

Política de Segurança da Informação e Continuidade de Negócios

Versão 5 · 09/10/2026

Campo	Informação
Documento	Política de Segurança da Informação e Continuidade de Negócios
Versão	5 (SEGINFO – 002/2026) — substitui a versão assinada em 02/09/2026 (SEGINFO – 001/2026)
Data de aprovação e vigência	09/10/2026 — Reunião do Conselho de Administração
Responsável primário	Diretor de Controles Internos
Contato institucional	compliance@hive securitizadora.com · (43) 98800-2424

1. Definições

Termo	Definição
Companhia	HIVE SECURITIZADORA S.A., entidade sujeita à presente Política.
Ativo de Informação	Sistema, aplicação, base, documento, credencial, equipamento ou dado que suporta processos da Companhia.
Informação Crítica	Informação cuja indisponibilidade, alteração ou divulgação causa impacto material às operações ou à conformidade.
Processo Crítico	Processo essencial ao funcionamento da Companhia cuja interrupção compromete a continuidade.
Análise de Impacto no Negócio (BIA)	Avaliação que identifica processos críticos, dependências e impactos temporais e financeiros.
RTO (<i>Recovery Time Objective</i>)	Tempo máximo aceitável para restauração de um processo ou sistema após interrupção.
RPO (<i>Recovery Point Objective</i>)	Perda máxima aceitável de dados, medida em tempo, entre pontos de recuperação.
Plano de Continuidade de Negócios (PCN)	Procedimentos e recursos para manter ou retomar operações críticas após interrupção.
Plano de Recuperação de Desastres (DRP)	Procedimentos técnicos para restauração de sistemas e infraestrutura após evento grave.
Plano de Resposta a Incidentes (IRP)	Procedimentos de detecção, contenção, investigação, remediação e comunicação de incidentes de segurança.
Incidente de Segurança	Evento confirmado ou suspeito que comprometa a confidencialidade, a integridade ou a disponibilidade de ativos.
Backup	Cópia de segurança de dados e configurações destinada à restauração em caso de perda.
Failover / Failback	Comutação para ambiente de contingência e retorno ao ambiente primário.
Terceiro Crítico	Fornecedor cujo serviço impacta materialmente a disponibilidade, a segurança ou a continuidade da Companhia (por exemplo, a plataforma

Termo	Definição
	Akrual, utilizada como ferramenta do <i>servicing</i> interno, e o provedor de guarda documental).
Questionário de <i>Due Diligence</i> (QDD)	Instrumento para avaliar controles e riscos de Terceiros Críticos antes da contratação.
Confidencialidade, Integridade e Disponibilidade (CID)	Princípios que orientam os controles e as prioridades desta Política.

2. Introdução, base normativa e finalidade

2.1. Esta Política estabelece princípios, diretrizes, responsabilidades e medidas mínimas para a proteção da informação, da infraestrutura tecnológica e dos processos críticos da Companhia, bem como para a prevenção, a resposta e a recuperação diante de incidentes que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade dos ativos de informação.

2.2. Base normativa:

- a) Resolução CVM nº 60/2021, art. 19 (regras, procedimentos e controles internos escritos e efetivos) e art. 20, I, II e IV (controle de informações confidenciais, testes periódicos de segurança dos sistemas e planos de contingência e continuidade de negócios);
- b) Resolução CVM nº 60/2021, art. 35, § 2º (manutenção dos registros das emissões em perfeita ordem), art. 46, III (divulgação das regras e controles internos na página da Companhia) e art. 57 (guarda de documentos por 5 anos);
- c) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD), em especial os arts. 46 a 49; e
- d) Estatuto Social, Artigos 19 e 50.

3. Escopo, aplicabilidade e documentos correlatos

3.1. Esta Política aplica-se a todos os administradores, colaboradores, prestadores de serviços e demais pessoas que atuem para ou em nome da Companhia, em todos os processos corporativos, regulatórios, operacionais e tecnológicos.

3.2. Esta Política deve ser interpretada em conjunto com o Manual de Compliance, a Política de PLD/FTP, a Política de Gestão de Riscos, a Política de Distribuição e Conduta, os contratos com Terceiros Críticos e os procedimentos de proteção de dados pessoais e de resposta a incidentes.

4. Governança, responsabilidades e incidentes

4.1. O Conselho de Administração aprova esta Política, promove a cultura de segurança da informação, assegura recursos compatíveis com o porte da Companhia e supervisiona a implementação dos controles e das medidas de continuidade.

4.2. O Diretor de Controles Internos é o responsável primário por esta Política, pela coordenação dos testes, pelo registro e tratamento de incidentes e pelo reporte trimestral ao Conselho de Administração (Artigo 19, iii, do Estatuto Social).

4.3. Todos os destinatários devem proteger os ativos de informação sob sua responsabilidade, observar as regras de acesso, uso e armazenamento, reportar tempestivamente incidentes, fragilidades, perdas, acessos indevidos, vazamentos ou indisponibilidades e cooperar com as medidas de resposta.

4.4. **Substituição.** Nas ausências e impedimentos temporários do Diretor de Controles Internos, suas funções serão exercidas pelo Diretor-Presidente, Cristiano dos Santos Macedo, designado substituto pelo Conselho de Administração em reunião realizada em 09/10/2026. O substituto não acumula, nesse período, as funções de securitização ou de distribuição (art. 5º, § 2º, da Resolução CVM nº 60/2021; Artigo 16 do Estatuto Social). Em caso de vacância, o substituto atuará interinamente por no máximo 30 (trinta) dias, prazo em que o Conselho de Administração elegerá o novo titular (Artigo 16, § 2º, do Estatuto Social). Contato: compliance@hivesecuritizadora.com.

5. Princípios, classificação da informação e controle de acesso

5.1. A Companhia orienta-se pelos princípios da confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, necessidade de acesso, menor privilégio, segregação de funções e responsabilidade individual. As informações são classificadas segundo sua criticidade e sensibilidade (pública, interna, confidencial e restrita), com regras proporcionais de acesso, armazenamento, compartilhamento, retenção e descarte.

5.2. O acesso físico e lógico a informações, sistemas, e-mails corporativos, bases de dados, credenciais e equipamentos é concedido apenas a pessoas autorizadas, em nível compatível com a função, com revisão periódica, revogação tempestiva de credenciais, autenticação de múltiplos fatores nos sistemas críticos e registro de acessos.

5.3. Informações confidenciais relativas a emissões em estruturação e a informações privilegiadas observam o controle de acesso desta Política e as regras do Regime Informacional da Companhia (art. 20, I, da Resolução CVM nº 60/2021).

6. Segurança lógica, física, backup e retenção

6.1. A Companhia mantém controles lógicos e físicos compatíveis com a criticidade de suas atividades, incluindo gestão de credenciais, autenticação adequada, proteção de estações e dispositivos, atualização de sistemas, controle de mídias removíveis e descarte seguro de equipamentos e documentos.

6.2. A Companhia mantém rotinas de *backup* e recuperação proporcionais à criticidade das informações, com periodicidade definida, testes de restauração, armazenamento seguro em ambiente vinculado ao CNPJ da Companhia e verificação de integridade. Os registros corporativos observam os prazos de guarda do art. 57 da Resolução CVM nº 60/2021 e das demais normas aplicáveis.

7. Segurança cibernética, monitoramento e resposta

7.1. A Companhia mantém mecanismos de prevenção, detecção e resposta a ameaças cibernéticas compatíveis com o seu porte, incluindo atualização de sistemas, segregação de ambientes, proteção contra software malicioso, monitoramento de eventos, análise de vulnerabilidades, gestão de correções, controle de mudanças e resposta coordenada a incidentes.

7.2. Incidentes de segurança são registrados, classificados e tratados tempestivamente, com contenção, investigação, remediação e registro das providências, e escalonados ao Diretor de Controles Internos conforme a criticidade.

7.3. Incidentes que envolvam dados pessoais e possam acarretar risco ou dano relevante aos titulares serão comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados no prazo máximo de 72 (setenta e duas) horas do seu conhecimento, nos termos do art. 48 da LGPD e da

regulamentação da ANPD. Incidentes que afetem emissões em circulação serão informados ao agente fiduciário e avaliados à luz do Regime Informacional da Companhia.

8. Continuidade de negócios e recuperação

8.1. A Companhia adota os tempos de recuperação e os objetivos de perda de dados (RTO/RPO) do Anexo II, aprovados pelo Conselho de Administração, que serão validados pelos testes do Anexo V e ajustados, se necessário, por nova versão desta Política.

8.2. O PCN será testado periodicamente e atualizado com base nos resultados e lições aprendidas (art. 20, IV, da Resolução CVM nº 60/2021).

9. Terceiros, privacidade e proteção de dados

9.1. A Companhia avalia, de forma proporcional ao risco, os impactos de Terceiros Críticos sobre a segurança da informação, a disponibilidade de sistemas, a continuidade de processos e a proteção de dados pessoais. A contratação de Terceiros Críticos observa o QDD do Anexo III e as cláusulas mínimas do Anexo VI, inclusive SLA, notificação de incidentes em até 24 horas, direito de auditoria e continuidade.

9.2. A contratação de prestador para atividade da Companhia não a exime de suas responsabilidades (art. 35, § 1º, da Resolução CVM nº 60/2021). O *servicing* e a cobrança dos lastros são exercidos pela própria Companhia, sob a responsabilidade do Diretor de Securitização; a plataforma Akruai é ferramenta tecnológica dessa atividade.

9.3. O tratamento de dados pessoais observa a LGPD e os princípios de finalidade, necessidade, adequação, segurança e responsabilização.

10. Treinamento, testes, monitoramento e reporte

10.1. A Companhia mantém programa de treinamento inicial e recorrente em segurança da informação, segurança cibernética, proteção de dados e continuidade de negócios, adequado às funções e à exposição ao risco (art. 20, III, da Resolução CVM nº 60/2021).

10.2. Os testes periódicos de segurança dos sistemas (art. 20, II, da Resolução CVM nº 60/2021) observam o cronograma do Anexo V, ancorado em eventos objetivos do ciclo da Companhia, e são documentados no modelo do Anexo IV.

10.3. A efetividade desta Política é monitorada por testes, revisões, indicadores e acompanhamento de ocorrências. O Diretor de Controles Internos incluirá suas conclusões no relatório anual que encaminhará aos órgãos de administração até o último dia útil de abril, relativo ao ano civil anterior, contendo (i) as conclusões dos exames efetuados, (ii) as recomendações sobre eventuais deficiências, com cronograma de saneamento, e (iii) a **manifestação do Diretor de Securitização** a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas ou adotadas para saná-las, nos termos do art. 21, I a III, da Resolução CVM nº 60/2021. O relatório ficará disponível para a CVM na sede da Companhia (art. 21, § 2º).

11. Revisão, atualização e gestão da Política

11.1. Esta Política vigora por prazo indeterminado e será revisada anualmente, ou antes, sempre que houver alteração regulatória relevante, mudança material no ambiente tecnológico, incidente relevante, alteração na estrutura operacional, contratação ou substituição de Terceiro Crítico, mudança no perfil de risco ou determinação do Conselho de Administração.

11.2. As evidências dos testes do Anexo V serão arquivadas em dossiê e disponibilizadas à auditoria e à CVM.

12. Informações da Política

Campo	Informação
Documento	Política de Segurança da Informação e Continuidade de Negócios da HIVE SECURITIZADORA S.A.
Versão	SEGINFO – 002/2026 (Versão 5)
Data de referência e de vigência	09/10/2026
Revisão	Anual, ou em prazo inferior nas hipóteses do item 11
Responsável primário	Diretor de Controles Internos

13. Disposições finais

13.1. Esta Política integra o arcabouço de governança, controles internos e gestão de riscos da Companhia. Sua existência não dispensa a implementação efetiva dos controles nem a manutenção de evidências suficientes para demonstrar seu cumprimento perante a CVM, os titulares de dados e demais interessados.

13.2. Esta Política é aprovada pelo Conselho de Administração (Artigo 50 do Estatuto Social) e divulgada na página da Companhia na rede mundial de computadores (art. 46, III, da Resolução CVM nº 60/2021).

Anexo I – Termo de Compromisso

O compromisso de observância desta Política pelos administradores é formalizado no **Termo de Adesão e Compromisso consolidado** da Companhia. Colaboradores e prestadores que venham a ter acesso a informações da Companhia firmarão o mesmo Termo, ou instrumento contratual com cláusula equivalente, antes do início de suas atividades.

Anexo II – Tabela RTO/RPO por Processo Crítico

Processo crítico	Descrição	RPO	RTO	Responsável	Dependências
Estruturação e emissão de CRI/CRA	Estruturação, documentação e emissão	24 horas	4 horas	Diretor de Securitização	Plataforma Akreal; custodiante; entidade registradora
Gestão de caixa e pagamentos dos patrimônios separados	Liquidação de fluxos, conciliação e pagamentos a investidores	8 horas	1 hora	Diretor de Securitização	Conta vinculada; banco liquidante; escriturador
Servicing e cobrança do lastro	Acompanhamento, conciliação e cobrança	24 horas	8 horas	Diretor de Securitização	Plataforma Akreal
Monitoramento de PLD/FTP	Monitoramento de operações e alertas	48 horas	24 horas	Diretor Responsável por PLD/FTP	Acesso a sistemas e bases de listas
Prestação de informações à CVM e ao mercado	Informes periódicos, fatos relevantes e comunicados	24 horas	12 horas	Diretor de Securitização	Sistemas da CVM; página da Companhia
Infraestrutura de TI	Servidores, bases de	24 horas	4 horas	Diretor de Controles	Redundância do

Processo crítico	Descrição	RPO	RTO	Responsável	Dependências
	dados e aplicações			Internos / fornecedor de infraestrutura	fornecedor
Recuperação de <i>backups</i>	Restauração de dados críticos	4 horas	1 hora	Diretor de Controles Internos / fornecedor de <i>backup</i>	Ambiente de guarda no CNPJ da Companhia

Os valores serão confirmados ou ajustados com base nos testes do Anexo V.

Anexo III — QDD resumido para Terceiros Críticos

Aplica-se a todos os prestadores que possam afetar a disponibilidade, a segurança ou a continuidade da Companhia.

Seção A — Identificação. Nome do fornecedor; serviço prestado; contato técnico e comercial.

Seção B — Segurança da informação. (1) Possui política de segurança da informação? Anexar. (2) Realiza teste de intrusão anual por terceiro independente? Anexar o relatório mais recente. (3) Possui monitoramento 24x7? Descrever. (4) Utiliza criptografia em trânsito e em repouso? Descrever padrões. (5) Gestão de vulnerabilidades e correções: periodicidade e SLA. (6) Item obrigatório: comprovar teste de intrusão por terceiro independente nos últimos 12 meses, com evidências de mitigação das vulnerabilidades críticas; na falta, apresentar cronograma de execução em até 60 dias do início do contrato.

Seção C — Continuidade e *backup*. (1) Possui plano de continuidade e recuperação? Anexar. (2) RTO e RPO oferecidos: máximo de 24 horas cada. (3) Localização dos datacenters (jurisdição). (4) Testes de restauração realizados (data e resultado).

Seção D — Contratos e SLAs. (1) Notificação de incidentes em até 24 horas. (2) Direito de auditoria e acesso a evidências. (3) Lista de subcontratados críticos e controles aplicados.

Seção E — Proteção de dados. (1) Conformidade com a LGPD: evidências. (2) Medidas de segregação e anonimização de dados.

Seção F — Declaração. O fornecedor declara que as informações são verdadeiras e autoriza sua verificação (nome, cargo, data e assinatura do representante).

Anexo IV — Checklist de Testes e Modelo de Relatório

Checklist mínimo (a cada execução): objetivo definido (*backup*, restauração, *failover*, teste de intrusão); escopo e processos envolvidos; data e hora; responsáveis e contatos; ambiente de teste isolado, quando aplicável; procedimento de reversão; evidências coletadas (registros, capturas de tela, métricas); resultado (sucesso, falha parcial ou falha); RTO e RPO observados; lições aprendidas e plano de ação com responsáveis e prazos; aprovação do relatório pelo Diretor de Controles Internos.

Modelo de relatório (campos): título do teste; data; objetivo; escopo; responsáveis; ambiente; procedimentos executados; evidências anexas; resultado; RTO observado; RPO observado; incidentes identificados; ações corretivas (ação, responsável, prazo); aprovação (nome, cargo, data e assinatura).

Anexo V – Cronograma de Testes

#	Teste	Objetivo	Marco de referência	Responsável	Evidências
1	Backup e restauração	Verificar integridade e restauração dos dados críticos (acervo societário e regulatório)	Antes do protocolo do pedido de registro na CVM	Diretor de Controles Internos / fornecedor de backup	Relatório no modelo do Anexo IV; RTO/RPO observados
2	Continuidade de processo	Validar a continuidade de pagamentos e fluxos dos patrimônios separados	Até 30 dias após o deferimento do registro e antes da 1ª emissão	Diretor de Securitização	Relatório de execução; RTO/RPO
3	Recuperação de emissão	Simular a recuperação do workflow de emissão (documentos, assinaturas, custódia)	Antes da 1ª emissão	Diretor de Securitização	Registros, checklist, RTO observado
4	Teste de intrusão	Avaliar vulnerabilidades críticas das aplicações e do perímetro	Até 60 dias após o deferimento do registro, ou comprovação do teste do fornecedor (Anexo III)	Diretor de Controles Internos / terceiro independente	Relatório; plano de correção; evidências de mitigação
5	Exercício de comunicação de crise	Testar escalonamento e comunicação interna e externa, inclusive ao agente fiduciário	Até 90 dias após o deferimento do registro	Diretor-Presidente / Diretor de Controles Internos	Registro do exercício; lições aprendidas
6	Revisão consolidada	Consolidar resultados e aprovar plano de ação	Anual, a partir do teste 5	Diretor de Controles Internos	Relatório consolidado; aprovação

Anexo VI – Cláusulas Contratuais Mínimas para Terceiros Críticos

Os contratos com Terceiros Críticos celebrados pela HIVE SECURITIZADORA S.A., CNPJ 69.105.205/0001-38, conterão, no mínimo:

1. **Objeto e escopo:** descrição do serviço crítico e escopo técnico anexo.
2. **Níveis de serviço:** disponibilidade mínima de 99,5% mensal; RTO e RPO de até 24 horas; penalidades por descumprimento (multa, créditos de serviço ou rescisão).
3. **Segurança da informação e privacidade:** política de segurança compatível com esta Política; criptografia; gestão de vulnerabilidades; notificação de incidentes por escrito em até 24 horas da detecção, com atualizações até a resolução; conformidade com a LGPD.
4. **Auditoria e evidências:** direito de auditoria anual e extraordinária em caso de incidente, com aviso prévio de 10 dias; fornecimento de registros, relatórios e evidências de testes; subcontratação apenas com autorização prévia, permanecendo o fornecedor responsável.
5. **Continuidade e substituição:** plano de continuidade testado; plano de substituição e migração em caso de falha material.
6. **Confidencialidade:** durante a vigência e por 5 anos após o término.
7. **Seguros:** apólices adequadas, inclusive seguro cibernético quando aplicável.

8. **Vigência e rescisão:** prazo e hipóteses de rescisão por descumprimento.
9. **Foro:** Comarca de São Paulo/SP.
10. **Representação da Companhia:** assinatura na forma do Artigo 23 do Estatuto Social.

Versão	Data	Descrição
4 (SEGINFO – 001/2026)	02/09/2026	Versão anterior, assinada em 02/09/2026
5 (SEGINFO – 002/2026)	09/10/2026	Substituto do Diretor de Controles Internos (Diretor-Presidente); manifestação do art. 21 pelo Diretor de Securitização; cronograma de testes ancorado no protocolo, no deferimento e na 1ª emissão; comunicação de incidentes com dados pessoais; base normativa corrigida; <i>servicing</i> interno; anexos sem campos em branco

Aprovação

Aprovada pelo Conselho de Administração da HIVE SECURITIZADORA S.A., nos termos do Artigo 50 do Estatuto Social, em reunião realizada em 09/10/2026, data a partir da qual passa a vigorar.

Cristiano dos Santos Macedo
Presidente do Conselho de Administração e Diretor-
Presidente

Vinicius Aparecido Cremonini Gregorio
Membro do Conselho de Administração e Diretor de
Securitização

Kaio Guilherme Ferreira
Membro do Conselho de Administração e Diretor de Controles
Internos

Wilson Aparecido Mello Junior
Membro do Conselho de Administração