SIGA GESTORA DE RECURSOS LTDA

24.613.511/0001-47

Política de Continuidade dos Negócios e Contingências

15/04/2024

Sumário

Capítulo I - Introdução

A SIGA Gestora de Recursos (“SIGA” ou “Gestora”), devidamente habilitada pela Comissão de Valores Mobiliários (CVM) por meio do Ato Declaratório nº 18.281, de 27 de novembro de 2020, para atuar como gestora de recursos e distribuidora dos próprios fundos, tem o compromisso de assegurar a continuidade de suas operações e serviços em todas as circunstâncias, inclusive em situações de contingência.

Como uma entidade aderente aos mais altos padrões de governança e conformidade, a SIGA reconhece a importância crítica de manter a estabilidade e a resiliência de suas operações, garantindo a proteção dos interesses dos investidores, o cumprimento das regulamentações aplicáveis e o cumprimento dos compromissos assumidos perante a ANBIMA.

Nesse contexto, a elaboração e implementação de uma Política de Continuidade dos Negócios (“PCN”) mais robusta se torna fundamental. Reitere-se que a PCN já fazia parte do Manual de *Compliance*, Regras, Procedimentos e Controles Internos da Gestora (Capítulo 21).

Esta política tem por objetivo estabelecer diretrizes e procedimentos claros para identificar, avaliar e responder a eventos adversos que possam interromper as operações da SIGA, garantindo a rápida recuperação e a continuidade das atividades críticas.

Além disso, como parte integrante do mercado de capitais e comprometida com a excelência operacional e a ética nos negócios, a SIGA é aderente aos códigos estabelecidos pela ANBIMA, incluindo Certificação Continuada, Administração de Recursos de Terceiros, Código de Ética, Processos da Regulação e Melhores Práticas, e Distribuição de Produtos de Investimento. Essa aderência reforça nosso compromisso com a transparência, a integridade e a proteção dos interesses de nossos investidores.

A presente Política de Continuidade dos Negócios reflete o compromisso da SIGA Gestora de Recursos em manter a resiliência e a eficácia de suas operações, protegendo os ativos e

interesses de seus investidores em todas as circunstâncias, e em conformidade com as melhores práticas e regulamentações do mercado financeiro.

Capítulo II – Escopo e Abrangência

Esta PNC aplica-se a administradores, funcionários e estagiários da Gestora. No entanto, não tem o intuito de abordar toda e qualquer contingência possível.

Para fins de clareza nos procedimentos especificam-se quatro elementos-chave na infraestrutura e recursos abrangidos pelo PCN: (i) Infraestrutura Física, compreendendo a única sede da SIGA localizada em um prédio comercial na cidade de Curitiba/PR; (ii) Pessoal, abarcando os colaboradores responsáveis pela condução das operações; (iii) Infraestrutura Tecnológica, contemplando sistemas de TI, servidores e conectividade de rede; e (iv) Serviços Externos, englobando fornecedores e prestadores de serviços externos que são críticos para as operações da gestora.

A implementação deste Manual se dará de forma imediata após a aprovação da Diretoria e será revisado, no mínimo, anualmente, ou em qualquer tempo que lhe possa agregar valor, de acordo com a relevância, para que seja garantida a sua adequação.

Em caso de mudanças significativas nos negócios ou na regulação, planos devem ser alterados. Deficiências de controles internos detectadas devem ser relatadas para as áreas responsáveis por tais controles e reportadas ao Comitê de Compliance.

Revisões extraordinárias destes procedimentos, códigos, manuais e políticas poderão ocorrer em caso de situações imprevistas e/ou mudanças significativas e repentinas, também com vistas a apurar a permanência da conformidade.

Seção I – Responsabilidade

Compete ao Diretor de Risco, *Compliance* e PLDFT a gestão e a aplicação desta deste Manual.

Os instrumentos de gerenciamento de riscos da SIGA incluem estrutura de controles internos revisada periodicamente com vistas à manutenção de um adequado acompanhamento dos riscos de contingências

As funções da Diretoria de Risco, *Compliance* e PLDFT englobam: (i). Garantir que os procedimentos e práticas adotados pelos profissionais estejam de acordo com os limites internos pré-estabelecidos e com aqueles recomendados pelos órgãos reguladores, pelos princípios éticos da SIGA e do mercado; (ii). Monitoramento de riscos; e (iii) Acompanhamento da gestão de valores mobiliários vis à-vis aos seus respectivos mandatos, regras e diretrizes.

O Comitê de Gestão de Riscos ("Comitê") é responsável por avaliar a PNC e instaurar o Comitê de Contingências, quando necessário, para determinar as diretrizes quando da ocorrência de qualquer evento de contingência. Este Comitê é formado por profissionais da área de Gestão de Recursos de Terceiros, que apresentam os ativos pretendidos, e pela Diretoria de Risco, Compliance e PLDFT, que analisa o enquadramento da operação nas políticas internas, normas legais e (auto)reguladoras e regulamentos.

O monitoramento ocorre sobre atividades contínuas e regulares para aferir a efetividade dos Planos de Contingências e permite detectar problemas identificados pelas ocorrências e eventos de exceção, qualitativamente pela análise de sua causa-raiz e quantitativamente pelos parâmetros de performance.

Capítulo III – Análise de Riscos e Vulnerabilidades

A PNC demonstra, sumariamente, as medidas básicas a serem tomadas, em caso de qualquer interrupção dos negócios. Esta política deve garantir a capacidade da SIGA em operar constantemente e em bases contínuas.

O Plano de Contingências e Continuidade de Negócios visa assegurar comunicação entre os membros da equipe, clientes e fornecedores, bem como com os reguladores, de modo a

permitir o gerenciamento das garantias, enquadramento de posições, revisões de exposição à riscos e movimentações de ativos.

O Comitê de Contingência será o responsável por encaminhar e informar a todos sobre os procedimentos adotados. Em síntese, serão tratados os planos que envolvem quatro grupos de contingência: a) Infraestruturas Físicas; b) Pessoal; c) Infraestruturas Tecnológicas; d) Serviços Externos.

Seção I – Infraestruturas Físicas e Tecnológicas

Impedimento de Acesso na Sede: Risco de impedimento ou restrição de acesso às instalações da sede da SIGA devido a eventos como desastres naturais, incidentes de segurança ou problemas de infraestrutura urbana.

Danos Físicos às Instalações ou Equipamentos Elétricos: Possibilidade de danos físicos às instalações da SIGA, incluindo incêndios, inundações, vandalismo ou acidentes, que possam comprometer a operacionalidade das instalações ou danificar equipamentos elétricos essenciais.

Falha no Fornecimento de Energia Elétrica: Risco de interrupção no fornecimento de energia elétrica à sede da SIGA, seja por falhas na rede elétrica local, cortes programados ou desligamentos não programados.

Falha no Fornecimento de Telefone e Internet: Possibilidade de interrupção nos serviços de telefone e internet, seja por falhas técnicas nos provedores de telecomunicações, problemas de infraestrutura de rede ou ataques cibernéticos.

Incidentes Cibernéticos: Os riscos de incidentes cibernéticos referem-se às ameaças relacionadas à segurança da informação e à integridade dos sistemas de tecnologia da informação da Siga. Isso inclui ataques de hackers, malware, phishing, ransomware, entre outros. Tais incidentes podem comprometer a confidencialidade, integridade e disponibilidade dos dados e sistemas, resultando em perdas financeiras, danos à reputação e interrupção das operações normais da organização.

Volatilidade do Mercado: Os riscos de volatilidade de mercado dizem respeito à possibilidade de flutuações significativas e imprevisíveis nos preços dos ativos financeiros, como ações, títulos, commodities e moedas. Essas flutuações podem ser causadas por uma variedade de fatores, incluindo eventos econômicos, políticos, sociais e geopolíticos, bem como mudanças nas condições de oferta e demanda nos mercados financeiros globais. A volatilidade de mercado pode afetar negativamente o desempenho dos investimentos e aumentar o risco de perdas para os investidores.

Falhas de Sistemas e Tecnologia: Os riscos de falhas de sistemas e tecnologia envolvem a possibilidade de interrupções ou mau funcionamento dos sistemas de tecnologia da informação e comunicação da SIGA. Isso pode incluir falhas de hardware, software, redes, servidores e outros componentes de infraestrutura de TI. As falhas de sistemas e tecnologia podem resultar em tempo de inatividade não planejado, perda de dados, interrupção das operações comerciais e impacto negativo nos serviços prestados aos clientes.

Seção II – Pessoal e Prestadores de Serviços

Licenças Médicas e Correlatas e Impossibilidade de Comparecimento: Risco de ausência temporária de colaboradores devido a licenças médicas, licenças maternidade/paternidade ou outras questões de saúde, impactando a capacidade da SIGA de manter suas operações normais.

Greves de Transportes Públicos: Possibilidade de paralisação dos serviços de transporte público, como ônibus, trens ou metrô, que podem afetar a mobilidade dos colaboradores e prejudicar o funcionamento regular da empresa.

Capítulo IV – Formas Alternativas para Processamento em Situações de Contingência

Considerando os riscos identificados na análise anterior, a SIGA Gestora de Recursos estabelece formas alternativas para o processamento de suas operações em situações de contingência. Abaixo estão as medidas específicas adotadas para cada um dos riscos mencionados:

Seção I – Infraestruturas Físicas e Tecnológicas

Impedimento de Acesso na Sede: (i) Implementação de um plano de trabalho remoto para os colaboradores, permitindo que realizem suas atividades fora da sede da empresa utilizando recursos de comunicação online, como videoconferências e ferramentas de colaboração em nuvem.

Danos Físicos às Instalações ou Equipamentos Elétricos: (i) Ativação de um local de contingência previamente identificado, onde a equipe possa se reunir e continuar as operações críticas da empresa enquanto os danos são reparados na sede principal; (ii) Utilização de equipamentos de reserva ou serviços de terceiros para substituir equipamentos danificados até que possam ser reparados ou substituídos.

Falha no Fornecimento de Energia Elétrica: (i) Utilização de geradores de energia ("no-break") como fonte alternativa para manter as operações essenciais em funcionamento durante uma interrupção no fornecimento de energia elétrica; e (ii) Implementação de procedimentos para migrar operações críticas para uma localização com fornecimento de energia elétrica contínuo, se necessário.

Falha no Fornecimento de Telefone e Internet: (i) Uso de pontos de acesso alternativos à internet, como conexões de dados móveis ou redes Wi-Fi de emergência, para garantir a conectividade dos colaboradores em caso de falha na conexão principal; e (ii) Utilização de sistemas de comunicação offline, como telefones celulares ou rádios, para manter a comunicação interna durante uma interrupção nos serviços de telefone e internet.

Riscos de Incidentes Cibernéticos: (i)implementação de medidas de segurança cibernética robustas, incluindo firewalls, antivírus, sistemas de detecção de intrusos e criptografia de dados; e (ii) Realização de backups regulares dos dados críticos e desenvolvimento de um plano de recuperação de desastres para restaurar sistemas e dados em caso de violação de segurança.

Volatilidade do Mercado: (i) Estabelecimento de procedimentos de monitoramento de mercado em tempo real para identificar rapidamente tendências emergentes e eventos que possam impactar os fundos sob gestão; e (ii) Desenvolvimento de estratégias de mitigação de risco, como ajustes na alocação de ativos e utilização de instrumentos de proteção, para proteger os interesses dos investidores durante períodos de volatilidade.

Falhas de Sistemas e Tecnologia: (i) Implementação de sistemas redundantes e de backup para garantir a disponibilidade contínua de sistemas críticos, minimizando o tempo de inatividade em caso de falha; e (ii) Estabelecimento de procedimentos de resposta a incidentes para identificar, isolar e resolver rapidamente problemas técnicos que possam afetar as operações da gestora.

Seção II – Pessoal e Prestadores de Serviços

Licenças Médicas e Correlatas: (i) Realocação temporária de tarefas e responsabilidades entre os membros da equipe para cobrir as ausências dos colaboradores devido a licenças médicas; (ii) Contratação de mão de obra temporária ou terceirizada para preencher lacunas de pessoal críticas durante períodos prolongados de ausência; (iii) Identificação de prestadores de serviços alternativos que possam ser acionados rapidamente para substituir o prestador original em caso de impossibilidade de cumprir suas obrigações.

Greves de Transportes Públicos: (i) Facilitação do trabalho remoto para colaboradores afetados pela paralisação dos transportes públicos, permitindo-lhes realizar suas tarefas remotamente sem a necessidade de deslocamento físico para o escritório; e (ii) Coordenação de esquemas de transporte alternativo, como serviços de carona solidária ou fretamento de vans, para garantir a mobilidade dos colaboradores durante uma greve de transporte público.

Capítulo V – Procedimentos de Ativação e Designação de Equipes

A SIGA Gestora de Recursos estabelece procedimentos claros para a ativação de medidas de contingência e a designação de equipes responsáveis pela implementação dessas medidas, sem prejuízo do disposto no capítulo que trata sobre as responsabilidades.

A ativação das medidas de contingência ocorre sob a supervisão do Comitê de Gestão de Riscos, convocado a qualquer tempo por qualquer membro, que avalia a necessidade de instaurar o Comitê de Contingências em caso de eventos adversos que possam impactar as operações da SIGA.

O Comitê de Contingências é convocado conforme necessário para avaliar a situação, determinar a gravidade do evento e estabelecer diretrizes para a ativação das medidas de contingência.

Após a ativação das medidas de contingência, equipes específicas são designadas para implementar as ações necessárias para garantir a continuidade das operações da SIGA.

A Diretoria de Risco, Compliance e PLDFT desempenha um papel fundamental na designação das equipes, garantindo que os profissionais designados possuam as habilidades e conhecimentos necessários para lidar com a situação de contingência de forma eficaz, sem que haja qualquer descumprimento às políticas de segregação da Gestora.

As equipes designadas são responsáveis por executar as tarefas atribuídas conforme as diretrizes estabelecidas pelo Comitê de Contingências, garantindo uma resposta coordenada e eficiente diante de eventos adversos.

Para perfectibilizar os procedimentos, entende-se que a comunicação eficaz é essencial durante a ativação das medidas de contingência. As equipes designadas são orientadas a manter uma comunicação regular e transparente, relatando o status das operações e qualquer desenvolvimento relevante ao Comitê de Contingências e à alta administração da SIGA.

A Diretoria de Risco, Compliance e PLDFT coordena as atividades das equipes designadas, garantindo uma resposta unificada e coordenada em situações de contingência.

A implementação eficaz dos procedimentos de ativação e designação de equipes permite que a SIGA Gestora de Recursos responda de forma ágil e eficiente a eventos adversos, garantindo a continuidade das operações e a proteção dos interesses dos investidores.

Capítulo VI – Recursos e Infraestrutura de Suporte

A SIGA reconhece a importância crítica de contar com recursos e infraestrutura de suporte adequados para garantir a eficácia das medidas de contingência. Esta seção destaca os recursos e a infraestrutura essenciais que apoiam a implementação do Plano de Continuidade de Negócios (PCN).

a. Recursos Humanos: A SIGA mantém uma equipe capacitada e treinada para responder de forma eficaz a situações de contingência. Essa equipe é composta por profissionais qualificados em diversas áreas, incluindo gestão de investimentos, tecnologia da informação, operações e conformidade regulatória. Além da equipe interna, a SIGA pode contar com consultores externos especializados, quando necessário, para fornecer suporte adicional durante eventos de contingência.

b. Infraestrutura Tecnológica: A infraestrutura tecnológica da SIGA é projetada para garantir a disponibilidade contínua de sistemas críticos, mesmo em situações de contingência. Isso inclui servidores redundantes, sistemas de backup e procedimentos de recuperação de desastres para proteger os dados e as operações da empresa. A SIGA também mantém contratos de suporte com fornecedores de tecnologia confiáveis, garantindo acesso a recursos técnicos adicionais em caso de necessidade.

c. Infraestrutura Física: As instalações físicas da SIGA são projetadas para garantir a segurança e o funcionamento contínuo das operações da empresa. Isso inclui medidas

de segurança física, como sistemas de alarme, controle de acesso e procedimentos de evacuação em caso de emergência.

d. Serviços Externos: A SIGA possui parcerias estratégicas com fornecedores de serviços externos, incluindo provedores de telecomunicações, fornecedores de energia elétrica e provedores de serviços de nuvem. Essas parcerias garantem o acesso a recursos adicionais e suporte técnico em caso de falha nos serviços essenciais.

A disponibilidade de recursos e infraestrutura de suporte adequados é fundamental para garantir a eficácia do Plano de Continuidade de Negócios da SIGA. Ao manter uma equipe capacitada, investir em infraestrutura tecnológica e física robusta e estabelecer parcerias estratégicas com fornecedores confiáveis, a Gestora está preparada para enfrentar e superar desafios emergenciais, garantindo a continuidade das operações e a proteção dos interesses dos investidores.

Capítulo VII – Testes e Revisões

A SIGA Gestora de Recursos reconhece a importância crítica da realização de testes regulares e revisões periódicas do Plano de Continuidade de Negócios (PCN) para garantir sua eficácia e relevância contínua. Esta seção destaca os processos de testes e revisões adotados pela SIGA:

Testes do Plano de Continuidade de Negócios: A SIGA conduz testes regulares do PCN para avaliar a prontidão e eficácia das medidas de contingência em várias situações. Os testes são planejados e coordenados pelo Comitê de Gestão de Riscos.
Os cenários de teste abrangem uma variedade de eventos de contingência, incluindo falhas de sistemas, interrupções de serviços e situações de emergência física, permitindo à SIGA avaliar sua capacidade de resposta em diferentes cenários.

Revisões Periódicas do Plano de Continuidade de Negócios: A SIGA realiza revisões periódicas do PCN para garantir que esteja alinhado com as mudanças nas operações da

empresa, regulamentações aplicáveis e melhores práticas do setor. As revisões são conduzidas pelo Comitê de Gestão de Riscos e Ativos, juntamente com a Diretoria de Risco, Compliance e PLDFT, para identificar áreas de melhoria e oportunidades de aprimoramento do PCN.

As revisões também consideram feedbacks de testes anteriores, lições aprendidas com eventos reais de contingência e avaliações de risco atualizadas para garantir a relevância e eficácia contínua do PCN.

Atualização do Plano de Continuidade de Negócios: Com base nos resultados dos testes e revisões, a SIGA realiza atualizações e aprimoramentos contínuos do PCN para garantir sua eficácia em face de novos desafios e ameaças emergentes. As atualizações são comunicadas a todas as partes relevantes da organização e incorporadas ao treinamento e preparação das equipes designadas.

Capítulo VIII – Disposições Gerais

Em caso de dúvidas de interpretação ou eventuais antinomias entre as regras aqui dispostas e outras vigentes na entidade, deverá haver consulta imediata ao Diretor de Risco, *Compliance* e PLDFT. Quaisquer alterações legais ou normativas expedidas pelos órgãos regulamentadores e competentes serão aplicadas imediatamente a esta política, e todos os colaboradores serão imediatamente alertados de eventuais mudanças.

Eventuais dúvidas deverão ser encaminhadas à Diretoria de Risco, Compliance e PLDFT, por intermédio do e-mail matheus.cardoso@sigafinance.com.br ou pelo telefone (41) 3044-7464