado pela tolerância do processo à perda de dados e é compatível com a capacidade de recuperação efetivamente disponível na Política de Backup; incompatibilidade entre o RPO exigido e a capacidade existente é registrada como risco e tratada, não ajustada no papel.

Os prazos aprovados constam da BIA, são reproduzidos no PCN e são os prazos estipulados para o reinício ou a normalização das atividades para os fins do art. 43, § 4º, da Resolução BCB nº 520/2025.

6.3. Nível mínimo aceitável de operação

Para cada processo crítico, a BIA define o nível mínimo aceitável de operação durante a contingência. Para os processos de custódia e movimentação de ativos virtuais, o nível mínimo inclui, em qualquer cenário, a capacidade de bloquear movimentações, de confirmar saldos e de atender ordem de autoridade, ainda que a operação normal esteja suspensa.

7. Cenários de Interrupção

As estratégias, os planos e os testes consideram, no mínimo, os cenários a seguir, que incluem os cenários de incidente exigidos pelo art. 3º, V, "a", e pelo art. 19, III, da Resolução BCB nº 85/2021:

- comprometimento, suspeita de comprometimento ou indisponibilidade de instrumento de controle de ativos virtuais, inclusive por falha ou indisponibilidade do prestador da infraestrutura de carteiras;
- indisponibilidade de prestador de serviço relevante de processamento, armazenamento de dados ou computação em nuvem, inclusive a indisponibilidade de uma região inteira do provedor de infraestrutura, com o cenário de substituição do prestador exigido pelo Capítulo de Nuvem da Política de Segurança Cibernética;
- perda, corrupção ou criptografia maliciosa de dados de produção, exigindo restauração a partir de cópia de segurança;

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

- incidente cibernético que exija o isolamento de ambientes ou a suspensão preventiva de serviços, inclusive ataque de negação de serviço e comprometimento de credenciais privilegiadas;
- indisponibilidade de pessoas-chave, em especial dos detentores de instrumentos de controle e dos administradores de plataforma, inclusive por indisponibilidade simultânea;
- indisponibilidade das instalações físicas ou dos meios de comunicação habituais, com operação integralmente remota;
- indisponibilidade de serviço de borda, de identidade ou de observabilidade que impeça o acesso dos clientes ou a operação dos controles de segurança.

Cada cenário tem estratégia definida no PCN e, quando envolver recuperação tecnológica, procedimento no PRD. Cenário sem estratégia é registrado como risco aceito pela alçada competente, com prazo para tratamento.

8. Gestão de Crise

Configura situação de crise a interrupção que atenda aos critérios da Seção 19.3 da Política de Segurança Cibernética: indisponibilidade de processo crítico por período superior ao MTPD definido na BIA; comprometimento de instrumento de controle de ativo virtual de cliente ou usuário; ou impossibilidade de restabelecimento pelos procedimentos ordinários do Plano de Ação e de Resposta a Incidentes.

A situação de crise é declarada pelo Diretor responsável, que ativa a Mesa de Crise composta, no mínimo, por ele, pelo Responsável pela Gestão de Continuidade, por Compliance e pelos gestores dos processos afetados. A Mesa decide a ordem de recuperação segundo as categorias da Seção 6.1, autoriza o uso das estratégias de contingência e aprova as comunicações. As decisões, os horários e os fundamentos são registrados em tempo real e consolidados após o encerramento.

A ativação e a desativação dos planos, os critérios de estabilização e o retorno à operação normal seguem a Norma de Gestão de Continuidade de Negócios. O retorno à operação normal depende de verificação de segurança pela Segurança da Informação, com registro.

9. Comunicação

A Organização comunica tempestivamente ao Banco Central do Brasil a situação de crise e as providências adotadas para o reinício das atividades, na forma e pelos canais da regulamentação, com decisão fundamentada pelo Diretor responsável e registrada conforme o Plano de Ação e de Resposta a Incidentes. A comunicação interna e externa necessária à

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

orientação sobre o restabelecimento das atividades integra o prazo de reinício, na forma do art. 43, § 4º, da Resolução BCB nº 520/2025.

Os clientes e usuários são informados sobre a interrupção de serviço que os afete, sobre o estado dos seus ativos e sobre a previsão de restabelecimento, por canal definido no PCN e com linguagem que distinga fato confirmado de estimativa. Quando a interrupção envolver dados pessoais, aplica-se a Política de Proteção de Dados Pessoais. As comunicações externas são aprovadas pelo Diretor responsável em conjunto com Compliance.

10. Prestadores de Serviços e Nuvem

Para cada prestador de serviço relevante é mantida alternativa de continuidade que contemple a substituição do prestador e o restabelecimento da operação, com prazo estimado de reinício compatível com os prazos da BIA, na forma do Capítulo de Nuvem da Política de Segurança Cibernética. A capacidade de continuidade dos prestadores é avaliada na diligência prévia e no monitoramento contínuo, com evidência documental, e os contratos contêm as cláusulas de continuidade, de acesso a dados e de devolução ali exigidas.

A concentração em um único provedor de infraestrutura, em uma única região ou em um único prestador de infraestrutura de carteiras é registrada como risco de concentração na Política de Gestão de Riscos e reavaliada anualmente, com a decisão de tratamento ou de aceitação registrada pelo Comitê de Compliance.

11. Programa de Testes

O programa anual de testes, aprovado com ciência do Comitê de Compliance, contempla, no mínimo: um exercício integrado de mesa por ano, com cenário cibernético e com a participação da Mesa de Crise; um teste técnico de recuperação por ano para cada sistema que suporte processo Crítico, inclusive com cenário de indisponibilidade de prestador relevante; e os testes de restauração de cópias de segurança na periodicidade do Processo de Teste de Restauração de Backup.

Cada teste tem objetivo, cenário, critérios de sucesso e responsáveis definidos previamente e é registrado em relatório, com os prazos efetivamente apurados, os desvios e as ações corretivas, acompanhadas até a conclusão. Um prazo aprovado que não seja alcançado em teste é reportado ao Comitê de Compliance e tratado antes que o plano seja considerado efetivo para aquele processo.

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Os resultados dos testes de continuidade integram o relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, na forma da Política de Segurança Cibernética e do art. 8º da Resolução BCB nº 85/2021.

12. Revisão

Esta Política é revista anualmente, e de forma extraordinária diante de alteração normativa, de aprovação ou revisão da BIA que altere categoria ou prazo de processo crítico, de ativação dos planos, de resultado de teste que evidencie incapacidade de atender prazo aprovado, de mudança material na arquitetura tecnológica ou nos prestadores relevantes, ou de apontamento de auditoria ou da supervisão.

13. Normas de Referência

- Resolução BCB nº 520, de 10 de novembro de 2025, em especial o art. 43, IV e § 4º, e os arts. 32 a 42.
- Resolução BCB nº 85, de 8 de abril de 2021, em especial o art. 3º, V, os arts. 8º, 19 e 20 e o Capítulo III, na redação vigente, aplicável às sociedades prestadoras de serviços de ativos virtuais pela Resolução BCB nº 552, de 3 de março de 2026, com as alterações da Resolução BCB nº 538/2025.
- Lei nº 14.478, de 21 de dezembro de 2022.
- ISO 22301:2019: Segurança e resiliência, Sistemas de gestão de continuidade de negócios, Requisitos.
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022, em especial os controles 5.29 (segurança da informação durante interrupção) e 5.30 (prontidão de TIC para continuidade de negócios).

14. 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.

	Política de Continuidade de Negócios	SEG-POL-010-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

15. 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