THREE

SECURITIZADORA

PLANO DE

CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

Versão 1.0 — Abril/2026

Elaboração: Compliance e PLD/FTP
Aprovação: Diretoria de Compliance e PLD/FTP
Base: Res. CVM 60/2021 (art. 20, IV) | Res. CVM 194/2023 | Lei 14.430/2022

Av. Brigadeiro Faria Lima, 1903, 6º andar — Jardim Paulistano — São Paulo — SP | www.threesecuritizadora.com.br

Elaboração:	Compliance e PLD/FTP
Aprovação:	Diretoria de Compliance e PLD/FTP
Vigente Desde:	Abril/2026
Versão:	1.0
Última Revisão:	Abril/2026
Base Normativa:	Resolução CVM 60/2021, art. 20, IV (alt. Res. CVM 194/2023) | Lei 14.430/2022

1. OBJETIVO

O presente Plano de Contingência e Continuidade dos Negócios ("PCN") tem por objetivo estabelecer as diretrizes, procedimentos e responsabilidades da THREE COMPANHIA SECURITIZADORA S.A. ("Companhia" ou "Three") para prevenção, resposta e recuperação diante de eventos que possam interromper, total ou parcialmente, suas atividades operacionais.

Este Plano foi elaborado em observância ao art. 20, inciso IV, da Resolução CVM 60/2021 (alterada pela Resolução CVM 194/2023), que exige das companhias securitizadoras a manutenção de plano de contingência atualizado, e em linha com a Lei 14.430/2022 (Marco Legal da Securitização), assegurando a proteção dos investidores e a integridade dos Patrimônios Separados.

A Three atua com emissões de valores mobiliários em regime de oferta pública, nos termos da Instrução CVM 400 e da Resolução CVM 160/2022, e em regime de oferta privada, conforme facultado pela Lei 14.430/2022 e pela regulamentação aplicável. Este Plano abrange as operações realizadas sob ambas as modalidades, assegurando a continuidade das obrigações da Companhia perante os investidores, os Patrimônios Separados e os reguladores, independentemente do regime de oferta adotado.

O PCN é parte integrante do conjunto de documentos internos da Three, devendo ser lido em conjunto com: (i) Política de Segurança da Informação e Cibernética; (ii) Manual de Controles Internos e PLD/FTP; e (iii) Código de Ética e Conduta.

2. ABRANGÊNCIA E APLICABILIDADE

Este Plano aplica-se a todos os sócios, administradores e Colaboradores da Three, bem como aos prestadores de serviços estratégicos contratados, incluindo assessores jurídicos, contábeis e de tecnologia da informação, nos termos da Política de Contratação de Prestadores de Serviços.

O PCN abrange os seguintes processos e ativos críticos da Companhia:

– Operações de securitização em curso (CRI, CRA, CR e debêntures), realizadas tanto em regime de oferta pública quanto de oferta privada;
– Gestão e monitoramento dos Patrimônios Separados;
– Sistemas de tecnologia da informação e segurança cibernética;
– Comunicações com a CVM, ANBIMA, agentes fiduciários, custodiantes e investidores;
– Fluxos financeiros dos Patrimônios Separados;
– Registros contábeis e documentação regulatória.

3. DEFINIÇÕES

Evento de Contingência

Qualquer ocorrência, prevista ou imprevista, que cause ou possa causar interrupção total ou parcial das atividades da Three, incluindo falhas tecnológicas, desastres naturais, pandemias, ataques cibernéticos, falhas de terceiros estratégicos ou eventos de força maior.

RTO — Recovery Time Objective

Tempo máximo tolerável para a retomada de um processo ou sistema crítico após um evento de contingência.

RPO — Recovery Point Objective

Ponto máximo de perda de dados tolerável, ou seja, o intervalo de tempo máximo admissível entre o último backup válido e o momento do incidente.

Acionamento do PCN

Declaração formal pelo Diretor de Compliance e PLD/FTP de que um Evento de Contingência justifica a aplicação das medidas previstas neste Plano.

Patrimônio Separado

Conforme Lei 14.430/2022 (art. 27): conjunto de direitos creditórios e bens vinculados a uma emissão, que não se confunde com o patrimônio comum da Three nem responde por suas obrigações.

Colaboradores

Todos os sócios, administradores, funcionários, estagiários e prestadores de serviço com acesso aos sistemas e informações da Three, conforme definido no Manual de Controles Internos e PLD/FTP.

Oferta Pública

Distribuição de valores mobiliários emitidos pela Three realizada nos termos da Resolução CVM 160/2022 e demais normas aplicáveis, sujeita a registro ou dispensa de registro perante a CVM.

Oferta Privada

Distribuição de valores mobiliários emitidos pela Three realizada sem esforços públicos de colocação, nos termos da Lei 14.430/2022 e da regulamentação aplicável, com destinação restrita a investidores previamente identificados.

4. CLASSIFICAÇÃO DE EVENTOS E CRITICIDADE

Os Eventos de Contingência são classificados em quatro níveis de criticidade, considerando o impacto potencial sobre as operações, os Patrimônios Separados, os investidores — de ofertas públicas e privadas — e as obrigações regulatórias da Three:

1	Crítico	Interrupção total de sistemas ou operações essenciais. Impacto imediato sobre os Patrimônios Separados ou obrigações regulatórias.	4h
2	Alto	Falha em processo relevante com possível impacto em emissões ativas (públicas ou privadas) ou no cumprimento de prazos regulatórios.	24h
3	Médio	Interrupção de atividades de suporte, sem impacto imediato nas operações ou nos investidores.	72h
4	Baixo	Ocorrências de baixo impacto, sem risco às operações de securitização ou às obrigações da Companhia.	7d

** RTO: tempo máximo para retomada das operações. 4h = quatro horas; 24h = vinte e quatro horas; 72h = setenta e duas horas; 7d = sete dias corridos. Os RTOs são objetivos e podem ser ajustados conforme a complexidade do evento.*

5. CENÁRIOS DE CONTINGÊNCIA IDENTIFICADOS

A Three identificou os seguintes cenários como principais riscos operacionais, em linha com a Política de Segurança da Informação e Cibernética e com o Manual de Controles Internos e PLD/FTP:

5.1 Falhas de Sistemas e Tecnologia

– Indisponibilidade da plataforma de securitização (Akrual ou equivalente): acionamento de ambiente de contingência; contato imediato com fornecedor; processamento manual temporário se necessário.

– Ataque cibernético (ransomware, DDoS, intrusão): aplicação imediata do Plano de Resposta a Incidentes previsto na Política de Segurança da Informação e Cibernética; isolamento de sistemas comprometidos; notificação ao Diretor de Compliance e PLD/FTP e à Área de SI.

– Perda de dados: restauração a partir do backup diário; RPO máximo de 24 horas.

5.2 Indisponibilidade de Pessoal-Chave

– Ausência temporária de Diretor: redistribuição de responsabilidades entre os demais Diretores, com registro formal da delegação.

– Afastamento prolongado ou definitivo: processo de substituição ou contratação conduzido pela Diretoria, com comunicação à CVM se aplicável.

– Pandemia ou crise sanitária: adoção de trabalho remoto para todos os Colaboradores; manutenção das ferramentas de acesso seguro previstas na Política de Segurança da Informação e Cibernética.

5.3 Falha de Prestadores de Serviços Estratégicos

– Falha do agente fiduciário ou custodiante: acionamento imediato do Diretor de Securitização; comunicação aos investidores (de ofertas públicas e privadas); avaliação de substituição conforme instrumentos de emissão.

– Falha do assessor jurídico ou contábil: acionamento de prestador substituto previamente cadastrado; continuidade das obrigações com suporte interno.

– Falha do provedor de TI/SI: restauração via backup em nuvem ou servidor redundante; acionamento de suporte técnico de contingência.

5.4 Eventos Externos e Força Maior

– Desastres naturais, incêndios ou interdição da sede: adoção de trabalho remoto; acesso aos sistemas via VPN segura; manutenção dos fluxos financeiros dos Patrimônios Separados.

– Instabilidade no sistema financeiro: monitoramento contínuo dos fluxos de caixa dos Patrimônios Separados; comunicação proativa com investidores de ofertas públicas e privadas.

– Alterações regulatórias emergenciais: análise imediata pelo Diretor de Compliance e PLD/FTP; adequação dos processos e comunicação à CVM se necessário.

6. RESPONSABILIDADES

A coordenação geral do PCN é de responsabilidade do Diretor de Compliance e PLD/FTP, com a participação dos demais Diretores conforme suas áreas de atuação, em linha com o Manual de Controles Internos e PLD/FTP e com o Manual de Estrutura Operacional da Three:

Diretor de Compliance e PLD/FTP	Coordenação geral do PCN; declaração de acionamento; comunicação à CVM e demais reguladores; supervisão da resposta ao incidente.
Diretor de Securitização	Garantir continuidade das obrigações relativas às emissões ativas (públicas e privadas) e aos Patrimônios Separados; comunicação com agente fiduciário e custodiante.
Diretor de Distribuição	Comunicação com investidores de ofertas públicas e privadas; suporte à continuidade das atividades comerciais e de relacionamento.
Área de SI / TI (terceiros)	Recuperação de sistemas, backups e infraestrutura tecnológica; suporte à Área de Segurança da Informação conforme Política de Segurança da Informação e Cibernética.

7. PROCEDIMENTOS DE ACIONAMENTO DO PCN

Diante da ocorrência ou iminência de um Evento de Contingência, os seguintes procedimentos devem ser adotados:

1. Identificação e Comunicação Interna

Qualquer Colaborador que identificar um Evento de Contingência deverá comunicar imediatamente ao seu superior imediato e ao Diretor de Compliance e PLD/FTP, conforme previsto na Política de Segurança da Informação e Cibernética.

2. Avaliação e Classificação

O Diretor de Compliance e PLD/FTP avaliará o evento, classificará o nível de criticidade (conforme Seção 4) e decidirá pelo acionamento formal do PCN.

3. Acionamento Formal

O acionamento é declarado formalmente pelo Diretor de Compliance e PLD/FTP, com registro escrito da data, hora, natureza do evento e nível de criticidade atribuído.

4. Execução das Medidas de Contingência

Cada Diretor adota as medidas previstas neste Plano para sua área de responsabilidade, com prioridade para a proteção dos Patrimônios Separados e o cumprimento das obrigações regulatórias, independentemente de as emissões afetadas serem de oferta pública ou privada.

5. Comunicação Externa

O Diretor de Compliance e PLD/FTP avalia a necessidade de comunicação à CVM, à ANBIMA, ao agente fiduciário, ao custodiante e/ou aos investidores — de ofertas públicas e privadas — nos prazos e formas exigidos pela regulamentação aplicável.

6. Monitoramento e Encerramento

O Diretor de Compliance e PLD/FTP monitora a evolução do evento, documenta as ações adotadas e declara formalmente o encerramento do acionamento do PCN quando as operações estiverem normalizadas.

7. Registro e Lições Aprendidas

Após o encerramento, é elaborado relatório com descrição do evento, medidas adotadas, resultados e recomendações de melhoria, arquivado por pelo menos 5 (cinco) anos na sede da Three.

8. TECNOLOGIA, BACKUPS E RECUPERAÇÃO

Em linha com a Política de Segurança da Informação e Cibernética da Three, as seguintes medidas técnicas de continuidade são adotadas:

– Backup diário automático de todos os dados operacionais e documentos regulatórios, com retenção mínima de 5 (cinco) anos, conforme exigido pelo Manual de Controles Internos e PLD/FTP;

– Armazenamento de backups em ambiente seguro, distinto da infraestrutura principal, com acesso restrito e autenticação multifator;

– Firewall, antivírus e varreduras periódicas conforme previsto na Política de Segurança da Informação e Cibernética;

– Acesso remoto seguro via VPN para todos os Colaboradores em situação de trabalho remoto;

– Testes periódicos de restauração de backup, com frequência mínima anual, documentados pela Área de SI;

– RPO máximo de 24 horas para dados operacionais críticos (sistemas de securitização e registros dos Patrimônios Separados), abrangendo operações de oferta pública e privada.

9. COMUNICAÇÃO EM SITUAÇÕES DE CRISE

A gestão da comunicação durante um Evento de Contingência é de responsabilidade do Diretor de Compliance e PLD/FTP, observando os seguintes princípios:

– Transparência: as informações relevantes serão comunicadas de forma clara, tempestiva e objetiva às partes interessadas;

– Hierarquia: a comunicação externa segue a ordem — reguladores (CVM, ANBIMA) → agente fiduciário e custodiante → investidores (de ofertas públicas e privadas) → demais partes;

– Registro: todas as comunicações externas realizadas durante o acionamento do PCN serão devidamente documentadas e arquivadas;

– Prazo: a comunicação à CVM, quando obrigatória, observará os prazos previstos na Resolução CVM 60/2021 e demais normas aplicáveis.

Nota: Incidentes cibernéticos com potencial impacto sobre dados de investidores ou sobre os Patrimônios Separados devem ser comunicados ao Diretor de Compliance e PLD/FTP em até 24 horas da identificação, conforme Política de Segurança da Informação e Cibernética.

10. TESTES E REVISÃO DO PLANO

O Diretor de Compliance e PLD/FTP realizará, ao menos uma vez por ano, revisão e teste dos procedimentos previstos neste Plano, incluindo:

– Verificação da atualidade das informações de contato dos responsáveis e prestadores estratégicos;

– Simulação de pelo menos um cenário de contingência, com registro dos resultados;

– Avaliação da eficácia dos RTOs e RPOs definidos;

– Atualização do Plano em caso de alterações relevantes na estrutura operacional, nos sistemas, nas modalidades de oferta (pública ou privada) ou na regulamentação aplicável;

– Integração com o treinamento anual de compliance previsto no Manual de Controles Internos e PLD/FTP.

O resultado dos testes e eventuais recomendações de melhoria serão registrados em relatório específico, arquivado na sede da Three pelo prazo mínimo de 5 (cinco) anos.

11. DISPOSIÇÕES GERAIS

Este Plano entra em vigor imediatamente na data de sua aprovação pela Diretoria de Compliance e PLD/FTP e poderá ser modificado a qualquer momento, sempre que houver alteração relevante na regulamentação, na estrutura operacional, nas modalidades de oferta (pública ou privada) praticadas pela Companhia ou nos sistemas da Three.

Em caso de conflito entre este Plano e o Código de Ética e Conduta da Three, este último prevalecerá. Para os aspectos de segurança da informação e cibernética, prevalecerão as disposições da Política de Segurança da Informação e Cibernética.

Quaisquer dúvidas relacionadas a este Plano podem ser endereçadas à Diretoria de Compliance e PLD/FTP.

São Paulo, abril de 2026.

JANICE ELIAS DE MORAES ORLANDO:21417289830

Assinado de forma digital por JANICE ELIAS DE MORAES ORLANDO:21417289830
Dados: 2026.04.23 15:04:50 -03'00'

Janice Elias de Moraes Orlando

_____

Diretoria de Compliance e PLD/FTP

Versão 1.0 – Abril/2026 | THREE COMPANHIA SECURITIZADORA S.A.