SPC GRAFENO

PLANO DE CONTINUIDADE DE NEGÓCIOS CORPORATIVO

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

SUMÁRIO

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

1. OBJETIVO

O presente Plano de Continuidade dos Negócios Corporativo (“PCN” ou “Plano”) estabelece, de maneira preventiva, um conjunto de procedimentos e medidas que visam assegurar a continuidade das atividades críticas da SPC Grafeno Infraestrutura e Tecnologia para o Sistema Financeiro S.A. (“Companhia”) na hipótese de ocorrência de um ou mais eventos fortuitos que afetem significativamente suas operações. Este plano é desenvolvido em conformidade com a Resolução 304 do Banco Central do Brasil e os Princípios para Infraestruturas de Mercado Financeiro (PFMI).

As disposições deste Plano devem ser interpretadas em conjunto com o Plano de Recuperação de Desastres (“PRD”) e Política de Segurança da Informação e Cibernética (“PSIC”).

2. ABRANGÊNCIA

O âmbito de aplicação do presente Plano engloba todas as atividades operacionais da SPC Grafeno, quando conduzidas sob condições normais, nas suas instalações centrais. Isso abrange não somente as infraestruturas físicas, mas também as soluções tecnológicas adotadas para tais operações.

3. DOCUMENTOS DE REFERÊNCIA

- Política de Gerenciamento de Riscos e Controles
- Plano de Recuperação de Desastres
- Política de Segurança da Informação e Cibernética
- Playbook Operacional
- Resolução 304 do Banco Central do Brasil
- Princípios para Infraestruturas de Mercado Financeiro (PFMI)

4. ALÇADAS DE APROVAÇÃO

- Comitê de Gerenciamento de Riscos – responsável pela revisão e aprovação do documento
- Conselho de Administração – responsável pela aprovação do documento

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

5. DIRETRIZES

5.1 PRINCIPAIS OBJETIVOS DO PLANO

- 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 de ativos financeiros. 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 propriedade intelectual, 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; e
- Assegurar que todos os colaboradores da SPC Grafeno conheçam o Plano de Continuidade de Negócio Corporativo.

5.2 CONCEITOS GERAIS

- **Gestão da Continuidade do Negócio:** Compreende treinamentos, testes, revisões e manutenções para garantir a execução e atualização do Plano de Continuidade da SPC Grafeno.
- **Business Impact Analysis (BIA):** Engloba todas as atividades ou processos críticos relacionados ao registro de ativos financeiros da SPC Grafeno.
- **Estado de Contingência Operacional:** Refere-se a situações em que os procedimentos operacionais não estão dentro da normalidade, limitando e prejudicando a eficiência dos Processos Críticos.
- **Incidente:** É qualquer evento que possa impactar negativamente a rotina operacional das atividades da SPC Grafeno, podendo, em casos graves, ser classificado como Desastre.
- **Desastre:** É um incidente que resultou em um "Tempo de Queda" ("Downtime") superior ao tempo máximo especificado no item 5.4 - Processos Críticos deste documento.
- **Playbook Operacional:** Plano de continuidade de negócios departamental que descreve as ações a serem executadas pelas pessoas chaves definidas no BIA, em caso de acionamento do estado de contingência.

5.3 RESPONSABILIDADES

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

5.3.1 Comitê de Gestão de Crise e de Risco Operacional (CGCRO)

O CGCRO da SPC Grafeno é um órgão de caráter permanente composto pelo Diretor de Riscos, Controles Internos e Compliance, Diretor de Operações, Diretor de Tecnologia e Gerente de Riscos, Controles Internos e Compliance da SPC Grafeno, sendo responsável pelas seguintes responsabilidades:

No âmbito de Operações:

- Coordenação e execução do Plano de Continuidade dos Negócios (PCN);
- Acompanhamento da disponibilidade do quadro de colaboradores, em linha com as diretrizes do PCN;
- Avaliação de eventual impacto reputacional, em eventos classificados como incidentes ou crises;
- Comunicação com os provedores de infraestrutura de mercado;
- Comunicação com as principais contrapartes, quando necessário;
- Decidir pela decretação do Estado de Contingência Operacional e de acionar as pessoas envolvidas no Plano de Continuidade dos Negócios.

No âmbito de Tecnologia da Informação:

- Comunicação com fornecedores de infraestrutura de TI;
- Coordenação e execução do Plano de Recuperação de Desastres (PRD);
- Avaliação de eventual impacto reputacional, em eventos classificados como incidentes ou crises;
- Acompanhamento da disponibilidade do quadro de colaboradores, em linha com as diretrizes do PCN;
- Em Estado de Contingência, acionamento da infraestrutura de TI de contingência, conforme Plano de Recuperação de Desastres;
- Em Estado de Contingência, acompanhamento da higidez da infraestrutura de TI.

No âmbito da Presidência:

- Comunicação com a mídia, quando necessário;
- Avaliação de eventual impacto reputacional, em eventos classificados como incidentes ou crises;
- Execução de medidas de contenção de riscos para a imagem da Companhia;
- Em Estado de Contingência Operacional, execução de medidas de contenção de riscos;

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

- Em Estado de Contingência Operacional, comunicação com os principais clientes, se necessário;
- Em Estado de Contingência Operacional, avaliar impacto nos clientes das medidas do PCN;

No âmbito de Compliance, Riscos e Controles Treinamento:

- Conscientização e comunicação com os colaboradores;
- Coordenação e execução do Plano de Continuidade dos Negócios (PCN);
- Avaliação da adequação das medidas tomadas em contingência às políticas, normas e regulação em vigor;
- Em Estado de Contingência Operacional, realizar registro das medidas tomadas e coleta de evidências;
- Acompanhamento da disponibilidade do quadro de colaboradores, em linha com as diretrizes do PCN;

5.3.2 Área de Operações

- Implementar o PCN, de forma a conduzir e participar dos testes periódicos e assegurar a manutenção dos processos críticos de negócio;
- Interagir com a Diretoria de Tecnologia para:
  - Encaminhar de forma estruturada os bugs e acompanhar resoluções, conforme SLOs acordados entre as áreas para garantir o cumprimento dos SLAs com os nossos clientes;
  - Sugerir evoluções e reportar melhorias capturadas em prospecções e/ou atendimento a clientes; Auxiliar no processo de revisão de GMUD e execução de planos de contingência.

5.3.3 Área de Riscos e Controles Internos

A área de Riscos e Controles Internos tem como responsabilidades:

- Revisar o Plano de Continuidade de Negócios e de Recuperação de Desastres, além do BIA (*Business Impact Analysis*), com a periodicidade anual;
- Realizar em conjunto com as áreas de TI e de Operações os testes anuais do PCN e PRD;
- Coordenar a efetividade de execução do Plano de Continuidade de Negócios;
- Monitorar a implementação de melhorias em relação às lições aprendidas.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

5.3.4 Área de Tecnologia da Informação

- Acionar o Plano de Recuperação de Desastres em caso de falhas na infraestrutura tecnológica que compõem a Plataforma SPC Grafeno;
- Manter comunicação com fornecedores de infraestrutura de Tecnologia da Informação;
- Acionar infraestrutura de Tecnologia da Informação de contingência, conforme PRD, em estado de contingência;
- Acompanhar a higidez da infraestrutura de tecnologia da informação em estado de Contingência;
- Atualizar PRD anualmente, ou a cada atualização de processos e tecnologia, juntamente com a área de Riscos e Controles Internos;
- Participar dos testes anuais do PCN e PRD, com o apoio de Riscos e Controles Internos e Operações; e
- Assegurar a continuidade das atividades da Companhia em tempo aceitável conforme regulamentação aplicada.

5.4 PROCESSOS CRÍTICOS

Processos Críticos são todos aqueles que, uma vez paralisados, por tempo superior ao definido pela Resolução nº 304, do Banco Central, irão afetar de forma sensível as operações e serviços da Companhia gerando impactos negativos em clientes internos e externos, ocasionando assim um desastre.

5.4.1 Processos Críticos da SPC Grafeno

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. Esses processos devem ser mantidos ativos em tempo integral. Em caso de qualquer interrupção que ultrapasse o RTO previsto, o CGCRO será acionado para decretar o estado de contingência operacional para que as medidas de contingência sejam implementadas e garantir a retomada o mais breve possível:

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

- **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.

O tempo máximo de queda mensal de processos críticos suportados para a Companhia é calculado através do conceito MTD = RTO + WRT. Sendo ele definido a seguir:

- MTD (*Maximum Tolerable Downtime*) = Tempo máximo que o negócio pode tolerar a ausência ou indisponibilidade de um processo crítico. A somatória de tempo dos processos de WRT e RTO deve ser igual ou inferior ao MTD definido pela Companhia.
- RTO (*Recovery Time Objective*) = Determina o tempo máximo tolerável para colocar todos os sistemas ou processos críticos online novamente. Por exemplo, restaurar dados do backup ou correção de uma falha.
- WRT (*Work Recovery Time*) = Determina a quantidade máxima tolerável de tempo necessária para verificar o sistema e/ou a integridade dos dados. Por exemplo, verificar os bancos de dados e logs, certificando-se de que os aplicativos ou serviços estejam em execução e disponíveis.

O valor do MTD não deve ser superior **a 2 (duas) horas**, o prazo definido pela Resolução nº 304, do Banco Central. Caso identificado pela análise do CGCRO que o prazo para retomada dos processos críticos irá ser superior àquele ao definido, será decretada situação de “Desastre” e acionado o PRD (Plano de Recuperação de Desastres) para contenção do impacto.

Os planos de continuidade de negócios departamentais, aqui chamados de “playbooks operacionais", descrevem as atividades que devem ser executadas pelas pessoas chaves definidas no BIA, quando da ativação do estado de contingência pelo CGCRO.

5.5 PLANO DE RESPOSTA A INCIDENTES

A SPC Grafeno possui o **Plano de Resposta a Incidentes** elaborado com o objetivo principal de estabelecer um conjunto de diretrizes, procedimentos e recursos necessários para lidar de forma eficaz com incidentes de segurança cibernética, desastres naturais, crises de negócios, ou qualquer evento que possa impactar significativamente as operações ou a segurança da organização. O Plano de Resposta a Incidentes é uma parte essencial da gestão de riscos e da continuidade de negócios, e seu principal objetivo é garantir que a organização possa responder de maneira coordenada, eficiente e eficaz a eventos adversos, minimizando seus impactos negativos.

Incidente é qualquer evento que possa impactar negativamente a rotina operacional das atividades da SPC Grafeno, podendo, em casos graves, ser classificado como Desastre.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

A análise da gravidade de Incidentes e/ou Crises leva em consideração uma avaliação qualitativa da urgência da necessidade do negócio *versus* a estimativa do tempo de interrupção do negócio, ambas as informações fornecidas pelas áreas de operação e tecnologia da informação. A partir da gravidade, identifica-se se é um Incidente ou Crise.

5.5.1 Exemplos de Ocorrências de Incidentes

Na análise dos possíveis Incidentes que podem estabelecer a situação de contingência, são levados em consideração aqueles que podem ocasionar falhas de equipamentos ou programas de computador, comprometer a comunicação, interrupção, por qualquer razão, do fornecimento de energia elétrica, dos serviços de comunicação, e o acesso às instalações físicas da Companhia:

- **Incapacidade de acesso às instalações físicas**: incêndios, explosões, inundações (vazamento, rupturas de tubulação), distúrbios civis (greves, passeatas), catástrofes naturais (chuvas, enchentes);
- **Falhas de equipamentos ou programas de computador**: falha de equipamento ou software intencional ou não, sabotagem, ataques internos e externos (vírus, hackers);
- **Falhas de equipamentos de comunicação**: sabotagem, ataques internos e externos (vírus, *hackers*), sobrecarga no tráfego da rede, perda de performance, indisponibilidade do *firewall*;
- **Interrupção do fornecimento de energia elétrica**: término do contrato, inadimplemento das partes contratantes, entre outras hipóteses;
- **Interrupção dos serviços de comunicação**: impossibilidade de uso de qualquer dos meios de comunicação para atendimento ao cliente;
- **Incidentes de Segurança da Informação ou Cibernéticos**: são eventos não planejados que comprometem a confidencialidade, integridade ou disponibilidade de dados e sistemas digitais. Eles podem incluir ataques cibernéticos, vazamentos de dados, malware ou qualquer atividade que represente uma ameaça à segurança das informações e sistemas de uma organização.

5.5.2 Acionamento do CGCRO

O CGCRO deve ser acionado em todas as situações de desastre, especialmente em casos classificados como "muito graves", nos quais a responsabilidade recai sobre este órgão colegiado da SPC Grafeno. Para outras situações, a responsabilidade pela ação deve permanecer com os gestores da área de negócios. Qualquer exceção deve ser submetida à análise do CGCRO.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

ESTIMATIVA DO TEMPO DE INTERRUPÇÃO	É POSSÍVEL AGUARDAR?	GRAVIDADE	ALÇADA DE ATUAÇÃO	CLASSIFICAÇÃO
Até 1 hora	Sim	Tolerável	Gestor da Área de Negócios	Incidente
	Não	Sério	Gestor da Área de Negócios	Incidente
Entre 1 e 2 horas	Sim	Relevante	Gestor da Área de Negócios	Incidente
	Não	Muito sério	Diretoria Executiva)	Incidente
Entre 2 e 4 horas	Sim	Muito relevante	Gestor da Área de Negócios	Incidente
	Não	Desastre	CGCRO	Desastre
Acima de 4 horas	Sim	Grave	CGCRO	Desastre
	Não	Catástrofe	CGCRO	Desastre

Tabela 2. Análise do grau da gravidade e classificação de Incidente e Crise

5.5.3. Incidentes de Tecnologia e Infraestrutura

Ao serem identificados incidentes tecnológicos, através das ferramentas descritas no Anexo 3 - “Infraestrutura do Ambiente Registradora”, ou qualquer outro incidente de fonte tecnológica que prejudique a operação da Companhia, os membros do CGCRO deverão ser comunicados pela área de Tecnologia.

Será analisado pelos membros do CGCRO o impacto gerado pelo incidente e o tempo necessário para normalização do ocorrido.

A área de Tecnologia será responsável por garantir a normalização dos processos críticos e, caso necessário, acionar o suporte necessário para garantir que o prazo MTD seja cumprido.

Etapas na Gestão de Incidentes de Tecnologia e Infraestrutura:

- **Incidente identificado**: Quando um eventual problema na plataforma é identificado e há atuação no reconhecimento ou resolução do problema, porém ainda sem previsão de resolução;
- **Incidente Monitorado:** Quando uma ou mais tentativas de resolução são aplicadas e a equipe está monitorando o efeito de tal ação. Importante destacar a ação singular na resolução dos ambientes, onde cada tentativa deve passar pelo ciclo de validação, a fim de próprias resoluções simultâneas não gerarem um novo incidente ou um falso positivo (ou falso negativo);
- **Incidente Resolvido:** Quando o incidente foi monitorado e após a implementação da resolução, o mesmo não teve reincidência no período de tempo especificado pela equipe para o monitoramento.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

5.5.4 Incidentes de Segurança da Informação e Cibernética

Os incidentes de Segurança da Informação e Cibernética são tratados de acordo com o descrito no documento Plano de Resposta a Incidentes da SPC Grafeno. Em caso de incidentes que possam afetar os processos críticos da Companhia, o Comitê de Gestão de Crise e Risco Operacional (CGCRO) realizará uma avaliação para determinar a necessidade de ativar o estado de contingência, seguindo as etapas estabelecidas no Plano de Continuidade de Negócios (PCN).

5.5.5 Incidentes de Infraestrutura Física

Na Companhia, nossa operação é predominantemente baseada em um ambiente de trabalho remoto, mantendo sua sede em endereço físico localizado na Av. Brigadeiro Faria Lima, 1355 – 1º andar, cuja infraestrutura está detalhada no **Anexo 1 – Infraestrutura do Edifício da Sede**, deste documento. Em caso de indisponibilidade do home office e do endereço físico do escritório (matriz), recorremos à nossa estrutura secundária (site backup) localizada a 700 metros do site principal.

Esta abordagem em camadas para a infraestrutura física garante a continuidade das operações da SPC Grafeno, mesmo diante de eventos imprevistos que possam afetar nossos locais de trabalho principais. Ao serem comunicados ao CGCRO os incidentes que resultem em impedimento de acesso ao prédio, é de sua responsabilidade estabelecer contato com a Administração do Condomínio para esclarecimentos. Os procedimentos de contingência física estão descritos no Anexo 4 - “Contingência da Infraestrutura Física”.

Administração do Prédio:

- Avenida Faria Lima – 1355 – São Paulo / SP - Telefone (11) 5041-6599

Telefones de Emergência:

- Bombeiros: 193 (Em casos de incêndio e ameaças de bombas)
- Defesa Civil: 199 (Em casos de ameaças de bombas, greves, bloqueios e inundações)
- Polícia Civil: 147 (Em casos de ameaças de bombas, roubo e furto de informações ou ativos)

5.5.6 Declaração de Estado de Contingência

Quando incidentes que possam impactar o funcionamento da Companhia forem identificados, é responsabilidade do CGCRO informar imediatamente a Presidência para que sejam tomadas as devidas ações de comunicação internas e externa e outras medidas necessárias. Além disso, a Companhia, por meio do Presidente do CGCRO, deve prontamente notificar o Banco Central do Brasil sobre quaisquer ocorrências ou interrupções que caracterizem uma situação de crise na Companhia, bem como as providências tomadas para retomar suas atividades, em observação ao inciso VIII do art. 78, da Res. 304.

Com base nas informações recebidas e com o prazo estipulado para normalização do incidente, é de responsabilidade do CGCRO declarar ou não o estado de contingência e de desastre.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

5.5.7 Ciclo do Gerenciamento da Contingência

A seguir são apresentadas as fases do Ciclo do Gerenciamento da Contingência (imagem 2) e descritas as ações a serem realizadas em cada período.

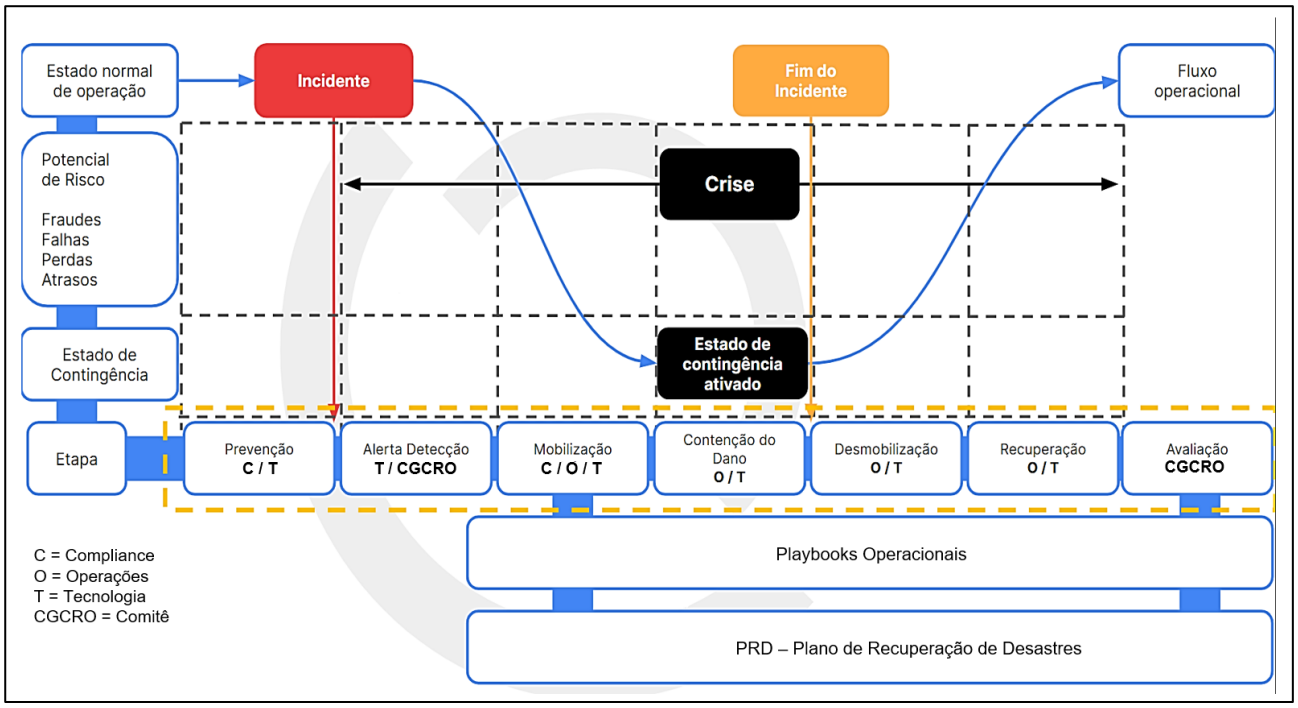


Imagem 2. Ciclo de Gerenciamento da Contingência

PREVENÇÃO

- Elaborar Playbooks Operacionais e o Plano de Recuperação de Desastres (PRD);
- Analisar ocorrências potenciais e respectivos efeitos nos Processos Críticos da Companhia;
- Realizar testes dos Playbooks Operacionais e Plano de Recuperação de Desastres; e
- Treinar colaboradores, fornecedores e terceiros com os quais a Companhia possua parceria comercial.

ALERTA/DETECÇÃO

- Identificar o evento;
- Decretar Estado de Contingência Operacional; e
- Analisar e classificar o evento.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

MOBILIZAÇÃO

- Acionar as pessoas chaves, processos e recursos alternativos.

CONTENÇÃO DO DANO

- Obter o atendimento das necessidades de negócios em Estado de Contingência Operacional, assegurando a conclusão das operações até o final do dia da ocorrência do evento; e
- Para as situações não previstas, buscar soluções para contornar o Incidente e superar os problemas oriundos dele.

DESMOBILIZAÇÃO

- Comunicar a implementação da correção dos problemas provocados pelo Incidente; e
- Decidir o início da recuperação do estado de normalidade operacional.

RECUPERAÇÃO

- Iniciar procedimentos para retomada do estado de normalidade operacional; e
- Verificar a integridade das operações cursadas durante o Estado de Contingência Operacional.

AVALIAÇÃO

- Avaliar as causas do Incidente;
- Registrar ocorrência em Sistema e informar detalhadamente o CGCRO para a mitigação de novas ocorrências;
- Avaliar a efetividade do PCN;
- Revisar e atualizar o PCN; e
- Aplicar novo treinamento aos colaboradores, fornecedores e terceiros com os quais a Companhia possua parceria comercial.

5.5.8 Ações a Serem Realizadas em Caso de Desastre

Caso decretado pelo CGCRO situação de Desastre, onde o prazo necessário para retomada de atividades seja superior ao MTD, é necessária ativação de Contingência, onde devem ser realizadas as seguintes ações:

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

ÁREA	AÇÃO	PROCESSO AFETADO
CGCRO	● Comunicar a Presidência do ocorrido; ● Avaliar o prazo estimado para retorno do processo e dispara a movimentação do time de operações para resumo do processo; ● Acionar a Equipe de Contingência; ● Encaminhar-se até o site de contingência para resumir operações críticas o mais rápido possível, se for necessário o deslocamento; ● Encaminhar comunicado aos clientes sobre o ocorrido e informe que apenas os processos críticos serão mantidos até normalização; ● Encaminhar comunicado aos clientes sobre encerramento de situação de desastre.	● Registro dos Ativos Financeiros no Sistema de Registro SPC Grafeno
Operações	● Interagir com a área de TI para a execução de planos de contingência, caso seja necessário.	● Registro dos Ativos Financeiros no Sistema de Registro SPC Grafeno
Tecnologia	● Contenção do incidente e, se necessário, acionar o PRD.	● Registro dos Ativos Financeiros no Sistema de Registro SPC Grafeno

5.5.9 Avaliação do Plano

Após normalização da situação de desastre ou contingência. O CGCRO será responsável por tomar nota de todas as medidas que foram adotadas para solução do incidente, assim como será responsável por avaliar planos de ação para que o incidente não volte a ocorrer, caso possível.

Ele também será responsável por avaliar as medidas tomadas e, caso as medidas tenham sido insuficientes, promover alterações nos planos de resposta para que passem a se adequar ao MTD disponível.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

6. ESTADO DE CONTINGÊNCIA OPERACIONAL

O Estado de Contingência Operacional tem início e fim descritos abaixo. As informações de contato dos profissionais que atuam na estrutura de contingência estão expostas no Anexo 2 – "Equipe de Contingência e Membros do CGCRO".

6.1. DECLARAÇÃO DE INÍCIO DA CONTINGÊNCIA OPERACIONAL

- As áreas de Compliance, Operações e Tecnologia acionarão todos os membros da Equipe de Contingência para a operação em contingência, através de seus contatos telefônicos e via e-mail, com acionamento do PRD.
- Na hipótese de algum membro da Equipe de Contingência não estar disponível, será acionado o membro alterno (*backup*), consoante a lista do Anexo 2 – "Equipe de Contingência e Membros do CGCRO" deste documento.
- O CGCRO comunicará, por *e-mail*, todos os funcionários da Companhia sobre a situação de contingência. Caso a contingência comprometa os serviços de *e-mail*, a comunicação acontecerá por mensagem de texto ou aplicativo de mensagem instantânea.
- Conforme necessário, o CGCRO, por meio do seu Presidente, informará, por *e-mail*, a todos os stakeholders eventualmente afetados pelo incidente, tais como provedores de infraestrutura, agentes de mercado, participantes, e o Banco Central do Brasil.

6.2 DECLARAÇÃO DE FIM DA CONTINGÊNCIA OPERACIONAL

O CGCRO decidirá o momento de finalizar a situação de contingência. Identificada a situação de fim da contingência, as seguintes ações serão tomadas:

- O CGCRO informa, a todos os colaboradores da Companhia sobre o encerramento da situação de contingência; e
- O CGCRO deve elaborar e apresentar para à Alta Administração um relatório sobre a situação de contingência ocorrida.

6.3 SITE DA CONTINGÊNCIA (OPERAÇÕES)

As operações em regime de contingência ocorrerão no "site backup", disponibilizado pela Galápagos Capital Investimentos e Participações Ltda, empresa sócia da Grafeno Holding Ltda, da qual a Companhia faz parte.

Considerada a arquitetura dos sistemas utilizados pela Companhia, todos baseados em *software* hospedados e processados em nuvem, o propósito do site de contingência é exclusivamente disponibilizar espaço de trabalho físico com controle de acesso, além de computadores adequados e com acesso à rede. Com esses recursos o time de contingência dará continuidade tempestiva à atividade da Companhia, bem como o adequado atendimento aos clientes e parceiros-chave e a execução em ambiente seguro das atividades operacionais.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

- **Endereço:** Avenida Brigadeiro Faria Lima, número 2055, 7º andar, conjunto 42, Jardim Paulistano, Cidade de São Paulo, Estado de São Paulo, CEP 01452-001. Coordenadas GPS: (-23.5749291, -46.6878304)
- **ETA da sede (carro)**: 05-10 minutos.
- **Telefone**: (11) 3777-2088.
- **Normalização do serviço de registro de ativos financeiros**: em até 2 horas.
- **Número de posições:** 08 (Registradora)
- **Recursos de telefonia:** 01 (um) ramal com acesso a ligações locais e à distância
- **Recursos computacionais**: rede Wi-Fi e estações de trabalho.
- **Recursos materiais**: 01 (uma) sala de reuniões com 08 (oito) posições e serviços compartilhados de impressão, videoconferência e projeção.

7. TESTES DE CONTINGÊNCIA

É fundamental que a Companhia valide o seu plano de contingência para que as equipes técnicas criem sinergia e que os objetivos de recuperação sejam avaliados e indiquem necessidades de correções, sempre de acordo com a realidade operacional da Companhia. A SPC Grafeno adota a prática de testar semestralmente o seu plano de contingência, da seguinte forma:

- **Cenário de Inacessibilidade da sede principal:** As áreas de Operação, Compliance e Tecnologia acionam todos os membros da Equipe de Contingência (Anexo 2 – Equipe de Contingência e Membros do CGCRO), que deverão se deslocar até o site backup, para a operação em contingência, quando necessário. As pessoas chaves definidas no BIA de cada processo crítico, serão acionadas para a realização das atividades no site backup, quando necessário.
- **Cenário de Perda de TI ou Ataque Cibernético:** A Equipe de Contingência efetuará todos os testes necessários a fim de garantir que a operação no site de contingência funcione conforme planejado no Roteiro de Testes e que a recuperação das atividades se dará de acordo com o prazo definido de 2 (duas) horas, conforme regulamentação vigente;
- As equipes de Tecnologia da Informação e Riscos e Controles Internos devem elaborar e apresentar à Alta Administração, um relatório com os resultados de teste de contingência; e
- No relatório, devem ser descritos os planos de ação visando sanar eventuais problemas apontados no teste de contingência.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

8. TREINAMENTOS E DIVULGAÇÃO

A Companhia mantém seu compromisso constante de promover treinamentos, divulgação e compartilhamento de informações sobre processos críticos e continuidade de negócios, regularmente.

Além disso, as diretrizes e informações pertinentes deste Plano são amplamente divulgadas e compartilhadas em toda a equipe através da nossa intranet.

9. REVISÃO E ATUALIZAÇÃO

Esse PCN, juntamente com o PRD, será continuamente revisto e atualizado, no mínimo anualmente, pelas áreas de Tecnologia da Informação, Segurança da Informação e Riscos e Compliance, de forma a se adequar a qualquer mudança de estrutura e do ambiente de negócios da Companhia, seja de sistemas, rotinas, legislação, regras de negócios e requisitos físicos. Qualquer alteração do presente PCN deverá ser aprovada pelo Conselho de Administração.

Qualquer modificação planejada pela Companhia que tenha potencial para significativamente impactar a administração da continuidade operacional será oficialmente notificada ao Banco Central do Brasil, com um prazo mínimo de 30 (trinta) dias de antecedência, através do CGCRO.

10. CONTROLE DE REVISÕES

Versão	Data	Responsável	Ocorrência
1.0	setembro/2019	Diretor de Tecnologia	Elaboração do Documento
2.0	junho/2020	Diretor de Tecnologia	Revisão do Documento
3.0	maio/2021	Diretor de Tecnologia	Revisão do Documento
4.0	março/2023	Gerente de Riscos, CI e Compliance	Revisão do Documento
4.0	março/2023	Diretor de Tecnologia e Diretor de Operações	Revisão do Documento
5.0	setembro/23	Comitê de Gerenciamento de Riscos	Revisão e Aprovação do documento.
5.0	setembro/23	Conselho de Administração	Aprovação do Documento

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

ANEXOS

ANEXO 1 – INFRAESTRUTURA DO EDIFÍCIO DA SEDE

Acesso pessoal: os pontos de entrada e saída do prédio são controlados por uma equipe de segurança profissional utilizando vigilância e passagem por catraca via autenticação por crachá. O prédio contempla saídas de emergência devidamente sinalizadas. Além disso, há controle de acesso no 1º andar do prédio, de modo que, ainda que liberadas a acessar o prédio, apenas pessoas autorizadas conseguem acessar o local de trabalho da Companhia.

Acesso aos equipamentos: os equipamentos requerem identificação pessoal e fornecimento de senha para operarem.

Energia elétrica: Fornecida pela Enel Distribuição São Paulo, os sistemas de energia elétrica são projetados para serem redundantes e passíveis de manutenção sem impacto para as operações, 24 horas por dia.

Caso a interrupção no fornecimento de energia se estenda por até 1 (uma) hora, será acionado o Estado de Contingência Operacional e seguidos os procedimentos descritos neste Plano e seus anexos.

Consulta de interrupções programadas: **https://www.eneldistribuicao.com.br**

Detecção e supressão de incêndio: A estrutura do prédio é dotada de equipamentos automáticos de detecção e supressão de incêndio por sensores de detecção de fumaça.

Local das Operações:

- **Endereço:** Avenida Brigadeiro Faria Lima, número 1355, 1º andar, sala 01, Bairro Jardim Paulistano, Cidade de São Paulo, Estado de São Paulo, CEP 01452-002
- **Coordenadas GPS:** (-23.5693986, -46.6912870)
- **Recursos de telefonia**: 04 (quatro) ramais com acesso a ligações locais e à distância

- **Recursos computacionais:** rede Wi-Fi e estações de trabalho com sistema operacional Windows 7 ou mais recente e pacote MS Office.

- **Recursos materiais:** 01 (uma) sala de reuniões com 08 (oito) posições e serviços de impressão, videoconferência e projeção.

ANEXO 2 – EQUIPE DE CONTINGÊNCIA E MEMBROS DO CGCRO

Equipe de Contingência

NOME / ÁREA	TELEFONE	E-MAIL
Membros Principais		
Bruno Arueira (Tecnologia)	(22) 99812-4481	bruno.arueira@spcgrafeno.com.br
Thiago Senna (Tecnologia)	(11) 98610-5339	thiago.senna@spcgrafeno.com.br
Marcelo Lopes (Riscos)	(11) 99962-0013	marcelo.lopes@spcgrafeno.com.br
Eli Aparecida Simão (Operações)	(11) 992267748	eli.simao@spcgrafeno.com.br
Membros Backup		
Hebert Junior (Tecnologia)	(31) 99176-2295	hebert.junior@spcgrafeno.com.br
Ícaro Oliveira (Tecnologia)	(79) 99928-4373	icaro.silva@spcgrafeno.com.br

2.2 Membros do CGRO

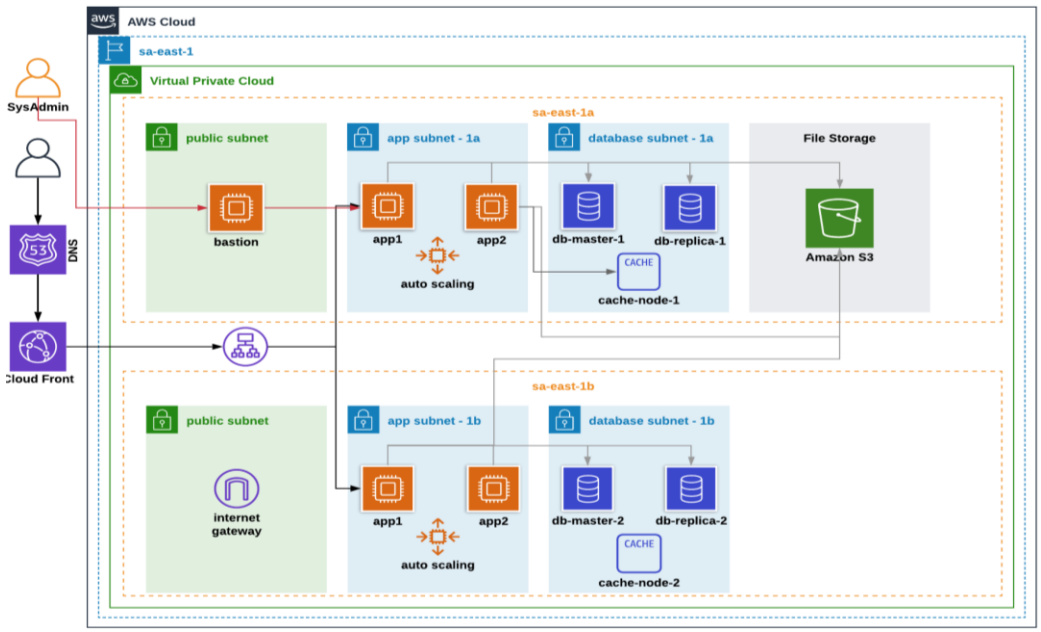
As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

CARGO	NOME	TELEFONE	E-MAIL
Membro do CGCRO	Jaimar Martins	(11) 99600-4501	jaimar.martins@spcgrafeno.com.br
Membro do CGCRO	Tiago Leocadio	(11) 95301-2868	tiago.leocadio@grafeno.digital
Membro do CGCRO	Nival Martins	(11) 98928-7646	nival.martins@spcbrasil.org.br
Membro do CGCRO	Marcelo Lopes	(11) 99962-0013	marcelo.lopes@spcgrafeno.com.br

ANEXO 3 – INFRAESTRUTURA DO AMBIENTE REGISTRADORA

A infraestrutura do ambiente completo onde é alocada aplicação da Registradora pode ser visualizada através do seguinte fluxo:



1. Alocação dos recursos, provedores e zonas de disponibilidade

Os data-centers que a SPC Grafeno utiliza são providos pela Amazon Web Services®, desta forma, todos os serviços que são necessários para manter a plataforma disponível, seja no site principal ou backup, são hospedados pela AWS (Programas da Conformidade da AWS).

Atualmente, a AWS conta com três zonas (data centers) de disponibilidade no Brasil, sendo elas no estado de São Paulo, com os mais avançados recursos na prestação de serviços data center

e infraestrutura cloud. Neste link AWS - Regions, Availability Zones, and Local Zones é possível acessar a documentação da AWS sobre o serviço de data center (em inglês), onde destacamos o seguinte trecho:

"Uma zona de disponibilidade (AZ) é um ou mais data centers distintos com rede energia, rede e conectividade redundantes em uma região da AWS. As zonas de disponibilidade permitem que você mantenha aplicações e bancos de dados de produção com maior disponibilidade, tolerância a falhas e escalabilidade do que seria possível em um único data center. Todas as zonas de disponibilidade em uma região da AWS são interconectadas com redes de alta largura de banda e baixa latência, através de fibra óptica totalmente redundante e dedicada, fornecendo redes de alta produtividade e baixa latência entre as zonas de disponibilidade. Todo o tráfego entre as zonas de disponibilidade é criptografado. O desempenho da rede é suficiente para realizar a replicação síncrona entre as zonas de disponibilidade. As zonas de disponibilidade facilitam a partição de aplicativos para alta disponibilidade. Se uma aplicação for distribuída nas zonas de disponibilidade, ela será melhor isolada e protegida de problemas como falta de energia, relâmpagos, tornados, terremotos e muito mais. As zonas de disponibilidade são fisicamente separadas por uma distância significativa de qualquer outra zona de disponibilidade, embora todas estejam a 100 km (60 milhas) uma da outra." (traduzido do inglês)

2. Distribuição dos recursos

As aplicações, dados e arquivos mantidos pela estrutura da Registradora são sempre segmentadas nas três zonas (data centers) disponíveis no Brasil. Os servidores de aplicação utilizam os três data centers, um produtivo e dois de contingência, dimensionados a assumir as demandas de produção em segundos, caso necessário.

Os bancos de dados utilizam dois data centers failover, sempre sincronizados, e backups diários são armazenados nos três data centers, o que permite a recuperação do serviço em até uma hora, no caso da hipótese remota de falha no banco de dados de produção e de contingência. Contamos ainda com outras estruturas de banco de dados em réplica para evitar gargalos de leitura no banco principal e que podem ser utilizadas em planos de contingência de desastres.

Pelo fato da replicação dos nós masters do banco de dados ser feita de forma automática e gerenciada pelo serviço da AWS em ambos data-centers, conseguimos garantir o mínimo de *Recovery Point Objective* no cenário de desastre no datacenter principal ou de falha no nó primário (não há perda de dados). Seguindo esse plano, o *Recovery Time Objective* se deve apenas a latência da rede e mudança de apontamento de DNS interno da resolução do serviço do banco, o é feito em poucos segundos (até 120 segundos).

A estrutura de cache de objetos é semelhante ao banco de dados principal.

3. Escala dos sistemas

Os servidores de aplicação são colocados atrás de balanceadores de carga, e quando necessário ou através de métricas de uso, sua capacidade pode ser aumentada de forma

horizontal, colocando mais servidores para atender as requisições em determinados endpoints da plataforma.

Já o banco de dados possui escala automática do storage conforme uso, e escala de recursos de CPU/Memória sendo feitos manualmente, de forma vertical.

A plataforma conta com constante monitoramento para readequação e alocação de novos recursos e incremento de capacidade computacional se for necessário.

4. Múltiplos Ambientes

A stack da plataforma conta com três ambientes semelhantes, que possuem a mesma arquitetura e podem assumir funções produtivas quando e se necessário.

Como a segmentação por zona de disponibilidade, seja para os servidores de aplicação ou banco de dados, facilita na operação e mitigação de problemas em um dos data-centers oferecidos, os ambientes não produtivos podem ser promovidos à produtivos se algum erro de aplicação ocorrer.

Por conceito e padrão, nenhuma alteração de código ou banco de dados é aplicada diretamente no ambiente produtivo sem antes passar pelos ambientes de desenvolvimento e homologação, de modo que testes automatizados e de comportamento sejam efetuados com o intuito de evitar que a plataforma seja prejudicada por deploys não conformes.

Os ambientes são isolados fisicamente, tanto no que tange a rede de comunicação quanto de banco de dados e aplicação, cada ambiente (stack) é devidamente replicado e reconfigurado quando necessário, de forma automatizada.

5. Proteção contra-ataques

Os load-balancers que respondem pelos endpoints da plataforma são protegidos por WAFs (Web Application Firewalls) que mitigam requisições maliciosas além de serem contemplados com a proteção do AWS Shield, que garante a disponibilidade mesmo em face de ataques DDoS mais conhecidos, dessa forma a plataforma não é afetada de forma direta, tanto a camada de aplicação quanto de banco de dados. No que tange a detecção de anomalias de rede, contamos com sistemas que verificam o tráfego gerado na rede interna e analisam possíveis tráfegos maliciosos.

6. *Disaster & Recovery*

Pelo fato de as aplicações serem *stateless*, em caso de perda de um dos nós que provêm acesso à plataforma, automaticamente outro nó será colocado de forma que possa responder às requisições do usuário final, com o mínimo de prejuízo possível, não gerando impacto na operação.

No que tange ao banco de dados, os backups são feitos diariamente e com período mínimo de retenção de 15 dias para ambientes produtivos e de 7 dias para ambientes de homologação. Ambientes de desenvolvimento tem o seu período de retenção diminuto e são constantemente atualizados baseados nos ambientes de homologação quando necessário.

6.1 Operação de contingência

Como possuímos toda a plataforma hospedada na AWS, temos a condição de utilizar outros ambientes como contingência para o ambiente produtivo. Se caso detectarmos que uma versão de software colocada no ambiente produtivo apresentou problemas ao usuário final, podemos promover a versão de homologação com alguns pequenos ajustes ou ainda fazer o deploy de uma nova stack de produção para que possa atender as requisições dos usuários.

No caso do banco de dados, temos monitoramento contínuo de uso computacional para que não haja prejuízo no uso da plataforma. a AWS nos garante contingência operacional do banco de dados principal em caso de falha com downtime de cerca de dois minutos entre a perda do nó principal e a recuperação do secundário em outras zonas de disponibilidade ou datacenter. No primeiro nível, possuímos a opção de restaurar o banco de dados em um momento anterior a cinco minutos da falha principal, recuperando o máximo de informação possível até o ponto de identificação da falha.

Em um segundo nível de backup/recovery, temos snapshots diários que podem ser recuperados a qualquer momento e em caso de falha total do serviço oferecido pela AWS (RDS), temos condição de restaurar o banco de dados através de um backup do dia anterior ou ainda podemos efetuar backup de arquivo recorrentes e recuperados em outro banco de dados ou máquina virtual.

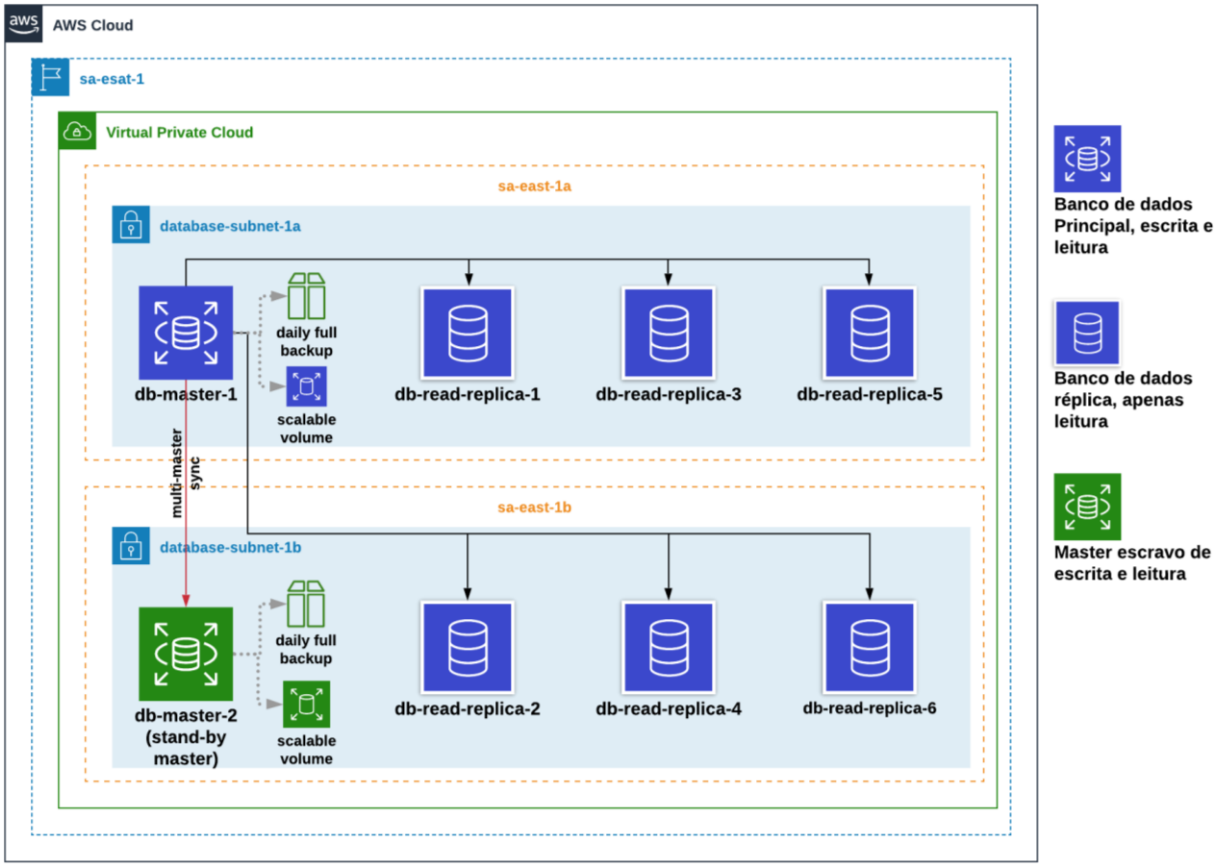
Este método requer mais tempo, porém é o terceiro nível de segurança/recovery disponível.

Atualmente, não há registros de desastres permanentes no serviço do RDS que tenha por consequência a total inoperabilidade de um servidor de banco de dados. Reiterando ainda, que tanto servidores de aplicação quanto de banco de dados não operam em apenas uma zona de disponibilidade, contando sempre com uma segunda zona de espera ou até mesmo de balanceamento e segregação de tráfego.

A estrutura de contingência e replicação do banco de dados pode ser encontrada no diagrama:

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública



7. Logs e Monitoramento

A Registradora conta com duas estruturas de monitoramento dos principais recursos computacionais utilizados como memória, CPU, tráfego de rede, uso de disco conexões do banco de dados, entre outras métricas importantes para operação da plataforma.

Uma delas sendo os painéis de monitoramento da própria AWS e a outra sendo os painéis de um servidor de coleta de métricas de operação e logs, configurado e gerenciado pela equipe da Grafeno.

Todas essas métricas são monitoradas e em caso de detecção de alguma anomalia, somos alertados de forma imediata através de e-mail ou no canal do grupo de comunicação instantânea da companhia.

Os principais logs dos servidores de aplicação e também do sistema operacional são salvos automaticamente na plataforma de gestão de logs da AWS. Os logs de banco de dados também são salvos, permitindo uma consulta posterior de forma organizada, executando filtros que nos possibilitam encontrar um possível problema de forma rápida e assertiva.

8. Serviços Essenciais

Todos a seguir possuem monitoramento ativo e alertas de forma que um eventual incidente possa ser identificado de forma pró-ativa, minimizando um eventual downtime e prejuízo na operação para o usuário final.

- Resolução DNS (Route53)
- Aplicação (Balanceadores de Carga inclusos)
- Banco de Dados
- Cache
- Storage de Objetos

ANEXO 4 – CONTINGÊNCIA DA INFRAESTRUTURA FÍSICA

O CGCRO é encarregado de declarar o estado de contingência física ao identificar incidentes que possam colocar em risco a integridade física dos colaboradores, fornecedores e parceiros comerciais da Companhia.

O plano de contingência será acionado de acordo com os parâmetros definidos neste Plano.

1. Evacuação da Sede

O CGCRO será responsável por coordenar uma situação em que seja necessário a desocupação da sede.

Procedimentos:

- Receber informação sobre o evento por meio de canais de notícias, segurança da Sede ou outro meio de comunicação.
- Verificar o local para avaliação primária.
- Realizar a contenção de perímetro, protegendo os colaboradores, terceiros e o patrimônio.
- Notificar a equipe de segurança da sede.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

- Acionar órgãos competentes.
- Solicitar reforço no quadro funcional,
- Avaliar o nível de segurança dos colaboradores.
- Manter as informações atualizadas.

2. Atendimento Ambulatorial

O CGCRO será responsável por coordenar uma situação em que seja necessário atendimento ambulatorial.

Procedimentos:

- Receber notificação do alarme de emergência, brigada de emergência ou da área de Gente e Cultura;
- Identificar os casos médicos gerados pela crise;
- Caso o atendimento no ambulatório da sede esteja impossibilitado ou seja necessário intervenções médicas, encaminhar para um dos seguintes hospitais:
    - Hospital e Pronto Socorro Itamaraty
        - Avenida Rebouças, 2274, Pinheiros
        - (11) 3674-7000
    - Hospital e Maternidade Jardins
        - Rua Artur de Azevedo, 1659, Pinheiros
        - (11) 3068-5888
- Avaliar a possibilidade de atendimento no ambiente interno da sede;
- Monitorar possíveis novos casos médicos;
- Comunicar aos contatos responsáveis dos colaboradores.

3. Distúrbios de Ordem Social

A equipe de Segurança Patrimonial da sede, sob monitoramento do CGCRO, será responsável por coordenar uma situação em que distúrbios de ordem social promovam risco à integridade de colaboradores, fornecedores e terceiros que possuam parceria comercial com a Companhia.

Procedimentos:

- Receber informação sobre a crise por meio de canais de notícias, segurança da sede ou outro meio de comunicação;
- Verificar o local para avaliação primária;
- Realizar a contenção de perímetro;

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública

- Acionar órgãos competentes conforme orientações do CGCRO;
- Solicitar reforço no quadro funcional, após obter anuência do CGCRO;
- Avaliar o nível de segurança dos colaboradores;
- Manter as informações atualizadas;
- Comunicar os membros do CGCRO.

4. Segurança Patrimonial

A equipe de Segurança Patrimonial da sede, sob o monitoramento do CGCRO, será responsável por coordenar uma situação de busca e apreensão por ordem judicial, arrombamento, furto ou roubo de grande porte nas instalações da sede.

Procedimentos:

- Receber notificação;
- Notificar a equipe de segurança da sede;
- Acionar órgãos competentes conforme orientações do CGCRO;
- Avaliar o nível de segurança patrimonial e propor ações corretivas ou preventivas;
- Comunicar os membros do CGCRO.

5. Manutenção

A equipe de Segurança Patrimonial da sede, sob o monitoramento do CGCRO, será responsável por coordenar uma situação de danos relativos à infraestrutura elétrica, hidráulica, mobiliário, limpeza e conservação.

Procedimentos:

- Receber notificação;
- Acionar órgãos e/ou serviços de execução de reparos;
- Avaliar o nível de segurança patrimonial;
- Propor ações corretivas e/ou preventivas;
- Comunicar os membros do CGCRO.

6. Meio de Comunicação Interna

O CGCRO comunicará, por e-mail, todos os funcionários da Companhia sobre a situação de contingência.

As informações contidas neste documento são de propriedade da SPC Grafeno Registradora S.A

#pública