PLANO DE CONTINUIDADE DE NEGÓCIOS

Controle de Versões

Versão	Atualizada em	Responsável:
4	Setembro/2026	Diretoria de Compliance, Risco e PLD

Sumário

1. INTRODUÇÃO 2
2. OBJETIVO 2
3. DIRETRIZES NA PREVENÇÃO E TRATAMENTO DAS CONTINGÊNCIAS 2
4. EQUIPE DE CONTINGÊNCIA 3
5. RECUPERAÇÃO DOS NEGÓCIOS E DAS ATIVIDADES 3
6. TRATAMENTO DAS CONTINGÊNCIAS OPERACIONAIS 4
7. TESTE DE CONTINGÊNCIA 5
8. ATIVAÇÃO DE MECANISMOS DE RESPOSTA 5
9. DIVULGAÇÃO E TREINAMENTO 7
10. DISPOSIÇÕES GERAIS 7
11. VIGÊNCIA E ATUALIZAÇÃO 7
12. MANUTENÇÃO DE ARQUIVOS 7
ANEXO I 8

1. INTRODUÇÃO

A **Sonata Gestora de Recursos Ltda.** (neste documento denominada ("Sonata" ou "Gestora") apresenta o seu Plano de Continuidade de Negócios ("Plano") relacionado ao controle de acesso às informações e manutenção de sistemas, controle de acesso e segurança física, em relação aos aspectos de continuidade das suas atividades em caso de contingências.

2. OBJETIVO

Este Plano tem por objetivo estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízos para as atividades da Sonata.

Utilizando-se do disposto na Resolução CVM n.º 21/21 e na Resolução CVM n.º 175/22, no Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código ANBIMA AGRT"), bem como, as Regras e Procedimentos de Deveres Básicos da ANBIMA (art.10) e no Guia ANBIMA de Cibersegurança em suas versões atualizadas, a Sonata observou os eventos com maior possibilidade de ocorrência, buscando mitigar os riscos nos pontos de vulnerabilidade da sua estrutura de tecnologia.

Desta forma, é possível conhecer e minimizar eventuais prejuízos para com seus clientes e Colaboradores no período pós-contingência, reduzindo o tempo para a normalização de suas atividades.

Este Plano se integra a Política de Segurança da Informação, Cibernética e Proteção de Dados da Sonata.

3. DIRETRIZES NA PREVENÇÃO E TRATAMENTO DAS CONTINGÊNCIAS

Para a eficaz implementação deste Plano de Continuidade de Negócios, a Sonata busca conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade, são tomadas medidas para:

a) Conhecer e minimizar os danos no período pós-contingência;
b) Minimizar as perdas para si, seus clientes, seus sócios e colaboradores advindos da interrupção de suas atividades; e
c) Normalizar o mais rápido possível as atividades de gestão.

Em linhas gerais, os passos para execução deste plano são:

a) Identificação das interdependências entre as instalações, equipamentos e processos de negócios da Sonata com outras empresas e/ou com fornecedores e contratados;
b) Listagem das diferentes atividades da Sonata e identificação daquelas com alto interesse estratégico e/ou aquelas com elevado potencial de risco financeiro, físico ou operacional;
c) Listagem das instalações, equipamentos, fornecedores, contratados que podem representar dificuldades ou restrição à aplicação deste plano; e
d) Verificação da adequação dos meios preventivos e de proteção às

características da operação e de negócio.

Para redução e controle de eventuais perdas com contingências, todos os sócios e Colaboradores da Sonata deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

4. EQUIPE DE CONTINGÊNCIA

Para coordenar todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da Sonata, foram definidos os seguintes responsáveis pela Equipe de Contingência:

a) Diretora de Compliance, Risco e PLD: Coordenação da Contingência;
b) Diretora de Gestão de Recursos: Responsável pela definição de prioridades da área de gestão e operações a ser operada em modo de contingência; e
c) Tecnologia e Segurança de Informação: A Diretoria de Compliance, Risco e PLD é responsável por acionar a empresa terceirizada prestadora de serviços de tecnologia da informação para contingência do âmbito tecnológico.

Essa equipe deverá tomar as decisões necessárias para acionar este Plano de Continuidade de Negócios se e quando necessário, tomando essa decisão em conjunto ou, isoladamente, conforme a urgência e deve ser comunicada imediatamente a todos os colaboradores da Sonata.

Em caso de impedimento da Diretora de Compliance, Risco e PLD, a coordenação da contingência será assumida pela Diretora de Gestão, e vice-versa, observados os poderes de representação previstos no contrato social. A Equipe de Contingência manterá Árvore de Contatos (colaboradores, administradores fiduciários, custodiantes, corretoras, prestadores de TI e de sistemas, CVM e ANBIMA), atualizada semestralmente.

5. RECUPERAÇÃO DOS NEGÓCIOS E DAS ATIVIDADES

A Sonata mantém atualizados seus principais processos de negócios, de forma que, em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação e perdas de tempo e de recursos humanos, físicos e materiais possíveis.

A Sonata mantém Análise de Impacto nos Negócios (BIA), revisada anualmente, com os seguintes tempos máximos de recuperação (RTO) e de perda de dados (RPO), a validar: envio de ordens e rateio – RTO 2 horas / RPO zero; conciliação e envio de informações ao administrador fiduciário – RTO 4 horas; cálculo de risco e liquidez – RTO até o fechamento do dia (D+0); atendimento a clientes e resgates – RTO 4 horas; screening de PLD – RTO 1 dia útil; e-mail e arquivos – RPO 24 horas.

Nesse sentido, no desenvolvimento deste Plano de Continuidade de Negócios, e de acordo com a sua Política de Segurança da Informação, Cibernética e Proteção de Dados, foi levado em consideração que para recuperar todos os procedimentos e atividades realizadas diariamente, a Sonata tem todos os seus arquivos e serviços de e-mail armazenados na nuvem, bem como possui um sistema de backup diário de dados, que possibilita a

salvaguarda dos dados brutos dos usuários, imagens das estações de trabalho (planilhas, bancos de dados, etc.) e outras informações operacionais, permitindo que a Sonata recomponha rapidamente o estado operacional em caso de falhas nos discos rígidos dos equipamentos.

Logo, em caso de alguma contingência que impossibilite o acesso ao escritório da Sonata ou o seu melhor uso, todos os Colaboradores têm a capacidade de acessar todo o conteúdo de forma remota de qualquer localidade, até que a contingência seja solucionada - nos termos da Política de Segurança da Informação, Cibernética e Proteção de Dados.

A Sonata ainda conta com sistema de *nobreaks*, que possibilita a continuidade das operações em caso de algum imprevisto, "pico" ou falta de luz por uma determinada quantidade de tempo.

Ainda, para a retomada célere e eficaz das operações após uma contingência, a Sonata mantém procedimentos que a permitem:

a) Utilizar alternativas de dentro ou fora para substituição de equipamentos danificados;
b) Manter saldo financeiro e/ou acesso a crédito para qualquer despesa de contingência ou compra de equipamentos ou serviços que se fizerem necessários;
c) Manter suas atividades mesmo durante os efeitos da contingência, através de acesso remoto por parte de seus Colaboradores;
d) Retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência; e
e) Avaliar as perdas da interrupção dos negócios.

6. TRATAMENTO DAS CONTINGÊNCIAS OPERACIONAIS

Para o tratamento das contingências diretamente relacionadas com a operação dos negócios, deverão ser mantidos sempre atualizados procedimentos que permitam à empresa:

a) Aumentar rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores caso a demanda por seus serviços aumente rapidamente sem que isso implique na queda da qualidade da prestação dos serviços;
b) Substituição de algum Colaborador em caso de saída do mesmo, no menor tempo possível;
c) Manter-se sempre competitiva e inovadora, de forma a evitar a perda de sua participação no mercado, com a exploração de seus pontos fortes e com a constante diminuição de seus pontos fracos;
d) Cuidar da base de clientes, de forma que seja mantido o grau de pulverização na carteira de clientes adequado ao porte da Sonata e a manutenção da confiabilidade e qualidade dos serviços prestados;
e) Manter um fluxo de caixa que seja hábil para fazer frente às despesas imprevisíveis, tais como interrupção no fornecimento de energia elétrica; e

f) Manter seguro empresarial para o caso de algum sinistro atingir sua sede principal de maneira que fiquem paralisadas suas operações.

O Anexo I descreve os eventos e as ações mitigatórias.

7. TESTE DE CONTINGÊNCIA

Os testes de contingência serão realizados anualmente, de modo a permitir que a Sonata esteja preparada para a continuação de suas atividades.

Os testes serão os seguintes:

a) Testes dos *nobreaks*, verificando o status de funcionamento e do tempo de suporte das baterias com carga;

b) Acesso aos sistemas e aos e-mails remotamente, dos notebooks e/ou computadores de contingência;

c) Acesso aos dados armazenados;

d) Teste de restauração de backups criptografados;

e) Acionamento da Árvore de Contatos;

f) Simulação de cenário de ataque cibernético (ransomware), com restauração a partir de backup isolado; e

g) Outros testes necessários à continuidade das atividades.

O resultado de cada teste será registrado no documento nomeado de Teste de Contingência que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência, e fará parte do Relatório Anual de Controles Internos da Sonata, conforme preconiza a Resolução CVM n.º 21/21.

8. ATIVAÇÃO DE MECANISMOS DE RESPOSTA

Os Colaboradores são responsáveis por comunicar a Diretoria de Compliance, Risco e PLD sobre toda e qualquer situação que possa dar origem a uma situação que possa levar a ativação dos procedimentos de contingência indicados neste Plano.

A ativação do Plano de Contingência ficará a critério da Equipe de Contingência.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

De forma a se prevenir da maneira mais adequada, a Sonata adotará os seguintes mecanismos de resposta para cada contingência específica:

I. <u>Indisponibilidade da Sede:</u>

Caso a indisponibilidade seja superior a 4 (quatro) horas durante o expediente

de trabalho, deverá ser contratada empresa especializada para se deslocar ao local da contingência de forma a solucionar o evento ou encontrar medida alternativa, ainda que temporária. Os demais colaboradores deverão ficar à disposição e desempenhar suas funções em *home office*;

II. <u>Indisponibilidade dos Servidores</u>

Caso a indisponibilidade seja superior a 4 (quatro) horas durante o expediente de trabalho, deverá ser contratada empresa especializada para se deslocar ao local da contingência, caso a empresa terceirizada de TI da Sonata não consiga solucionar o evento ou encontrar medidas alternativas, ainda que temporárias. Os demais colaboradores deverão desempenhar suas funções por acesso remoto aos sistemas em nuvem, a partir de local com conectividade disponível;

III. <u>Indisponibilidade de Conexão por Internet com o Exterior</u>

A respectiva indisponibilidade poderá ser dividida em 02 (duas) modalidades: (i) caso a indisponibilidade seja inferior a 4 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de acesso à internet, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a respectiva conexão; e (ii) caso a indisponibilidade seja superior a 4 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de acesso à internet e ser contratada empresa especializada a ser deslocada para local de modo a restaurar a indisponibilidade ou encontrar soluções alternativas, ainda que temporária, caso a empresa terceirizada de TI da Sonata não consiga solucionar. Os demais colaboradores deverão permanecer na sede da Sonata e desempenhar suas funções;

IV. <u>Indisponibilidade de Informações sobre os Ativos Financeiros</u>

A respectiva indisponibilidade poderá ser dividida em 2 (duas) modalidades: (i) caso a indisponibilidade seja inferior a 4 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de informações, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a respectiva conexão; e (ii) caso a indisponibilidade seja superior a 4 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de informações e ser contratada empresa especializada a ser deslocada para o local de modo a restaurar a indisponibilidade ou encontrar soluções alternativas, ainda que temporária, caso a empresa terceirizada de TI da Sonata não consiga solucionar. Os demais colaboradores deverão permanecer na sede da gestora e desempenhar suas funções;

V. <u>Indisponibilidade de Prestador Crítico</u>

Em caso de indisponibilidade de administrador fiduciário, custodiante ou sistema crítico (ex.: Sonar, Comdinheiro), a Equipe de Contingência acionará o contato de contingência do prestador, adotará os procedimentos manuais alternativos previamente definidos e comunicará os clientes e demais prestadores afetados. A Sonata verificará anualmente a existência e os testes dos PCN desses prestadores.

VI. <u>Redução no Quadro de Colaboradores</u>

A Sonata avaliará a possibilidade de locomoção até o local de sua sede e determinará quais serão as funções a serem desempenhadas pelos

Colaboradores disponíveis até que se encontre soluções alternativas, mesmo que temporária. Os Colaboradores que não conseguirem se locomover à sede da Sonata deverão ficar à disposição e desempenhar suas funções em *home office;* e

VII. <u>Tempos de Resposta dos Colaboradores</u>

É de responsabilidade de cada Colaborador manter seus meios de contato atualizados e de conhecimento da Sonata. Da mesma maneira, é de responsabilidade de cada Colaborador estar acessível e comunicar suas respectivas localizações tão logo tenham conhecimento da ocorrência de um evento que possa colocar em risco a continuidade de sua função, mesmo que momentaneamente, ou, dos negócios da Sonata. Deverão, também, reportar a localização de outros Colaboradores caso tenham certeza da localização destes.

9. DIVULGAÇÃO E TREINAMENTO

Um dos fatores de primordial importância para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a Sonata definiu que serão realizadas sessões de divulgação a todos os colaboradores e envolvidos na continuidade de negócios.

A divulgação será organizada pela Diretoria de Compliance, Risco e PLD, sempre que necessário, visando manter os colaboradores atualizados sobre os conceitos de continuidade, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação dos negócios vigente.

10. DISPOSIÇÕES GERAIS

Em cumprimento à Resolução CVM n.º 21/21, o Código ANBIMA AGRT e o Guia ANBIMA de Cibersegurança o presente Plano descreve os procedimentos adotados em caso de contingências e desastres, visando sempre cumprir o dever fiduciário da Sonata, sempre com boa fé, diligência e lealdade.

11. VIGÊNCIA E ATUALIZAÇÃO

Este Plano entra em vigor na data de sua aprovação e deverá ser revisado em até 12 (doze) meses ou em prazo inferior se exigido por regulamentação específica. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

12. MANUTENÇÃO DE ARQUIVOS

Todas as revisões e evidências dos testes deverão ser arquivadas pelo período mínimo de 5 (cinco) anos.

Sem prejuízo do prazo mínimo regulatório acima referido, documentos que possam servir como meio de prova em processos judiciais ou administrativos serão conservados pelo prazo prescricional aplicável, observando-se o limite de 10 (dez) anos previsto no art. 205 do Código Civil.

ANEXO I

Evento Potencial	Probabilidade de Ocorrência	Análise de Risco	Impacto	Ações Mitigatórias de Respostas ao Evento
Impedimento do acesso físico à sede (desastres naturais, incêndio, interdição, etc.)	Baixa	Impossibilidade de acesso às estações de trabalho na sede	Alto	Sistemas rodam em servidores em "nuvem" Método de trabalho Home Office
Problemas com a Infraestrutura de comunicação da sede	Baixa	Falta de acesso ao telefone fixo ou ao e-mail corporativo	Médio	Uso de telefones celulares Comunicação aos clientes e prestadores de serviços quanto a comunicação de contingência
Problemas com infraestrutura de sistemas e rede (nuvem)	Baixa	Incapacidade de acessar o sistema ou outras ferramentas e documentos nos diretórios da rede (nuvem)	Médio	Sistemas rodam em servidores em "nuvem" Arquivos de dados com backup diário
Perda de fornecimento de energia elétrica (serviço público)	Média	Incapacidade de acesso aos sistemas ou ferramentas e documentos nos diretórios de rede (nuvem)	Alto	Computadores com nobreaks próprios que suportam de 15 (quinze) minutos a 2 (duas) horas.
Perda de fornecimento de internet (serviço privado)	Média	Incapacidade de acesso aos sistemas ou ferramentas e documentos nos diretórios de rede (nuvem)	Alto	Uso de Internet de celulares. Método de trabalho Home Office.
Falha de Equipamento	Baixa	Problema de continuidade de alguns processos	Alto	Acionamento da empresa terceirizada prestadora de serviços de tecnologia da informação.
Perda de pessoas chaves na organização	Baixa	Perda de conhecimento	Médio	Políticas e Procedimentos escritos.

		específico e potencial problema de continuidade de alguns processos		Treinamentos internos. Férias obrigatórias de no mínimo duas semanas consecutivas para funções críticas, com substituto designado, testando a continuidade dos processos.
Ataque Cibernético / ransomware	Média	Indisponibilidade ou sequestro	Alto	MFA, EDR, backup isolado e imutável, Plano de Resposta a Incidentes da SI.
Indisponibilidade de prestador crítico (administrador, sistema de boletagem / risco)	Baixa	Impossibilidade de operar ou conciliar	Alto	Contatos de contingência, procedimentos manuais, verificação anual dos PCN dos prestadores.