SPC GRAFENO

POLÍTICA DE GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

SPC GRAFENO INFRAESTRUTURA E TECNOLOGIA PARA O SISTEMA FINANCEIRO S.A.

SUMÁRIO

1. OBJETIVO

Esta Política de Gerenciamento de Riscos (“Política”), aplicável à SPC Grafeno Infraestrutura e Tecnologia para o Sistema Financeiro S.A. ("Companhia"), tem por objetivo apresentar e estabelecer os princípios e diretrizes de gestão dos riscos, pelos quais visa disseminar e fortalecer a cultura do tratamento do risco entre seus Colaboradores, Participantes e Fornecedores, incluindo também processos de identificação, avaliação, mensuração, controle, mitigação, monitoramento e reporte, dos riscos, bem como estabelecer os respectivos papéis e responsabilidades em seus diversos níveis.

2. ABRANGÊNCIA

Os procedimentos descritos nesta Política são aplicáveis à Companhia, a todos os seus Colaboradores, e Prestadores de Serviços Terceirizados. Esta Política deverá ser amplamente divulgada dentro da Companhia e disponibilizada a todos os integrantes e *stakeholders* do processo.

3. DOCUMENTOS DE REFERÊNCIA

- Código de Ética e Conduta
- Política de Governança e Compliance
- Plano de Continuidade de Negócios
- Política de Gestão de Terceiros
- Política de Segurança da Informação e Cyber
- Política de Gestão de Fraudes
- Manual de Riscos e Controles Internos
- Declaração de Apetite por Riscos (RAS)
- Resolução BCB 304/2023 – Regulamenta a atividade de Registro de Ativos
- Lei n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais
- *Principles for Financial Market Infrastructures* – BIS/IOSCO

4. ALÇADAS DE APROVAÇÃO

- Comitê de Riscos, Compliance e SI – responsável pela revisão e aprovação da Política
- Conselho de Administração – responsável pela aprovação final da Política.

5. DIRETRIZES

5.1 CONCEITOS GERAIS

O processo de gestão de riscos visa assegurar que os responsáveis pela tomada de decisão, em todos os níveis da Companhia, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais ela está exposta, de forma a aumentar a qualidade no alcance dos seus objetivos e reduzir os riscos a níveis aceitáveis. Visa, também, preservar o patrimônio, a segurança das pessoas e a integridade do meio ambiente e comunidades, por meio da melhoria dos processos, do controle adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

A estrutura de controle é compatível com a natureza de suas operações, complexidade dos seus produtos e serviços, atividades, processos, sistemas e a dimensão de sua exposição aos riscos.

A Política de Gerenciamento de Riscos e Controles Internos está alinhada aos objetivos estratégicos da Companhia, às melhores práticas do mercado, em conformidade com leis e regulamentos emitidos por Órgãos Reguladores.

5.2 ATRIBUIÇÕES E RESPONSABILIDADES

A Companhia dispõe de estrutura organizacional e administrativa efetiva e transparente, de modo a possibilitar, inclusive, a avaliação do desempenho dos administradores e contemplar os interesses dos participantes.

5.2.1. Conselho de Administração

- Aprovar regulamentos, políticas, planos, e manuais da Companhia, bem como quaisquer mudanças e atualizações com relação a tais documentos;
- Aprovar o apetite e tolerância ao risco (RAS) para cada uma das categorias, no âmbito do direcionamento estratégico;
- Aprovar a Matriz de Riscos, os Planos de Tratamento dos Riscos e o Planos de Contingência.
- Manifestar-se sobre relatório e as contas da Diretoria, bem como sobre as demonstrações financeiras do exercício que deverão ser submetidas à Assembleia Geral Ordinária;
- Escolher e destituir auditores independentes da Companhia, bem como indicar aos mesmos as diretrizes, normas e prazos a serem seguidos para a prestação de informações;
- Aprovar qualquer mudança substancial e materialmente relevante nas políticas contábeis da Companhia;
- Manifestar-se acerca das recomendações feitas pelo Comitê de Auditoria para contratação ou substituição de auditor independente e da auditoria interna ou externa;
- Instalação e regulamentação de comitês de assessoramento ao Conselho de Administração, incluindo o regimento interno do Comitê de Auditoria.

5.2.2. Comitê de Gestão de Crise e de Risco Operacional

- Decidir pela decretação do estado de contingência operacional;
- Acionar as pessoas envolvidas no Plano de Contingência de Negócios (“PCN”);

- Acompanhar todos os eventos de crise auxiliando as necessidades dos envolvidos, de modo a garantir eficiência na condução dos processos;
- Garantir a execução dos planos de continuidade e resposta a crises;
- Avaliar a adequação das medidas tomadas em contingência às políticas, normas e regulação em vigor;
- Receber relatórios sobre o evento uma vez que tenha sido desmobilizado o time de crise;
- Reavaliar e executar medidas de contenção de riscos para a reputação da Companhia;
- Responder de forma imediata a eventos que coloquem em risco a integridade física dos colaboradores, fornecedores e terceiros que possuam parceria comercial com a Companhia;
- Garantir a execução do plano de comunicação interno e externo;
- Garantir que seja realizada a comunicação com clientes e fornecedores chaves;
- Elaborar relatórios pós-crise, ressaltando lições aprendidas.

5.2.3. Comitê de Riscos, Compliance e SI

- Avaliar e monitorar as exposições de riscos da Companhia, promovendo seu gerenciamento, de acordo com as políticas vigentes;
- Tomar ciência de riscos corporativos;
- Acompanhar as atividades da auditoria interna e da área de controles internos da Companhia;
- Assegurar a conformidade de rotinas, práticas e procedimentos com as políticas, regras, regulamentos e leis aplicáveis;
- Apreciar os relatórios emitidos pelos Órgãos Reguladores e Auditorias;
- Manter registros de suas deliberações e decisões; e
- Receber e avaliar relatório enviados produzidos para verificação dos controles, sua efetividade e consistência com a natureza, nível de risco das operações realizadas pela Companhia.

5.2.4. Diretoria de Riscos, Controles Internos, Compliance e SI

- Disseminar a cultura orientada à gestão e controles dos riscos, tendo como principal objetivo a redução de eventos e perdas associados aos riscos;
- Implementar processo contínuo, integrado e abrangente para a gestão dos riscos da Companhia;
- Assegurar que as políticas, procedimentos e métricas de gestão de riscos estejam alinhadas com o apetite e tolerância ao risco (RAS) da Companhia;
- Implementar procedimentos e controles com o principal objetivo de mitigar ou, sempre que possível, eliminar os riscos de inadequação ou deficiência em contratos firmados pela Companhia;
- Implementar as melhores práticas para gestão e controle dos riscos operacionais, mantendo atualizada uma base de eventos de perdas;

- Implementar a Gestão de Continuidade de Negócios, de forma a conduzir testes periódicos e assegurar a manutenção dos processos críticos da Companhia em potenciais incidentes ou eventos de crise;
- Testar e avaliar a aderência da Companhia perante os normativos regulatórios vigentes sobre o Gerenciamento de Riscos e Controles;
- Implementar processos de gerenciamento de terceiros relevantes, durante a contratação de serviços, bem como durante a vigência do relacionamento;
- Avaliar previamente os riscos sobre novos produtos e serviços, alterações relevantes em processos, sistemas ou modelo de negócio da Companhia.

5.2.5. Diretoria de Tecnologia, Dados e Inovação

- Garantir o bom funcionamento de todos os componentes de tecnologia da informação, sobretudo no que diz respeito à resiliência a eventos de risco operacional;
- Participar da elaboração, implementação, revisão e testes periódicos do Plano de Contingência de Negócios e de Recuperação de Desastres, juntamente com as demais áreas da Companhia;
- Assegurar a implementação do Plano de Contingência de Negócios em todos os aspectos relacionados à infraestrutura de tecnologia da informação;
- Estabelecer processo contínuo, integrado e abrangente de gestão de segurança de informação da Companhia;
- Assegurar a integridade, a segurança e a disponibilidade dos dados e dos sistemas de informação utilizados pela Companhia, em linha com as Política de Segurança da Informação e Cibernética;
- Implementar mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

5.2.6. Diretoria de Operações

- Auxiliar no processo de elaboração, padronização, revisão anual, aprovação e publicação de políticas institucionais, especialmente o Plano de Continuidade do Negócio;
- Estabelecer controles mitigatórios de riscos nas operações da Registradora.

5.2.7. Auditoria

- Avaliar e auditar periodicamente e sempre que houver mudanças significativas, os processos relativos ao gerenciamento de riscos e controles internos, como parte do processo de auditoria interna.

5.2.8. Demais Colaboradores

- Implementar as melhores práticas de gestão de riscos operacionais em todas as atividades desempenhadas, consoante com a presente Política e demais comunicados, treinamentos

e orientações emanados do Conselho de Administração, da Diretoria, do Comitê de Gestão de Crise e de Risco Operacional e de todas as demais áreas envolvidas na gestão dos riscos da Companhia; e

- Comunicar, tempestivamente, à Área de Riscos, CI e Compliance todo e qualquer evento de risco operacional.

6. ESTRUTURA DA GESTÃO DE RISCOS E CONTROLES INTERNOS

A Companhia está alinhada com o modelo do IIA (Instituto de Auditores Interno) sobre a aplicação da estrutura de Três Linhas, para o Gerenciamento de Riscos e Controles e tomada de decisões.

O modelo apresenta a estrutura de Governança da Companhia (Corpo Administrativo) como sendo responsável pela prestação de contas aos *stakeholders* pela supervisão organizacional, atuando com integridade, liderança e transparência e em seguida, as três linhas com os papéis de responsabilidade para o atingimento dos objetivos organizacionais (primeira e segunda) e a avaliação e assessoria independente sobre a adequação e eficácia da governança e gerenciamento dos riscos (terceira linha).

- **Primeira linha:** Representa as ações de gerenciar riscos pelas áreas operacionais da Companhia (fornecimento de produtos e serviços aos clientes). São responsáveis pela identificação, avaliação, reporte e controle dos riscos inerentes às suas atividades;
- **Segunda linha:** Representa as ações de gerenciar riscos, fornecendo a *expertise*, apoio, monitoramento e questionamento sobre questões relacionadas a riscos, para a primeira linha. As áreas de Compliance, Riscos, Controles e Segurança da Informação, atuam nesse papel; e
- **Terceira linha:** Representa a avaliação independente da Auditoria Interna com o papel de avaliar e assessorar as questões relativas ao atingimento dos objetivos.

Essas responsabilidades estão diretamente atreladas à estratégia da Companhia, seus respectivos gestores e equipes. O programa de disseminação da cultura de riscos enfatiza a necessidade do gerenciamento, tempestivo, dos riscos das instituições em todos os seus processos, possibilitando efetivamente o funcionamento correto do modelo.

Os riscos inerentes da Companhia são identificados, avaliados e gerenciados com uma abordagem *top-down*. Já o mapeamento de riscos e identificação dos controles nos processos de negócios, são realizados pela abordagem *bottom up.*

A estrutura de gerenciamento de riscos da Companhia está sob responsabilidade do Diretor de Riscos, CI, Compliance e SI, o qual detêm a independência necessária para cumprimento de suas funções. A Auditoria também opera de maneira independente e é responsável pela supervisão da estrutura de gerenciamento de riscos.

7. PROCESSO DE GESTÃO DE RISCOS

O processo da gestão de riscos considera a identificação do perfil de exposição e tolerância a riscos (apetite por risco) através da avaliação do ambiente interno e externo.

Os principais componentes do processo de gestão de riscos da Companhia são:

- **Identificação dos eventos:** Consiste em identificar e classificar os eventos de risco a que a Companhia está exposta, indicando áreas de incidência, causas e potenciais impactos financeiros associados aos processos, produtos e serviços.

  Com base nos macroprocessos e processos das áreas claramente definidas e registradas no inventário de processos, cria-se o cronograma de mapeamento com as áreas, de acordo com a complexidade dos temas e prioridade conforme a governança estipulada.

- **Avaliação dos riscos:** Consiste em dimensionar e quantificar a exposição ao risco com o objetivo de avaliar o impacto nos negócios da Companhia. Pode, também, envolver uma avaliação qualitativa dos riscos identificados, estimando sua probabilidade de ocorrência e impacto de forma a determinar o nível de apetite ao risco. A Companhia tem parametrizada e aprovada a Matriz de Riscos e Controles, de modo a permitir uma rápida e fácil classificação dos riscos quanto ao seu nível de impacto (crítico, alto, moderado e baixo) e probabilidade de ocorrência (baixa, moderada, alta e crítica) resultando na classificação de níveis de riscos:

  - **Risco Crítico:** Os riscos críticos são aqueles com uma probabilidade muito alta de ocorrer e um impacto extremamente grave nas operações ou nos objetivos da Companhia. Eles representam uma ameaça iminente à sobrevivência ou à capacidade da organização de atingir seus objetivos estratégicos. A gestão de riscos deve priorizar esses riscos e implementar medidas robustas de mitigação para minimizar sua probabilidade de ocorrência e seu impacto;

  - **Risco Alto:** Riscos que têm uma probabilidade significativa de ocorrer e um impacto substancial nas operações ou nos objetivos da Companhia. Esses riscos podem representar uma ameaça significativa para o sucesso da organização e geralmente exigem a implementação de medidas de mitigação para reduzir sua probabilidade ou impacto e evitar consequências graves;

  - **Risco Moderado:** Riscos que têm uma probabilidade moderada de ocorrer e um impacto moderado nas operações ou nos objetivos da Companhia. Embora não sejam tão preocupantes quanto os riscos altos ou críticos, ainda exigem atenção e podem necessitar de medidas de mitigação para reduzir sua probabilidade ou impacto;

  - **Risco Baixo:** Riscos considerados de baixa prioridade devido à sua baixa probabilidade de ocorrência e ao impacto limitado que teriam nas operações ou nos objetivos da Companhia. Esses riscos geralmente podem ser tolerados sem a necessidade de medidas de mitigação significativas.

Os critérios para avaliação do impacto e probabilidade estão relacionados no **Anexo I – Critérios para avaliação de impacto e probabilidade** e o quadrante de riscos definido para a Companhia, consta no **Anexo III – Quadrante de Riscos**, desta Política.

- **Atividades de controle:** Acompanhar os pontos vulneráveis de possíveis eventos de risco. Dada a ocorrência de algum evento, deve-se cadastrar os eventos, junto com a sua classificação de fator de risco e frequência pelas áreas responsáveis. Dessa forma, a área de Riscos e Controles Internos pode dimensionar e verificar se os níveis dos riscos estão aderentes ao apetite de risco da Companhia, além de criar mecanismos que garantam a eficiência dos controles.
- **Mitigação de Riscos:** Consiste em criar e implementar mecanismos para modificar o risco buscando reduzir as perdas operacionais por meio da remoção da causa do risco, alteração da probabilidade de ocorrência ou alteração das consequências do evento de risco.

  Após a conclusão do mapeamento e identificados os riscos, a área de Riscos e Controles Internos sugere ações com o intuito de mitigá-los. As soluções para mitigação dos riscos devem ser específicas e factíveis e podem contemplar desde revisão de processos e inclusão de controles em sistemas, criação de relatórios e indicadores de desempenho, confecção de políticas e procedimentos, implantação de mecanismos de monitoramento e controle, até alteração de competências e atribuições de uma área ou de instrumentos de governança.
- **Informações e Comunicações:** A gestão dos riscos se torna eficaz quando há um diálogo regular entre a área de Riscos e Controles Internos e cada unidade de negócio, resultando em uma missão compartilhada de equilibrar a conformidade com a eficiência operacional.

  As informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos os níveis da organização.
- **Monitoramento:** A integridade da gestão de riscos e controles internos é monitorada e são realizadas as modificações necessárias, sempre que aplicável. O monitoramento é realizado através de atividades gerenciais contínuas em todas as áreas, automações/alertas para responsáveis ou avaliações independentes ou de todas as formas. Sendo aplicados testes periódicos para avaliar a qualidade dos controles e mitigadores de riscos.

7.1. DECLARAÇÃO DE APETITE POR RISCOS (RAS)

A SPC Grafeno é conservadora em seu apetite por riscos, agindo de acordo com o documento Declaração de Apetite por Riscos (RAS), devidamente aprovado pelo Conselho de Administração, para alcançar objetivos estratégicos, empregando princípios sólidos de gerenciamento, decisões transparentes e comunicação efetiva para priorizar a gestão de riscos.

O apetite por riscos, neste contexto, refere-se aos tipos e níveis de riscos que a SPC Grafeno se dispõe a admitir na realização das suas atividades e objetivos.

A Declaração de Apetite por Riscos reforça a cultura de riscos ao possibilitar a disseminação do conhecimento sobre os principais aspectos do apetite por riscos da SPC Grafeno a todos os seus membros, devendo ser revisada anualmente, ou sempre que necessário, pelo Comitê de Riscos, Compliance e SI e aprovada pelo Conselho de Administração.

8. DICIONÁRIO DE RISCOS

O dicionário de riscos é um documento que contém informações detalhadas sobre os diversos tipos de riscos que SPC Grafeno pode enfrentar. Ele fornece uma compreensão abrangente dos riscos que podem afetar as operações, os projetos e os objetivos estratégicos da Companhia. O dicionário de riscos está relacionado no **Anexo II – Dicionário de Riscos, desta Política.**

Ao realizar o mapeamento e a identificação dos riscos, as seguintes categorias de riscos são consideradas na Companhia, em linha com a Resolução nº 304/23 do Banco Central do Brasil:

- **Risco Operacional:** Os riscos operacionais gerenciados pela Companhia, incluem riscos à integridade dos dados, à segurança dos dados e à continuidade dos negócios, além disso considera as "deficiências de sistemas tecnológicos ou nos processos internos, erros humanos, falhas de gestão ou perturbações causadas por eventos externos que resultem na redução, deterioração ou interrupção dos serviços fornecidos no âmbito de um sistema do mercado financeiro.
- **Risco Geral Do Negócio:** a Companhia mantém o controle para identificar, monitorar e gerenciar riscos gerais de negócios, incluindo perdas por má execução da estratégia de negócios, fluxos de caixa negativos ou despesas operacionais inesperadas e excessivamente grandes. Além disso, a Companhia mantém planos de contingência para casos em que os recursos disponíveis sejam insuficientes para suportar as perdas decorrentes desses riscos gerais do negócio. Adicionalmente, existe o monitoramento para que os ativos mantidos pela Companhia possuam alta qualidade e liquidez adequada para mitigar riscos gerais de negócios, com o objetivo de assegurar que a Companhia seja capaz de honrar suas despesas operacionais presentes e futuras, mesmo diante de desafios do mercado.
- **Risco Estratégico:** O processo de monitoramento atende os ciclos de avaliação dos planejamentos estratégicos correspondentes, de modo que essas atividades possam se integrar e contribuir harmonicamente com as atividades de elaboração, monitoramento, avaliação e revisão destes planejamentos, para o devido alcance dos objetivos estratégicos da Companhia.
- **Risco de Imagem/Reputacional:** O Código de Ética e Conduta da Companhia, expressa a responsabilidade de todos os colaboradores para a preservação da imagem e da marca da SPC Grafeno, procurando-se evitar qualquer desgaste em razão de publicidade negativa e reputação perante clientes, concorrentes e reguladores.
- **Risco Regulatório / Legal:** A Companhia considera que riscos Regulatório ou de Compliance e Legal se referem a potenciais litígios, investigações e processos regulatórios inerentes às suas atividades, gerando assim possíveis riscos de sanções legais ou regulatórias, multas ou penalidades, perda financeira ou danos à reputação resultantes do incumprimento de leis, regulamentos, regras ou outros requisitos regulamentares.
- **Risco Financeiro:** A Companhia mantém o monitoramento constante sobre possíveis impactos nos fluxos de caixa e, quando pertinente, no capital, com o objetivo de assegurar uma gestão contínua e efetiva dos riscos comerciais da Companhia. Além disso, a

Companhia incorpora o capital em conformidade com os padrões internacionais de capital baseados em riscos, como parte de uma estratégia abrangente para mitigar os riscos gerais de negócios, reforçando sua solidez financeira e a capacidade de enfrentar desafios em suas atividades comerciais.

9. CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da Companhia e suas atividades de valor agregado.

Estes itens estão abordados no Plano de Continuidade do Negócio (“PCN”), que contempla as ações gerenciais e operacionais que visam garantir a continuidade dos negócios, considerando o tempo necessário de retorno dos processos críticos. Neles encontram-se formalizados a metodologia, a definição dos conceitos, o estabelecimento de responsabilidades bem como os demais procedimentos relacionados consoantes com as boas práticas e regulamentações dos Órgãos Reguladores.

9.1. PROCESSOS CRÍTICOS

O Business Impact Analysis (BIA) é uma parte fundamental do Plano de Continuidade de Negócios Corporativo. O BIA é um processo sistemático que identifica e avalia o impacto potencial de interrupções nos processos críticos de negócios. Ele examina a dependência de recursos, a recuperação necessária e os prazos para retomar as operações normais após uma interrupção.

Para realizar o BIA, a equipe de Riscos e Controles conduz entrevistas e realiza análises detalhadas com as áreas de negócios. O resultado desse processo é um formulário que classifica os processos de acordo com sua criticidade e estabelece as prioridades para a recuperação.

O BIA é revisado anualmente para garantir que reflita com precisão as mudanças em nossos processos de negócios, tecnologias e riscos, garantindo assim a relevância contínua de nosso plano de continuidade de negócios.

A SPC Grafeno reconhece como processos críticos, devido à sua importância estratégica e ao impacto significativo que têm nas operações e serviços da Companhia:

- **Registro de ativos financeiros:** O registro de ativos financeiros autorizados (duplicatas, notas promissórias e CCB (Cédulas de Crédito Bancário), é essencial para a operação da SPC Grafeno como uma registradora. Esses registros são fundamentais para a eficiência das transações financeiras e para fornecer segurança e validade legal aos ativos registrados. Qualquer falha nesse processo poderia afetar negativamente a confiabilidade e a credibilidade da SPC Grafeno, prejudicando a confiança dos clientes e parceiros.

10. GESTÃO DE PROVEDORES DE SERVIÇOS CRÍTICOS

Entende-se por provedor de serviços críticos (PSC), aquele prestador de serviço cuja atividade profissional, dada a sua relevância e imprescindibilidade, constitui elemento essencial para a Companhia e que, se malconduzida e/ou não fiscalizada de forma adequada, pode trazer riscos sistêmicos de alto custo para a SPC Grafeno.

Na contratação e gestão de serviços críticos, especialmente quanto a serviços de processamento e armazenamento de dados em nuvem, a Companhia deve avaliar a relevância do serviço considerando a criticidade do serviço e a sensibilidade dos dados e informações a serem processados, armazenados e gerenciados pelo prestador de serviço terceirizado, conforme estipulado na Resolução BCB 304/23.

Dentre as principais atividades de gerenciamento provedores de serviços críticos, estão:

- Verificação da capacidade do Prestador de Serviço;
- Inventário dos fornecedores;
- Priorização de fornecedores relevantes por critérios estabelecidos;
- Priorização e criticidade de fornecedores;
- Avaliação de Due Diligencie (questionários de avaliação de riscos); e
- Análise de Contratos.

Esse processo está mais bem detalhado na Política de Gestão de Terceiros aprovada pelo Conselho de Administração.

11. GESTÃO DE FRAUDES

A Companhia deve realizar uma análise abrangente para identificar e compreender os riscos e possibilidades de fraude em seus produtos, serviços e processos.

Essa análise deve considerar tanto os riscos individuais como os coletivos, abrangendo a Companhia, seus participantes e outros sistemas do mercado financeiro com os quais haja relacionamento, com base nas etapas abaixo:

- Identificação e compreensão dos riscos e fraudes em produtos, serviços e processos, considerando a instituição, seus participantes e outros sistemas do mercado financeiro relacionados;
- Estabelecimento e implementação de requisitos de segurança para prevenção, detecção e resposta a fraudes pela Companhia e seus participantes;
- Promoção da conformidade dos participantes com os requisitos de segurança, incluindo a mitigação de vulnerabilidades identificadas por meio de avaliações internas e externas;
- Fornecimento de informações e ferramentas para melhorar continuamente a prevenção, detecção e resposta a fraudes entre a Companhia e seus participantes;

- Resposta rápida a indícios de fraudes, envolvendo a Companhia e seus participantes;
- Promoção contínua de treinamento, divulgação e compartilhamento de informações sobre gestão de fraudes, respeitando as leis de sigilo bancário e proteção de dados; e
- Aproveitamento da experiência em gestão de fraudes para evoluir e coordenar práticas, inclusive com outras instituições.

As responsabilidades e o detalhamento para a execução do reporte de eventos de risco operacional de fraude, bem como o gerenciamento dos procedimentos realizados pela área de Fraudes para garantir a conformidade com a regulamentação vigente estão descritos na Política de Gestão de Fraudes.

12. ESTRUTURA DE CONTROLES INTERNOS

A estrutura de Riscos e Controles da Companhia, através do mapeamento de riscos e controles, testes de efetividade dos controles mitigatórios e monitoramento dos indicadores de Apetite por Riscos, tem como objetivo garantir o monitoramento e testes periódicos que viabilizem a melhoria dos processos e operações da Companhia e a redução do impacto no caso de materialização de riscos e fornece ao Comitê de Riscos, Compliance e SI e Conselho de Administração o resultado dos trabalhos desenvolvidos e o grau de exposição aos Riscos.

A Auditoria Interna também deve possuir processo de avaliações periódicas, acerca da eficácia dos sistemas de controles internos e dos principais riscos associados às atividades da Companhia.

Nas avaliações anuais de riscos inerentes e no trabalho periódico de verificação dos riscos residuais, são considerados fatores de riscos, **como por exemplo**:

- **Erros Operacionais:** Falhas humanas ou sistêmicas que resultam em erros na execução de transações ou processos;
- **Tecnologia e Infraestrutura:** Interrupções de sistemas, falhas de hardware ou software que podem afetar a continuidade dos negócios;
- **Segurança Cibernética:** Riscos relacionados a ataques cibernéticos, violações de dados ou comprometimento da segurança da informação;
- **Processos Ineficientes:** Falhas nos processos internos que levam a atrasos, retrabalho ou desperdício de recursos;
- **Controles Internos Inadequados:** Falhas nos controles internos que permitem fraudes, manipulação de dados ou violações regulatórias;
- **Gestão Orçamentária e Financeira:** Possibilidade de falhas na gestão de orçamentos, por alocação de capital indevida ou falhas no orçado x realizado; Possíveis falhas na gestão financeira (cobrança e fluxo de caixa).
- **Processos Não Documentados:** Possível falta de documentação adequada de processos operacionais críticos, tornando difícil a replicação ou recuperação em caso de falha.

Os controles mitigatórios devem ser propostos, sob a ótica de custo versus benefício com o objetivo de otimizar e adequar os níveis de riscos, por meio da adoção de novos controles ou a otimização dos controles atuais do processo. O custo de um controle não deve ser mais caro do que o benefício gerado por ele.

As ações de correção e melhorias propostas devem ser registradas, orientadas conforme descrito no Manual de Riscos e Controles Internos da Companhia.

13. TREINAMENTO E CONSCIENTIZAÇÃO

A SPC Grafeno estabelece programas de treinamento e conscientização para garantir que todos os colaboradores entendam suas responsabilidades em relação ao gerenciamento de riscos e controles internos e tenham o conhecimento necessário para desempenhar efetivamente seus papéis. Atualmente, são os seguintes treinamentos disponibilizados na plataforma corporativa educacional:

- Segurança da Informação e Cyber
- Compliance e Riscos
- Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo
- Código de Ética e Conduta
- Lei Geral de Proteção de Dados
- Assédio

14. RELATÓRIO REGULAMENTAR

De acordo com o art. 32 da Resolução nº 304, do Banco Central deve ser elaborado relatório, com periodicidade mínima anual, contendo as conclusões dos exames realizados, recomendações relacionadas a eventuais deficiências, incluindo cronograma para correção, quando aplicável e manifestação dos responsáveis pelas áreas pertinentes sobre as deficiências encontradas em verificações anteriores e as medidas efetivamente tomadas para correção, quando aplicável.

15. RETENÇÃO DE ARQUIVOS

Todos os arquivos e papéis de trabalho produzidos pelos processos definidos nesta Política, formalizados em qualquer tipo de mídia ou papel, devem ser mantidos pelo prazo de 5 (cinco) anos ou por prazo superior caso assim seja exigido por regulamentação vigente.

16. DISPOSIÇÕES GERAIS

16.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

16.2. CASOS OMISSOS

Os casos omissos serão regulados pelo Conselho de Administração da Companhia, conforme necessário.

16.3. DIVISIBILIDADE

A invalidade ou ineficácia de qualquer disposição desta Política não afetará os demais dispositivos, que permanecerão em pleno vigor e efeito.

17. REVISÃO DA POLÍTICA

Esta Política poderá ser revisada anualmente. Eventuais correções ou aprimoramentos devem ser objeto de recomendação ao Conselho de Administração.

18. VIOLAÇÕES

As violações dos termos da presente Política serão examinadas pelo Comitê de Ética da SPC Grafeno e poderá aplicar as ações disciplinares descritas na Política de Consequências, reportando ao Conselho de Administração.

19. CONTROLE DE VERSÕES

Versão	Data	Responsável	Ocorrência
1.0	26/09/2019	Diretor de Riscos, CI e Compliance	Elaboração do documento
1.0	26/09/2019	Diretor de Operações	Revisão do documento
2.0	13/07/2022	Analista de Riscos e Controles	Revisão da 1.0 e criação da versão 2.0
3.0	14/12/2022	Gerente de Riscos, CI e Compliance	Alteração do nome da Política e aderência do conteúdo ao Programa de Compliance, Riscos e Controles da SPC Grafeno.
4.0	20/06/2023	Analista de Compliance Sr. - Gerente de Riscos, CI e Compliance	Revisão da 3.0 e criação da versão 4.0
4.0	15/09/2023	Comitê de Gerenciamento de Riscos	Revisão/Aprovação do documento
4.0	29/09/2023	Conselho de Administração	Aprovação final do documento
5.0	02/04/2024	Área de Riscos, CI e Compliance	Revisão do Documento (adequação à PFMI)
5.0	23/04/2024	Comitê de Riscos, Compliance e CI	Aprovação do documento
5.0	26/04/2024	Conselho de Administração	Aprovação final do documento

***

ANEXO I – Critérios para avaliação do impacto e probabilidade

IMPACTO				
Critérios	**Baixo**	**Moderado**	**Alto**	**Crítico**
	1	**2**	**3**	**4**
Estratégicos Peso: 15%	Associado à tomada de decisões inadequadas por parte da alta administração, em decorrência da utilização de premissas inadequadas, baseadas em dados/informações obtidos através de atividades/serviços irregulares/insuficientes. **Sem implicações à imagem e/ou negócios ou dano pouco significativo e reversível para a Companhia**	Associado à tomada de decisões inadequadas por parte da alta administração, em decorrência da utilização de premissas inadequadas, baseadas em dados/informações obtidos através de atividades/serviços irregulares/insuficientes. **Implicações significativas à imagem e/ou negócios, mas de possível reversão**	Associado à tomada de decisões inadequadas por parte da alta administração, em decorrência da utilização de premissas inadequadas, baseadas em dados/informações obtidos através de atividades/serviços irregulares/insuficientes. **Danos à imagem e/ou negócios relacionados aos participantes atuais e novos**	Associado à tomada de decisões inadequadas por parte da alta administração, em decorrência da utilização de premissas inadequadas, baseadas em dados/informações obtidos através de atividades/serviços irregulares/insuficientes. **Danos à imagem e/ou negócio perante o mercado e ao regulador**
Operacionais Peso: 25%	Possibilidade da ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas ou eventos externos, incluindo perda decorrente de terceiros e não conformidade fiscal/tributária. **Eventos que não afetam ou pouco afetam a continuidade das operações da Companhia**	Possibilidade da ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas ou eventos externos, incluindo perda decorrente de terceiros e não conformidade fiscal/tributária. **Eventos que acarretam perda de produtividade das operações da Companhia**	Possibilidade da ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas ou eventos externos, incluindo perda decorrente de terceiros e não conformidade fiscal/tributária. **Eventos que acarretam interrupção das operações da Companhia com possibilidade de reversão do cenário**	Possibilidade da ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas ou eventos externos, incluindo perda decorrente de terceiros e não conformidade fiscal/tributária. **Eventos que acarretam interrupção das operações da Companhia, podendo levar a situações irreversíveis**
Reputacional Peso: 20%	Perda de credibilidade da Companhia diante do público externo e interno, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas por pessoas não autorizadas ou por meios de comunicação inadequados; e por veiculação de notícias negativas sobre a Companhia. **Situações com impacto mínimo na reputação da Companhia. Geralmente, essas situações podem ser gerenciadas com facilidade e não têm efeitos significativos a longo prazo.**	Perda de credibilidade da Companhia diante do público externo e interno, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas por pessoas não autorizadas ou por meios de comunicação inadequados; e por veiculação de notícias negativas sobre a Companhia. **Situações com o potencial de causar danos limitados e temporários à reputação da Companhia. Pode ser gerenciado eficazmente com ações corretivas e estratégias de comunicação.**	Perda de credibilidade da Companhia diante do público externo e interno, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas por pessoas não autorizadas ou por meios de comunicação inadequados; e por veiculação de notícias negativas sobre a Companhia. **Situações com o potencial de causar danos consideráveis à reputação da Companhia, embora possam ser mitigados com o tempo e esforço. Pode resultar em perda de confiança temporária e impactos significativos nas relações com partes interessadas.**	Perda de credibilidade da Companhia diante do público externo e interno, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas por pessoas não autorizadas ou por meios de comunicação inadequados; e por veiculação de notícias negativas sobre a Companhia. **Situações com o potencial de causar danos significativos e duradouros à reputação da Companhia. Isso pode resultar em perda substancial de confiança por parte dos clientes, parceiros de negócios, investidores e outras partes interessadas.**
Jurídico/ Regulatório Peso: 15%	Relacionado ao não cumprimento da regulamentação aplicável ao setor de atuação, bem como a não conformidade a determinações legais e contratuais, causando: processos administrativos, suspensão das atividades, condenação judicial e/ou intervenção por parte de autoridades em decorrência da não observância das regulamentações vigentes e funções legais. **Falha no atendimento regulatório com contorno breve sem impacto ao regulador e judiciário.**	Relacionado ao não cumprimento da regulamentação aplicável ao setor de atuação, bem como a não conformidade a determinações legais e contratuais, causando: processos administrativos, suspensão das atividades, condenação judicial e/ou intervenção por parte de autoridades em decorrência da não observância das regulamentações vigentes e funções legais. **Falha no atendimento regulatório ou**	Relacionado ao não cumprimento da regulamentação aplicável ao setor de atuação, bem como a não conformidade a determinações legais e contratuais, causando: processos administrativos, suspensão das atividades, condenação judicial e/ou intervenção por parte de autoridades em decorrência da não observância das regulamentações vigentes e funções legais. **Falha no**	Relacionado ao não cumprimento da regulamentação aplicável ao setor de atuação, bem como a não conformidade a determinações legais e contratuais, causando: processos administrativos, suspensão das atividades, condenação judicial e/ou intervenção por parte de autoridades em decorrência da não observância das regulamentações vigentes e funções legais. **Falha no atendimento regulatório ou**

		judiciário com ofícios ou notificações deliberando ações imediatas	**atendimento regulatório ou judicial com penalidades.**	**judicial com sanções pelo regulador ou judiciário, além de penalidades**
Financeiros Peso: 25%	A exposição ao risco financeiro associado ao evento é mínima. Isso pode ser devido a medidas de mitigação eficazes já em vigor ou à natureza intrinsecamente baixa do risco financeiro associado ao evento.	Embora haja algum impacto, o nível "baixo" sugere que a saúde financeira geral da empresa não está seriamente comprometida. Isso pode significar que a empresa tem margens de lucro saudáveis ou reservas financeiras adequadas para absorver as perdas potenciais.	Situações que diminuem a margem de lucro ou resultam em prejuízos financeiros consistentes que podem impactar negativamente a capacidade da Companhia de reinvestir, expandir ou competir efetivamente no mercado.	Impacto financeiro crítico pode levar a cortes drásticos nos investimentos, despesas operacionais e recursos humanos. Isso pode afetar negativamente a capacidade da Companhia de cumprir suas obrigações, realizar projetos estratégicos e manter operações eficientes.

PROBABILIDADE				
Critérios	**Baixa**	**Moderada**	**Alta**	**Crítica**
	1	**2**	**3**	**4**
Experiência do negócio Peso: 30%	Este risco não possui tendência de materialização.	A chance desse risco ocorrer é muito pequena.	Estamos sujeitos a este risco, porém não é capaz de precisar em quanto tempo o risco poderá se materializar.	Estamos sujeitos a este risco em um curto prazo (a materialização do risco deverá ocorrer em breve)
Repetição Peso: 40%	O risco pode ocorrer uma vez a cada 3 anos.	O risco pode ocorrer uma vez por ano.	O risco pode ocorrer em intervalos semestrais.	O risco pode ocorrer em intervalos trimestrais.
Efetividade do Controle (*)	Existem medidas de gerenciamento de risco que praticamente eliminam a chance de ocorrência	Existem medidas de gerenciamento de risco efetivas em limitar a chance de ocorrência	Existem medidas de gerenciamento de risco, mas são pouco efetivas em limitar a chance de ocorrência	Existem medidas de gerenciamento de risco, mas não são efetivas
Possibilidade Peso: 30%	Improvável: < 34% de chances de ocorrer.	Possível: entre 35% e 64% de chances de ocorrer.	Provável: entre 65% e 89% de chances de ocorrer.	Quase certo: > 90% de chances de ocorrer.

(*) Critério utilizado para a avaliação do risco residual

ANEXO II – Dicionário de Riscos

ID Risco	Classificação	Cenário de Risco	
RIS_01	**Estratégico**	• Falha de planejamento estratégico • Falha no gerenciamento de projetos • Gestão de Conhecimento • Práticas Comerciais • Sucessão • Relacionamento com Acionistas • Responsabilidade Social	• Concorrência e Mercado • Desenvolvimento de Produto/Serviços • Estrutura Organizacional • Investimento em Projetos • Fusão e Aquisição • Marcas e Patentes • Satisfação do Cliente
RIS_02	**Imagem | Reputacional**	• Reputação / Imagem • Conduta Antiética	
RIS_03	**Regulatório | Legal**	• Não cumprimento de requisitos contratuais • Descumprimento de regras - não compliance • Comunicação e Divulgação • Obrigação Contratual de fornecedores	• Terceirização e Parceria • Não cumprimento de requisitos legais ou regulatórios • Trabalhista • Tributário/Fiscal • Cível Ambiental
RIS_04	**Financeiro**	• Investimento • Cenário Econômico • Políticas e Procedimentos • Concentração de Receitas • Garantia • Inadimplência • Câmbio	• Taxa de Juros • Custo de Oportunidade • Disponibilidade de Capital • Fluxo de Caixa/Contábil • Perda e/ou Obsolescência • Orçamento / Resultados
RIS_05	**Operacional**	• Falhas operacionais • Turnover • Incentivo de Desempenho • Capacidade Operacional • Efetividade e Eficiência • Falha de Produto/Serviço • Capacitação e treinamento • Dependência de Pessoal • Limite de Autoridade • Disponibilidade Sistêmica	• Saúde e Segurança • Fraude • Vulnerabilidade Cibernética • Segurança Patrimonial • Acesso e Confidencialidade • Disponibilidade da Informação • Integridade da Informação • Indisponibilidade Tecnológica • Continuidade de Negócios • Dados e Inovação
RIS_06	**Risco Geral do Negócio**	• Declínio nas vendas • Perda de participação de mercado • Incapacidade de competir	• Problemas financeiros persistentes • Mudanças regulatórias ou legais

ANEXO III – Quadrante de Riscos

PROBABILIDADE						
	Crítica	4	Moderado	Alto	Alto	Crítico
	Alta	3	Moderado	Moderado	Alto	Alto
	Moderada	2	Baixo	Moderado	Moderado	Alto
	Baixa	1	Baixo	Baixo	Moderado	Moderado
			1	2	3	4
			Baixo	Moderado	Alto	Crítico
			IMPACTO			