SPC GRAFENO

POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

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

SUMÁRIO

1. OBJETIVO 3

2. ABRANGÊNCIA 3

3. DOCUMENTOS DE REFERÊNCIA 3

4. ALÇADAS DE APROVAÇÃO 4

5. DIRETRIZES 4

5.1. PRINCIPAIS OBJETIVOS DA POLÍTICA 4

5.2. CONCEITOS GERAIS 5

5.3. PAPÉIS E RESPONSABILIDADES 6

5.4. PROCESSO DE ANÁLISE DE IMPACTO NOS NEGÓCIOS 9

5.4.1. Business Impact Analysis (BIA) 9

5.4.2. Tempo de Recuperação 9

5.4.3. Serviço de Processamento em Nuvem 10

5.5. ESTRATÉGIAS PARA ASSEGURAR A CONTINUIDADE DAS ATIVIDADES 10

5.6. TRATAMENTO DE INCIDENTES RELEVANTES 11

5.6.1. Situação de Crise 11

5.7. PLANO DE CONTINUIDADE DE NEGÓCIOS 12

5.8. TESTES DE RESILIÊNCIA OPERACIONAL 12

5.8.1. Escopo e Abrangência dos Testes 13

5.8.2. Cenários de incidentes considerados nos Testes de Resiliência Operacional 14

5.8.3. Compromisso com a continuidade de serviços contratados 14

5.8.4. Estrutura e Comunicação sobre os resultados dos testes 15

5.9. GESTÃO DE MUDANÇAS 16

5.10. TREINAMENTO E CAPACITAÇÃO 16

5.11. COMUNICAÇÃO 16

5.12. MELHORIA CONTÍNUA 17

6. DISPOSIÇÕES GERAIS 17

6.1. VIGÊNCIA 17

6.2. CASOS OMISSOS 17

6.3. DIVISIBILIDADE 17

7. REVISÃO DA POLÍTICA 17

8. VIOLAÇÕES 17

9. CONTROLE DE VERSÕES 17

1. OBJETIVO

Esta Política descreve os princípios básicos e a estratégia do Sistema de Gestão da Continuidade de Negócios da ***SPC GRAFENO Infraestrutura e Tecnologia para o Sistema Financeiro S.A.*** (***SPC GRAFENO)***, incluindo definições, estrutura organizacional, normativa e responsabilidades, visando minimizar os danos e impactos gerados oriundos de eventos de incidentes críticos ou crises, preservar as instalações e a segurança dos colaboradores e prestadores de serviços e restabelecer a operação, dentro das melhores práticas de mercado para gerenciamento de riscos de resiliência operacional e continuidade de negócios.

A Companhia define a Política para a gestão da Continuidade de Negócios, dentro de padrões estabelecidos, observando-se a gestão de riscos operacionais, a Política de Segurança da Informação e Cibernética, bem como as resoluções, instruções normativas e legislação vigentes.

Para tanto, a Companhia deve:

- Estruturar, organizar, definir processos, atribuições e responsabilidades individuais e das equipes envolvidas no Sistema de Gestão da Continuidade de Negócios da ***SPC GRAFENO***;
- Manter ações de identificação, prevenção e mitigação dos riscos de ameaças específicas;

Esta Política é desenvolvida em conformidade com as Resoluções 304/23 e 339/23 do Banco Central do Brasil, os Princípios para Infraestruturas de Mercado Financeiro (PFMI) e com a NBR/ISO 22301- Sistema de Gestão de Continuidade de Negócios.

2. ABRANGÊNCIA

Esta Política contém diretrizes aplicáveis em todas as atividades operacionais da **SPC GRAFENO**, e abrange as soluções tecnológicas adotadas para suportar tais operações, bem como as infraestruturas físicas.

Esta Política é aplicada para os colaboradores, parceiros de negócios, fornecedores e prestadores de serviços.

3. DOCUMENTOS DE REFERÊNCIA

- Política de Gerenciamento de Riscos e Controles
- Política de Segurança da Informação e Cibernética
- Política de Gerenciamento de Incidentes
- Resolução 304/23 do Banco Central do Brasil
- Resolução 339/23 do Banco Central do Brasil
- Princípios para Infraestruturas de Mercado Financeiro (PFMI)
- ABNT NBR/ISO 22301:2020- Sistema de Gestão de Continuidade de Negócios – Requisitos.

4. ALÇADAS DE APROVAÇÃO

- Área de Riscos e Controles Internos – responsável pela elaboração e revisão do documento;
- Comitê de Riscos, Compliance e SI – responsável pela aprovação do documento;
- Conselho de Administração – responsável pela aprovação final do documento

5. DIRETRIZES

A Gestão de Continuidade de Negócios da SPC Grafeno estrutura processos para garantir resiliência operacional e resposta eficiente a incidentes, protegendo operações críticas e a reputação da Companhia.

As diretrizes do processo de Gestão da Continuidade de Negócios deverão considerar, prioritariamente, os objetivos estratégicos, os processos de negócio, os requisitos legais, além de estar alinhadas à Política de Gerenciamento de Riscos e Controles da **SPC GRAFENO**.

A Continuidade de Negócios contempla o gerenciamento da recuperação dos negócios em caso de interrupção, e gestão de toda a Continuidade de Negócios por meio de treinamentos, testes, revisões e manutenções, a fim de garantir que o Plano de Continuidade de Negócios e o Plano de Recuperação de Desastres, estejam atualizados e operacionais.

O Sistema de Gestão da Continuidade de Negócios da **SPC GRAFENO** tem as seguintes diretrizes:

- Atender as expectativas de clientes, acionistas e colaboradores na administração de uma interrupção de negócio e na proteção da reputação da empresa no mercado;
- Definir as estratégias de resposta aos incidentes, principalmente nas atividades e operações críticas, visando limitar os impactos e retornar à normalidade;
- Aplicar, quando necessário, as ações de recuperação definidas, visando a proteção da **SPC GRAFENO** contra a interrupção no fornecimento dos seus produtos e serviços;
- Disponibilizar aos colaboradores os procedimentos a serem adotados face a um incidente;
- Conformidade com as Resoluções 304/23 e 339/23 do Banco Central do Brasil e os Princípios para Infraestruturas de Mercado Financeiro (PFMI).

5.1. PRINCIPAIS OBJETIVOS DA POLÍTICA

- Oferecer um conjunto de estratégias capazes de preservar a integridade física e tecnológica da plataforma e dos serviços essenciais para consecução das atividades da **SPC GRAFENO.** Nesse contexto, a Companhia mantém estrutura de Governança e Compliance alinhada com as melhores práticas de governança corporativa do mercado;
- Responder imediatamente a eventos que coloquem em risco a integridade física dos colaboradores, fornecedores e parceiros comerciais da Companhia;
- Proteger a reputação, marca, os bens físicos, interesses das partes envolvidas, bem como as atividades de valor agregado da **SPC GRAFENO**;

- Identificar ameaças potenciais inerentes aos negócios da **SPC GRAFENO** e avaliar os possíveis impactos nas operações, fornecendo uma metodologia capaz de desenvolver um nível de resiliência organizacional que permita e mantenha a execução de atividades críticas;
- Assegurar que todos os colaboradores da **SPC GRAFENO** conheçam o Plano de Gestão de Continuidade de Negócio.

5.2. CONCEITOS GERAIS

Para fins desta Política e de todos os documentos correlatos (PCN, PCO, BIA e PRD), adotam-se os seguintes conceitos uniformes:

- **Business Impact Analysis (BIA):** Engloba todas as atividades ou processos críticos relacionados às operações da **SPC GRAFENO**.
- **Continuidade:** ações planejadas para assegurar que os processos críticos permaneçam operacionais ou sejam retomados em prazo definido;
- **Contingência:** medidas emergenciais para manter temporariamente processos críticos em funcionamento, até que a normalidade seja restabelecida;
- **Classificação dos processos críticos:** A classificação de processos críticos seguirá três categorias: **Vital**, **Relevante** e **Essencial**, conforme metodologia descrita no BIA.
- **Desastre:** É um incidente que resultou em um "Tempo de Queda" ("Downtime") superior ao tempo máximo regulatório especificado.
- **Gestão da Continuidade do Negócio:** Compreende treinamentos, testes, revisões e manutenções para garantir a execução e atualização do Plano de Continuidade da **SPC GRAFENO**.
- **Incidente:** Qualquer evento que possa impactar negativamente a rotina operacional das atividades da SPC GRAFENO, podendo, em casos graves, ser classificado como Crise.
- **Plano de Continuidade de Negócios:** Plano de Continuidade de Negócios que descreve as ações a serem executadas pelas pessoas chaves definidas no BIA, em caso de acionamento do estado de contingência;
- **Plano de Continuidade Operacional:** Descreve os responsáveis, escalonamento e acionamento, bem como o plano alternativo de execução do processo, com o objetivo de minimizar os impactos operacionais, financeiros, regulatórios e reputacionais decorrentes de indisponibilidades ou falhas;
- **Resiliência Operacional:** Refere-se à capacidade da Companhia de antecipar, resistir, adaptar-se e recuperar-se de- incidentes, interrupções ou crises, mantendo a continuidade das operações essenciais;
- **Teste de Resiliência Operacional:** Englobam tanto os testes de contingência, que avaliam a resposta a eventos imprevistos e a recuperação de sistemas e processos críticos, quanto os testes de continuidade de negócios, que verificam a eficácia dos planos para assegurar a operação contínua durante e após interrupções. Esta abordagem integrada visa fortalecer a robustez da Companhia contra uma ampla gama de desafios, garantindo a sustentação dos serviços e a minimização dos impactos negativos.

- **Sistema de Gestão de Continuidade de Negócios - SGCN:** é um conjunto de processos, procedimentos e atividades projetados para garantir a continuidade das operações de uma organização, mesmo diante de eventos inesperados ou interrupções que possam afetar seus serviços e produtos. Em outras palavras, a GCN visa minimizar o impacto de incidentes, como desastres naturais, ciberataques, falhas de sistemas ou crises financeiras, sobre a capacidade da empresa de operar e atender aos seus clientes.
- **SMF:** Sistemas do Mercado Financeiro e o Banco Central é o responsável por sua gestão e operação.

5.3. PAPÉIS E RESPONSABILIDADES

CONSELHO DE ADMINISTRAÇÃO

O Conselho de Administração desempenha um papel crucial na gestão da continuidade de negócios (GCN), atuando como um órgão de orientação e supervisão. É responsabilidade do Conselho de Administração da **SPC GRAFENO**, no âmbito de suas atribuições:

- Garantir que a empresa esteja em conformidade com as regulamentações aplicáveis à GCN, como as estabelecidas pelo Banco Central.
- Deve aprovar a identificação, avaliação e mitigação dos riscos que podem afetar a continuidade dos negócios, como riscos cibernéticos, operacionais e de eventos naturais extremos;
- Deve aprovar a Política de Gestão de Continuidade de Negócios e respectivas estratégias, garantindo a identificação, avaliação e mitigação dos impactos que podem afetar a continuidade dos negócios, como impactos financeiros, operacionais, legais e de imagem e reputação;
- Fortalecer a cultura de resiliência organizacional através de treinamentos, workshops ou outro meio que valorize a importância da GCN e incentive a participação de todos os colaboradores;
- Deve acompanhar o desempenho da GCN, tomando conhecimento do resultado de exercícios de simulação e testes elaborados periodicamente.

DIRETORIA EXECUTIVA

É responsabilidade da alta direção da **SPC GRAFENO**, no âmbito de suas atribuições:

- Considerar sempre a segurança das pessoas como prioridade;
- Considerar a preservação dos ativos e a imagem da Companhia;
- Aprovação da Avaliação e Aceitação dos Riscos.;
- Aprovar a Análise de Impacto nos Negócios (BIA), estabelecendo o consenso sobre a classificação de criticidade dos processos e as respectivas operações de contingência;

- Apoiar ao Comitê de Gestão de Crises e Risco Operacional na coordenação das ações de ativação de contingência, comunicação com as partes interessadas, acionamento das pessoas chave;
- Acompanhar o andamento do sistema de gestão, alocando recursos materiais e humanos necessários ao seu desenvolvimento e execução.

COMITÊ DE GESTÃO DE CRISES E RISCO OPERACIONAL (CGCRO)

- O Comitê de Gestão de Crises e Risco Operacional (CGCRO) é responsável por coordenar a resposta a incidentes críticos, monitorar riscos operacionais e assegurar a execução dos planos de continuidade e comunicação.
- Este Órgão é responsável por nomear o Gestor responsável pelo sistema de Gestão de Continuidade de Negócios, que coordenará as ações de ativação de contingência, comunicação com as partes interessadas, acionamento das pessoas chave, com apoio da Diretoria de Tecnologia, Dados e Inovação, Diretoria de Riscos, CI, Compliance e SI, e Diretoria de Operações.

DIRETORIA DE RISCOS, CI, COMPLIANCE E SI

- Responsável por garantir que todos os processos e práticas estejam em conformidade com regulamentos e normas aplicáveis, identificando e mitigando riscos que possam impactar a continuidade dos negócios. Suas principais responsabilidades incluem avaliar e monitorar a aderência às políticas de continuidade, assegurar que os controles internos sejam robustos e eficazes durante crises, realizar avaliações periódicas para verificar a preparação da Companhia, e promover uma cultura de risco e conformidade, garantindo que todos os colaboradores entendam e sigam os procedimentos estabelecidos para a continuidade dos negócios em situações de interrupção.
- A área de Segurança da Informação desempenha um papel crucial na proteção e recuperação dos ativos digitais da Companhia durante e após incidentes disruptivos. Suas principais responsabilidades incluem assegurar que os sistemas de TI sejam resilientes a ataques cibernéticos, implementar e gerenciar controles de segurança, e garantir a confidencialidade, integridade e disponibilidade das informações.
- A área deve desenvolver e manter políticas de segurança, realizar avaliações regulares de vulnerabilidades, e implementar medidas de mitigação de riscos. Além disso, é responsável por revisar os Planos de Resposta a Incidentes e Recuperação de Desastres, garantindo que os dados críticos possam ser recuperados rapidamente e que as operações possam ser restabelecidas com o mínimo de interrupção possível.

DIRETORIA DE OPERAÇÕES

- A Diretoria de Operações desempenha um papel crucial na manutenção e recuperação das atividades essenciais da Companhia durante e após incidentes disruptivos. Suas principais responsabilidades incluem a implementação de planos de continuidade específicos para

processos operacionais críticos que garantam a redundância e resiliência dos sistemas e recursos necessários.

- A área de Operações deve assegurar que todos os procedimentos operacionais sejam documentados para responder eficazmente a crises. Além disso, é responsável por monitorar continuamente as operações para identificar potenciais riscos e participar dos testes regulares de resiliência operacional para validar a eficácia dos planos, permitindo uma rápida recuperação e minimização dos impactos operacionais.

DIRETORIA DE TECNOLOGIA, DADOS E INOVAÇÃO

- Dentro da estrutura de Gestão de Continuidade de Negócios, a área de Tecnologia da Informação (TI) desempenha um papel fundamental em garantir a resiliência e a recuperação dos sistemas tecnológicos críticos da Companhia durante e após incidentes disruptivos. Suas principais responsabilidades incluem desenvolver, implementar e manter Planos de Recuperação de Desastres (PRD) e de Continuidade de Negócios (PCN) específicos para infraestruturas de TI, executando os testes regulares de resiliência operacional programados.
- A área de TI deve assegurar que todos os sistemas e dados críticos tenham backups regulares e que existam soluções de redundância para minimizar o tempo de inatividade. Além disso, é responsável por realizar testes periódicos de resiliência operacional, monitorar e responder a incidentes de segurança cibernética, e garantir que todos os funcionários tenham acesso aos recursos tecnológicos necessários para manter as operações durante uma interrupção.
- A área de TI também deve colaborar com outras áreas da Companhia para alinhar as estratégias de continuidade de negócios com os objetivos gerais da empresa.

AUDITORIA

O processo de auditoria interna exerce um papel essencial na Gestão da Continuidade de Negócios (GCN), ao avaliar a adequação e conformidade do programa de continuidade de negócios da Companhia.
auditorias serão conduzidas periodicamente, conforme os ciclos de planejamento da área, com o objetivo de fornecer informações sobre a eficácia do sistema de gestão da continuidade dos negócios e garantir que os processos, planos e estratégias implementados estejam em conformidade com os requisitos regulatórios e alinhados aos objetivos organizacionais.

Os elementos fundamentais da auditoria incluem:

- Verificar se a estrutura de GCN abrange adequadamente todas as operações críticas da Companhia, incluindo a avaliação de processos, arcabouço normativo interno e regulatório e monitoramento de riscos;
- Avaliar os resultados dos testes e verificar se as falhas identificadas são corrigidas e documentadas.

5.4. PROCESSO DE ANÁLISE DE IMPACTO NOS NEGÓCIOS

A análise de impacto é um processo da continuidade de negócios que deve identificar e mensurar os impactos quantitativos e/ou qualitativos na interrupção das atividades em processos críticos, possibilitando a determinação da prioridade de recuperação, do tempo de retomada e das necessidades mínimas de recursos e equipes, justificando desta forma investimentos que visem minimizar estes impactos.

A avaliação dos potenciais efeitos, em caso de incidente, terá sua identificação, classificação, severidade e a natureza do impacto econômico / financeiro, operacional, legal / regulatório, imagem / reputação, e estratégico durante às janelas operacionais, definidas no BIA.

Definem-se como processos críticos aqueles que, uma vez paralisados irão afetar de forma sensível as operações e serviços da Companhia gerando impactos negativos em clientes internos e externos, ocasionando assim uma situação de crise.

5.4.1. Business Impact Analysis (BIA)

O Business Impact Analysis (BIA) da SPC Grafeno identifica os processos críticos e avalia os impactos de eventuais interrupções. Essa análise determina os prazos e recursos necessários para a retomada operacional. O BIA é revisado anualmente para garantir que reflita com precisão as mudanças nos processos de negócios, tecnologias e riscos, garantindo assim a relevância contínua do Plano de Continuidade de Negócios e dos Planos de Continuidade Operacionais.

5.4.2. Tempo de Recuperação

Na SPC Grafeno, o RTO para processos críticos é de até 2 horas e o RPO é zero, conforme a Resolução BCB 304/23, garantindo recuperação rápida e sem perda de dados. Essas duas métricas são referências para planejar a recuperação de sistemas e processos.

- **Recovery Time Objective (RTO):** O RTO é o tempo máximo aceitável que um sistema, serviço ou processo pode ficar indisponível após uma falha ou interrupção. Ele representa o prazo dentro do qual os processos críticos devem ser restaurados para evitar impactos significativos no negócio. Conforme o art. 96, inciso II da Resolução BCB 304/23, o tempo de recuperação objetivado para o processo crítico deve ser de até 2(duas) horas.
- **Recovery Point Objective (RPO):** O RPO é o ponto máximo aceitável em termos de tempo de dados que pode ser perdido devido a uma falha ou interrupção. De acordo com o art. 95 da Resolução BCB 304/23 o ponto de recuperação objetivado pelos SMF deve ser igual a 0 (zero), de forma a preservar a totalidade dos dados.
- **Índice de Disponibilidade:** De acordo com o art.94 da Resolução BCB 304/23 o índice de disponibilidade deve ser, no mínimo, 99,8% (noventa e nove inteiros e oito décimos por cento).

De acordo com o BIA, a graduação da severidade do impacto está relacionada a uma escala para cada natureza do impacto (Estratégico, Econômico/Financeiro, Operacional, Reputação/Imagem e Legal/Regulatório). O cálculo do índice de criticidade deve considerar ainda, o RTO estipulado para cada processo.

5.4.3. Serviço de Processamento em Nuvem

Em situação de incidente no prestador de serviços de nuvem, com consequente indisponibilidade dos serviços para a **SPC GRAFENO** por um período superior a resiliência dos processos de negócios envolvidos, haverá impacto na operação pela interrupção dos serviços, no financeiro como perda de receita, reputacional como danos à imagem, desconfiança dos clientes e Regulatório pelo não cumprimento de normas e contratos.

A avaliação dos potenciais efeitos, em caso de incidente, terá sua identificação, classificação de severidade e natureza do impacto, bem como a avaliação do histórico de falhas e/ou indisponibilidade do prestador de serviços, conforme a definição da Matriz de Impacto e Severidade, constante no BIA.

5.5. ESTRATÉGIAS PARA ASSEGURAR A CONTINUIDADE DAS ATIVIDADES

As estratégias de continuidade devem identificar e descrever as soluções táticas e estratégicas para suportar e garantir a restauração das atividades exigidas dentro de um tempo desejado de recuperação, no caso de um desastre ou outros incidentes graves.

Para assegurar a continuidade das atividades da **SPC GRAFENO** e limitar as perdas decorrentes da interrupção dos processos críticos de negócio, as seguintes estratégias são consideradas, e estão descritas e detalhadas a seguir:

- **Plano de Continuidade de Negócios (PCN):** Plano abrangente que identifica os processos críticos, os recursos necessários para mantê-los operacionais e os procedimentos de recuperação, prazos estimados para reinício e recuperação das atividades em caso de interrupção, bem como as ações de comunicação necessárias, incluindo gestão de crises, com atualizações, no mínimo, anuais e prevendo a realização de testes de continuidade de negócios periódicos para garantir que o plano funcione conforme esperado e faça ajustes conforme necessário.
- **Plano de Continuidade Operacional (PCO):** Conjunto de ações de preparação, prontidão e ações operacionais capazes de assegurar a retomada das atividades do(s) processo(s) de negócios classificados como **"Vital"** pela análise de impacto nos negócios (BIA).
- **Plano de Recuperação de Desastres (PRD):** Trata-se de um conjunto de ações específicas, dentro da estratégia de resiliência operacional, focado na recuperação e restauração de sistemas de TI, infraestrutura e dados após a ocorrência de incidente ou desastre, que venha a afetar os processos classificados como "Vital" para a Companhia, prejudicando a continuidade no fornecimento de produtos e/ou serviços.
- **Parcerias e Serviços Externos:** Colaboração com fornecedores de tecnologia para garantir suporte rápido e eficaz em caso de falhas de sistemas e estabelecimento de contratos de manutenção e suporte com cláusulas de resposta rápida.
- **Treinamento e Conscientização:** Realização de treinamentos regulares para capacitar os usuários no Plano de Continuidade de Negócios, em situações de incidentes e desastres e suas necessidades para uma eficiente utilização de seus recursos no gerenciamento e gestão de incidentes, crise e/ou desastres.

Capacitar os membros do Comitê de Gestão de Crises e Risco Operacional nas Estratégias de Continuidade de Negócios, Plano de Continuidade de Negócios e normativos internos, para gerenciamento e gestão de incidentes, crise e/ou desastres.

- **Monitoramento e Avaliações Contínuas:** Implementação de sistemas de monitoramento contínuo para detectar e responder rapidamente a falhas ou interrupções e realização de avaliações regulares do Plano de Continuidade de Negócios e Recuperação de Desastres para garantir conformidade e eficácia.
- **Planejamento de Contingência para Infraestrutura Física:** Manutenção de site alternativo preparado para ser utilizado em casos de emergência, onde os colaboradores possam trabalhar caso o acesso remoto seja comprometido, bem como a garantia de que os colaboradores tenham acesso remoto seguro e robusto aos sistemas críticos, permitindo a continuidade das operações, mesmo em home office. A Companhia prevê a utilização de locais alternativos, como coworkings, para garantir a continuidade das operações em caso de indisponibilidade do trabalho remoto. Esses locais deverão assegurar requisitos mínimos de segurança da informação. O reembolso de tais medidas dependerá de avaliação e aprovação prévia da área Financeira e do Diretor responsável, conforme estabelecido no PCN.

5.6. TRATAMENTO DE INCIDENTES RELEVANTES

Incidente relevante é um evento que tem um impacto significativo para a Companhia ou em seu ecossistema. Geralmente, afeta a continuidade de negócios, a segurança da informação ou o ambiente cibernético, a imagem pública da Companhia e pode trazer implicação para a estabilidade financeira e/ou para o ecossistema de atuação da IOSMF ou a saúde e segurança dos funcionários e clientes.

A **SPC GRAFENO** reconhece os processos críticos, devido à sua importância estratégica e ao impacto significativo que têm nas operações e serviços da Companhia, os quais devem ser mantidos ativos em tempo integral. O CGCRO será acionado para avaliar a ativação do estado de contingência operacional para que as medidas de contingência sejam implementadas e garantir a retomada o mais breve possível.

Nesse contexto, a Política de Continuidade de Negócios considera os processos estabelecidos para a resposta a incidentes, conforme o documento interno Política de Gerenciamento de Incidentes, bem como contempla nos cenários de testes regulares, incidentes relacionados à Tecnologia da Informação e Segurança da Informação e Cibernética.

5.6.1. Situação de Crise

É compromisso da Companhia, estabelecer critérios que configurem uma situação de crise com objetivo de estabelecer uma estrutura clara e objetiva para a triagem e classificação de incidentes, permitindo a rápida avaliação do impacto e da gravidade de cada ocorrência.

Isso assegura uma resposta adequada e eficiente, alinhada com os requisitos regulatórios e operacionais, ajuda a priorizar recursos e ações para minimizar a interrupção das operações e atender aos níveis de serviço estabelecidos.

A graduação da gravidade e classificação de incidentes serão baseados na estimativa de tempo de interrupção e recuperação dos processos críticos, bem como do impacto operacional e dos negócios da Companhia. Este processo está descrito na Política de Gerenciamento de Incidentes da SPC Grafeno.

São premissas da **SPC GRAFENO** para respostas a situação de crise:

- A segurança de pessoas;
- A extensão dos danos à infraestrutura de Tecnologia da Informação e Segurança;
- Indisponibilidade de se comunicar com outros sistemas (ecossistema e Interop);
- A disponibilidade de pessoa(s)-chave(s) para operação e manutenção de processos de negócios críticos para a companhia;
- A duração da falha / interrupção.

5.7. PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade de Negócios (PCN) da **SPC GRAFENO** é desenvolvido para assegurar que as operações críticas sejam retomadas rapidamente em caso de interrupções. Com base na Análise de Impacto no Negócio (BIA), o PCN define procedimentos de continuidade de negócios (PCO), o procedimento de respostas a incidentes (PRI) e o procedimento de recuperação de desastres (PRD), claros e com prazos definidos para a recuperação das atividades, além de ações de comunicação necessárias para manter todas as partes interessadas informadas.

As equipes de continuidade são identificadas por pessoas chaves com responsabilidades pelos processos críticos, garantindo uma resposta coordenada e eficaz. A comunicação é fundamental, com planos específicos para manter a transparência durante a recuperação. No caso de acionamento de colaboradores backup, serão seguidos os critérios formais estabelecidos no Plano de Continuidade de Negócios e no Plano de Continuidade Operacional, devendo ser documentado e avaliado em testes de resiliência. Cada processo “Vital” identificado no BIA deve ter designado o **titular e backup**, para a execução da atividade.

Para assegurar a eficácia, o PCN é regularmente testado e revisado, com ajustes contínuos baseados nos resultados dos testes e mudanças no ambiente de negócios. A preparação inclui treinamento constante da equipe e a manutenção de recursos essenciais e plano de contingência.

5.8. TESTES DE RESILIÊNCIA OPERACIONAL

Os testes de resiliência operacional da **SPC GRAFENO** são realizados, no mínimo, anualmente, para validar a recuperação de processos críticos e aprimorar planos de contingência com base nos resultados observados. Esses testes abrangem o ambiente de infraestrutura do negócio e a operação dos processos críticos definidos no BIA e respectivos procedimentos operacionais (PCOs).

Os testes a serem realizados devem seguir as seguintes diretrizes do art. 78 da Resolução BCB 304/23:

- Eventos que possam acarretar a interrupção das atividades críticas e a perda ou inacessibilidade da equipe responsável por essas atividades;

- Tenham seus resultados documentados, incluindo a descrição de eventuais providências a serem adotadas para melhoria dos procedimentos;
- Tenham seus resultados avaliados por equipe independente e levados ao conhecimento dos administradores;
- Incluam a participação das áreas operacionais de acordo com os Planos de Continuidade Operacional (PCOs) desenvolvidos para os processos críticos;
- Incluam a participação de terceiros responsáveis pela prestação de serviços críticos e agentes do mercado; e
- Sejam realizados preferencialmente em condições normais de funcionamento da IOSMF.

Durante os testes, deverão ser verificadas a eficácia dos procedimentos de recuperação e a prontidão das equipes de resposta. As pessoas chave e os recursos necessários são avaliados para garantir que todas as ações necessárias possam ser executadas conforme planejado. A comunicação interna e externa também é testada para assegurar a transparência e a coordenação durante incidentes.

5.8.1. Escopo e Abrangência dos Testes

Os testes de resiliência operacional devem prever o envolvimento das áreas de Negócios, a interação com agentes do mercado e prestadores de serviços críticos e abrangerem**, no mínimo**, os seguintes requisitos:

- Simulação de ataque Cibernético: derrubada da aplicação;
- Simulação de Desastre e Backup: derrubada do Banco de dados;
- Simulação da Integração entre sistemas;
- Simulação de Negócios: Operações realizadas e processadas pelo cliente, durante o Teste;
- Simulação de troca de zona geográfica: Negócio rodando em outra região Geográfica;
- Avaliação de Negócio: Usuário (cliente) realizando operações durante o período simulado (em contingência e no retorno para produção);
- Simulação de Operações: Área de Operações validando as operações efetuadas, durante o teste;
- Testes periódicos de Segurança e Cyber: Scan de Vulnerabilidades; Pentest e exercícios de simulação dos procedimentos de respostas à incidentes;
- Testes de continuidade operacional dos processos classificados como “Vital” (conforme escopo a ser definido no Planejamento do Teste de Resiliência Operacional), estabelecidos no BIA;
- Simulação do Plano de Resposta a Incidentes (PRI); e
- Testes relacionados ao Plano de Recuperação e Saída Ordenada.

5.8.2. Cenários de incidentes considerados nos Testes de Resiliência Operacional

- **Cenário de Perda de TI ou Ataque Cibernético:** A Equipe de Contingência efetuará todos os testes necessários a fim de garantir que a operação e a recuperação das atividades se darão de acordo com o prazo definido, conforme regulamentação vigente. Para este cenário de teste, devem ser considerados como apoio, os resultados dos testes periódicos de Scan de Vulnerabilidades (mensal) e Teste de Penetração – Pentest (anual).
- **Cenário de Indisponibilidade da infraestrutura física no local de pessoa chave com acesso remoto**: Para as pessoas chave que residem em outras localidades, será permitido que realizem os testes em locais alternativos previamente definidos no PCO (Plano de Continuidade Operacional) ou no Planejamento do Teste de Resiliência Operacional. Esses locais alternativos devem garantir que todos os envolvidos possam participar efetivamente dos testes, independentemente de sua localização, e assegurando a viabilidade dos planos de continuidade de negócios em diferentes cenários. Devem ser elaborados relatórios para cada teste executado, contendo as evidências e resultados dos testes, bem como pontos de falhas e melhorias identificados.
- **Cenário de Inacessibilidade da sede principal:** A SPC Grafeno conta com um site secundário que poderá ser utilizado para o deslocamento das pessoas chaves, em situação de contingência, quando necessário. Para os testes periódicos de continuidade de negócios, as pessoas chave poderão se deslocar para o site alternativo principal, conforme definido no PCO (Plano de Continuidade Operacional).

As atividades dos testes e os resultados, serão considerados como insumos para o teste de estresse planejado, conforme o Plano de Recuperação e Saída Ordenada, com o objetivo de validar a capacidade de resposta da Companhia, em caso de falha crítica em sua infraestrutura tecnológica.

5.8.3. Compromisso com a continuidade de serviços contratados

A SPC GRAFENO adota procedimentos para garantir a continuidade de seus serviços críticos, incluindo atividades de escrituração e registro de duplicatas, processamento e armazenamento de dados, e utilização de computação em nuvem. Para isso, conta com a infraestrutura confiável da AWS, reconhecida mundialmente pela segurança, escalabilidade e alta disponibilidade de seus serviços.

A AWS é responsável pela segurança e disponibilidade da nuvem, assegurando a proteção, configuração e operação da infraestrutura que suporta seus serviços. Essa infraestrutura inclui hardware, software, redes e instalações que mantêm a operação de todos os recursos oferecidos.

Como parte do compromisso com a continuidade dos negócios, a SPC GRAFENO utiliza o serviço de múltiplas zonas de disponibilidade da AWS. Em caso de indisponibilidade de uma zona de disponibilidade (data center físico da AWS), o fornecedor realiza a comutação automática dos sistemas e recursos lógicos para outra zona ativa dentro da mesma região. Atualmente, a SPC GRAFENO opera na infraestrutura da AWS localizada na Região de São Paulo (região **sa-east-1**), que disponibiliza três zonas de disponibilidade, assegurando resiliência e capacidade de recuperação em situações de falha.

Além disso, a SPC GRAFENO realiza testes regulares de resiliência operacional, incluindo a simulação de falhas nos serviços contratados. Esses testes são essenciais para verificar a eficácia dos planos de recuperação, preparar as equipes para responder a incidentes de forma ágil e

identificar melhorias contínuas. Esse compromisso reflete a prioridade da SPC GRAFENO em manter a operação de seus serviços com excelência e segurança para os clientes.

5.8.4. Monitoramento de dependência e aceite de risco

A SPC Grafeno possui monitoramento contínuo da disponibilidade dos serviços AWS, com alertas automatizados e planos de resposta a incidentes. Conta também com suporte Premium contratado junto à AWS, garantindo atendimento prioritário e suporte técnico especializado.

A eventual substituição do provedor contratado será considerada com base nessas análises e, quando aplicável, tratada por controles e documentos estratégicos de acesso restrito (PRD, PCN e Matriz de Riscos e Controles).

A Companhia mantém documento formal de Aceite de Risco, sobre essa dependência do provedor de serviços críticos, com avaliação operacional, jurídica e regulatória, que registra:

- arquitetura de múltiplas zonas de disponibilidades e controles;
- viabilidade e limitações de Multi-Nuvem (complexidade/custo/portabilidade);
- interdependências sistêmicas externas;
- suporte Premium contratado; e
- classificação de probabilidade/impacto emitida por avaliação técnica independente.

O aceite foi aprovado pelo Conselho de Administração, com gatilhos de reavaliação (p.ex., descumprimento recorrente de SLA, incidentes severos, alterações contratuais/regulatórias ou elevação do risco residual) e revisão periódica.

5.8.5. Estrutura e Comunicação sobre os resultados dos testes

Para cada teste realizado, será emitido um relatório individual, contendo:

- Objetivo do Teste;
- Escopo e Cenários Avaliados;
- Resultados Obtidos;
- Identificação de Gaps e Oportunidades de Melhoria;
- Plano de Ação e Responsáveis.

O relatório dos testes realizados deve conter o resultado do escopo e abrangência definidos para os testes, ser avaliado e assinado pela Diretoria de Operações, pela Diretoria de Riscos, CI, Compliance e SI e Diretoria de Tecnologia, Dados e Inovação, endereçado para o Diretor Presidente e, conforme descrito no artigo 78 da Resolução BCB 304/23, deve ser avaliado por equipe independente. Caso algum item do escopo de testes não tenha sido testado, a justificativa deverá constar neste relatório. Adicionalmente, o relatório deverá ser enviado para o conhecimento dos órgãos de governança da Companhia.

Os resultados apresentados pelos testes devem ser utilizados para identificar áreas de melhoria e ajustes nos procedimentos e planos para melhoria contínua da resiliência operacional da empresa.

Isso inclui atualizações na documentação, treinamento adicional para a equipe e ajustes nos recursos de contingência.

5.9. GESTÃO DE MUDANÇAS

O Sistema de Gestão de Continuidade de Negócios, adotará o processo de gestão de mudanças com o objetivo de proteger o sistema de gestão contra mudanças não autorizadas, provendo a governança das solicitações de mudanças, conforme definições do Manual de Gestão de Mudanças da Companhia.

A **SPC GRAFENO** deve garantir que as mudanças no sistema de gestão sejam controladas e adequadas durante sua execução, com o objetivo de proteger o sistema de gestão contra mudanças não autorizadas, provendo a governança das solicitações de mudanças.

As mudanças devem:

- Serem implantadas com o mínimo impacto durante o horário comercial, assim como em períodos de fechamento contábil;
- Devem atualizar os documentos que compõem o Sistema de Gestão de Continuidade de Negócios;
- Serem autorizadas antes de sua implantação e devem respeitar os controles e a continuidade do ambiente; e
- As alterações planejadas pela Companhia que venham a afetar de maneira relevante a Gestão da Continuidade de Negócios, deve ser comunicada ao Banco Central do Brasil com 30 (trinta) dias de antecedência.

5.10. TREINAMENTO E CAPACITAÇÃO

A **SPC GRAFENO** deve manter um programa contínuo de treinamento e capacitação técnica, com objetivo de assegurar o desenvolvimento das competências necessárias para que todas as equipes envolvidas, em suas atribuições e funções, estejam aptas para gerenciar, planejar, desenvolver, formalizar, manter, testar, executar e liderar as estratégias de continuidade de negócios da Companhia, diante de incidentes, eventos inesperados e disruptivos.

5.11. COMUNICAÇÃO

A SPC Grafeno adota estratégias de continuidade para garantir a rápida recuperação das operações diante de eventos disruptivos. Para isso, estabelece um processo de comunicação e acionamento de equipes estruturado**,** garantindo que, em caso de incidente, os responsáveis sejam notificados imediatamente e possam executar as ações necessárias para a mitigação do impacto.

O acionamento do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD) ocorre a partir da decisão do Comitê de Gestão de Crise e Risco Operacional (CGCRO), que coordena as ações em conjunto com as áreas responsáveis.

Todo incidente que comprometa a continuidade dos serviços deve ser comunicado de imediato ao Gestor da Continuidade de Negócios e à Unidade de Negócio responsável, para as providências necessárias e o acionamento dos respectivos planos de continuidade.

Deve-se comunicar tempestivamente o Banco Central do Brasil sobre as ocorrências e as interrupções que configurem uma situação de crise pela IOSMF, bem como as providências para o reinício das suas atividades.

5.12. MELHORIA CONTÍNUA

Buscando aprimoramento da qualidade e efetividade do sistema de gestão, a **SPC GRAFENO** adota um processo de melhoria e investe em novas metodologias e na capacitação de seus colaboradores, visando atingir padrões cada vez mais elevados para os processos de Gestão de Continuidade de Negócios.

Para assegurar a implementação e efetividade de uma Política de Continuidade de Negócios (PCN), a **SPC GRAFENO** definira e implementará mecanismos sólidos de acompanhamento e controle, através de Indicadores de aderência à Política e procedimentos.

6. DISPOSIÇÕES GERAIS

6.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

6.2. CASOS OMISSOS

Os casos omissos serão regulados pelo Comitê de Ética da Companhia, conforme necessário.

6.3. DIVISIBILIDADE

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

7. REVISÃO DA POLÍTICA

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

8. VIOLAÇÕES

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

9. CONTROLE DE VERSÕES

Versão	Data	Responsável	Ocorrência

1.0	02/08/2024	Área de Riscos e Controles Internos	Elaboração do documento
1.0	27/08/2024	Comitê de Riscos, Compliance e SI	Aprovação do documento
1.0	03/10/2024	Conselho de Administração	Aprovação final do documento
2.0	21/01/2025	Área de Riscos e CI (Consultoria SION)	Revisão do documento
2.0	14/03/2025	Comitê de Riscos, Compliance e SI	Aprovação do documento
2.0	08/04/2025	Conselho de Administração	Aprovação final do documento
3.0	09/09/2025	Área de Riscos e CI	Revisão do documento: Ajustes no item 5.2 – definições separadas de continuidade, contingência, classificação dos processos críticos e definição de desastre; Item 5.3 - Reformulada as atribuições da Auditoria Interna, uma vez que esta área não realiza auditorias de certificação de ISOs específicas. Item 5.8.2 – Inclusão sobre os testes de estresses financeiro (RGN) que deverá constar no planejamento dos testes de GCN; Item 5.8.4 – Reforço sobre a formalização do aceite de riscos pela dependência de um único provedor de serviços de nuvem; Revisão geral do normativo e harmonização de termos e disposições, sobretudo Política, BIA e PCN.
3.0	26/09/2025	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento.
3.0	30/09/2025	Conselho de Administração	Aprovação final do documento.
4.0	01/10/2025	Área de Riscos e Controles Internos	Revisão do documento: Inclusão de menção à atividade da Escrituradora; Inclusão de cenários de testes (incidentes e PRSO).
4.0	07/11/2025	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento
4.0	07/11/2025	Conselho de Administração	Aprovação final do documento

***