SPC GRAFENO

# POLÍTICA DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

**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 objetivo deste documento (Política) é estabelecer diretrizes e práticas eficazes para a gestão e uso estratégico da tecnologia dentro da SPC Grafeno, visando garantir a integridade, segurança e disponibilidade dos dados, ao mesmo tempo em que promove a inovação contínua através de metodologias ágeis. A política busca otimizar recursos, melhorar processos e fomentar um ambiente que suporte o crescimento e a adaptação contínua às mudanças tecnológicas.

## 2. ABRANGÊNCIA

Esta Política de Tecnologia da Informação abrange todos os departamentos, unidades de negócios e colaboradores da Companhia, bem como os parceiros externos e fornecedores que interagem com os sistemas de tecnologia da informação da SPC Grafeno.

## 3. ALÇADAS DE APROVAÇÃO

- Área de Tecnologia da Informação – responsável pela elaboração e revisão da Política;
- Comitê de Riscos, Compliance e Segurança – responsável pela aprovação da Política;
- Conselho de Administração – responsável pela aprovação final desta Política.

## 4. DOCUMENTOS RELACIONADOS

- Política de Gerenciamento de Incidentes
- Política Segurança da Informação e Cibernética
- Política de Proteção de Logs e Trilhas de Auditoria
- Política de Continuidade de Negócios
- Política de Gerenciamento de Riscos e Controles
- Manual de Procedimentos Garantia de Qualidade de Software
- Manual Integrado de Segurança no Desenvolvimento e Operações
- Manual de Gestão de Mudanças
- Manual de Uso Aceitável de Recursos de Tecnologia
- Manual de Uso de Criptografia
- Plano de Continuidade de Negócios
- Plano de Recuperação de Desastres
- Plano Diretor de TI


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

#pública

## 5. DEFINIÇÕES GERAIS

- **Deploy**: Ato de lançar e instalar uma aplicação ou atualização em um ambiente de produção.
- **Design Thinking**: Metodologia centrada no usuário para resolver problemas complexos de forma criativa.
- **Dockerização e Kubernetes:** O Docker é uma plataforma que automatiza grande parte dos processos manuais necessários para implantar, gerenciar e escalar aplicações em containers e o Kubernetes é uma plataforma para executar e gerenciar contêineres em larga escala**.**
- **Downtime**: Período em que um sistema ou serviço está indisponível ou inoperante.
- **Health Check**: Verificação do estado e funcionamento de um sistema ou serviço.
- **MVP**: Minimum Viable Product, uma versão inicial de um produto com funcionalidades básicas para testar hipóteses de mercado.
- **Ping ou latência**: é um comando que serve para testar a conectividade entre equipamentos de uma rede utilizando o protocolo ICMP.
- **POD:** Um Pod do Kubernetes é um conjunto de um ou mais containers Linux®, sendo a menor unidade de uma aplicação Kubernetes. Os Pods são compostos por um container nos casos de uso mais comuns ou por vários containers fortemente acoplados em cenários mais avançados.
- **RDS:** Relational Database Service, um serviço gerenciado de banco de dados relacional na nuvem.
- **Rollback**: Processo de reverter um sistema ou aplicação para uma versão anterior.
- **RoR:** Ruby on Rails, um framework de desenvolvimento web escrito em Ruby que facilita a criação de aplicações web.

## 6. PAPÉIS E RESPONSABILIDADES

- **CTO (Chief Technology Officer ou Diretor de TI):** Organiza as frentes de trabalho para atender os objetivos estratégicos da SPC Grafeno, sendo responsável pelo orçamento da área de TI, entrega dos níveis de serviços, condução de projetos de manutenção e evolução de sistemas, monitoramento e manutenção da infraestrutura, ambiente seguro e gestão de fornecedores.
- **Área de Tecnologia da Informação:** A área de tecnologia da informação (TI) detém a responsabilidade sobre este documento, uma vez que é responsável pela gestão de serviços da Plataforma SPC Grafeno. Cabe à área de TI garantir a efetividade e atualização deste documento, bem como implementar as políticas e práticas descritas neste documento. Além disso, a área de TI deve assegurar que a equipe envolvida na gestão de serviços esteja devidamente capacitada para executar as atividades descritas neste documento, visando


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

#pública

garantir a qualidade, confiabilidade e segurança dos serviços prestados aos usuários da plataforma.

- **Sustentação:** Time que dá apoio aos chamados da Central de Suporte e realiza correções de bugs e eventuais melhorias de performance.
- **Desenvolvimento:** Equipes organizadas por grupos de serviços e responsáveis pela criação, manutenção e atendimento de incidentes relacionados à sistemas, serviços de TI e produtos oferecidos aos Participantes da Plataforma SPC Grafeno.
- **Infraestrutura:** Responsável pela administração e monitoramento dos ambientes computacionais internos e em cloud service, atendimento e resolução de incidentes envolvendo ambientes de desenvolvimento, homologação e produção, acompanhamento pró-ativo dos níveis de serviço, tomando as ações necessárias para garantir a capacidade e disponibilidade necessária para operação dos sistemas da SPC Grafeno, sempre pautado pelos SLAs previamente acordados.

## 7. DIRETRIZES

### 7.1. METODOLOGIA DE DESENVOLVIMENTO

A SPC Grafeno adota processos conhecidos como "ágeis" na gestão do portfólio de seus produtos e serviços e no desenvolvimento de sistemas.

Nosso modelo é de evoluções e ajustes nos serviços sendo implantados periodicamente, geralmente a cada 2 (duas) semanas, resultado de frentes de trabalho que chamamos de Sprint.

De forma geral, o *Sprint* é dividido em 3 (três) etapas:

1. ***Backlog:*** Antes de iniciar o *Sprint*, todas as demandas dos serviços do *Squad* são priorizadas, sejam elas melhorias ou incidentes, e são definidas quais serão desenvolvidas no próximo ciclo.

2. ***Sprint:*** Momento em que o time desenha, desenvolve e testa as demandas priorizadas.

3. **Serviço:** É entregue em produção uma melhoria ou correção de um serviço existente, ou até mesmo um novo serviço.

Todo este processo é registrado utilizando ferramenta de mercado com esta finalidade, permitindo a rastreabilidade das versões, serviços e sistemas impactados a cada fim de *Sprint*, assim como a verificação das comunicações entre a equipe e dos registros de decisões tomadas e que influenciaram na entrega, além disso, a documentação de validação e descrição de mudanças da versão são aqui documentadas, servindo como uma gestão de mudanças contínuas no fluxo de entrega.


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

#pública

As diretrizes para as avaliações de segurança em aplicações web dentro da Companhia, as quais são realizadas para identificar fraquezas potenciais ou percebidas como resultado de configuração incorreta, autenticação fraca, tratamento insuficiente de erros, vazamento de informações confidenciais, entre outros, estão descritas no **Manual Integrado de Segurança no Desenvolvimento e Operações** da SPC Grafeno.

## 7.2. ARQUITETURA E INFRAESTRUTURA

Visando maior segurança e escalabilidade de serviços, a arquitetura da SPC Grafeno foi estruturada para operação em nuvem, utilizando a tecnologia de Dockerização, Kubernetes e micro serviços. Esse modelo visa garantir a isonomia da aplicação, provendo uma arquitetura auto escalável de acordo com a demanda de cada serviço. Os serviços são separados em Pods, o que permite maior eficiência no dimensionamento de cada máquina, além de proteger o sistema contra indisponibilidades, uma vez que, caso haja um problema em um serviço específico, o mesmo só afeta o Pod do serviço e não a totalidade da aplicação.

A Infraestrutura Tecnológica da Companhia compreende o modelo em nuvem, que é uma solução altamente escalável, segura e flexível para a execução de aplicativos e armazenamento de dados em nuvem. Os serviços e recursos disponíveis oferecem ferramentas de segurança e conformidade, como criptografia de dados em repouso e em trânsito, autenticação multifator, firewalls de rede e gerenciamento de chaves de criptografia.

A infraestrutura deverá ser testada periodicamente quanto à sua resiliência e capacidade de recuperação, conforme a Política e Plano de Continuidade de Negócios e Plano de Recuperação de Desastres da Companhia.

**Redundância de rede:** O provedor de serviço em nuvem da SPC Grafeno, possui uma estrutura de redundância complexa e altamente disponível para garantir a continuidade dos serviços em caso de falhas ou interrupções. Existem vários níveis de redundância na arquitetura, desde a infraestrutura física até a aplicação em si. A infraestrutura física do provedor é composta por data centers em várias regiões geográficas, cada um com várias zonas de disponibilidade (AZs) independentes, separadas por uma distância significativa para garantir a resiliência. Cada AZ é composto por um ou mais data centers, cada um com sua própria fonte de energia, rede, sistema de refrigeração e hardware. Além disso, o provedor de serviço em nuvem usa uma técnica de replicação síncrona de dados que garante que os dados armazenados sejam copiados em tempo real para outras regiões geográficas (dentre as limitações contratadas e exigidas), garantindo a disponibilidade em caso de falha.

**Ambiente de contingência:** Visa criar mecanismos para diminuir o impacto da ocorrência de desastres: O provedor de infraestrutura e serviços em nuvem possui o recurso de múltiplas zonas no Brasil e o projeto já está configurado para, em caso de falha ou desastre em uma zona, a migração para outra zona disponível ocorrer, de forma automática. Para banco de dados, além de todos os outros itens citados, caso haja alto consumo no storage do banco, ele poderá escalar automaticamente.


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

#pública

A estrutura técnica denominada “CI/CD” (integração contínua e entrega contínua) de esteira de desenvolvimento, segrega os ambientes de desenvolvimento, homologação/staging e produção, de forma que sejam acessados por colaboradores distintos com acessos restritos para cada ambiente, garantido a segregação total de todos os serviços utilizados pela aplicação (gestão de usuários, banco de dados, infraestrutura de rede e gestão de código). Além da segregação técnica, existe uma segregação visual para garantir clareza aos usuários técnico e não técnico de qual ambiente está sendo utilizado.

- **Ambiente em Homologação/Staging**: a utilização de RDS com cache é uma estratégia comum para garantir alta disponibilidade e desempenho confiável em soluções da SPC Grafeno. O RDS pode ser configurado para funcionar em alta disponibilidade, o que significa que o serviço é executado em várias zonas de disponibilidade (AZs) para evitar pontos únicos de falhas. E o seu cache foi configurado para melhorar o desempenho do banco de dados. Este tipo de estratégia permite que os dados frequentemente acessados sejam armazenados na memória do servidor, o que pode reduzir o tempo de resposta do banco de dados e melhorar o desempenho da aplicação garantindo que seus dados estejam sempre disponíveis e acessíveis, mesmo em caso de falhas ou interrupções de serviço.

- **Ambiente de Desenvolvimento:**

  - **Código:** O sistema roda em um ambiente cloud nos moldes descritos acima e a aplicação é construída com a tecnologia Ruby on Rails (RoR). O RoR é um framework de desenvolvimento de aplicativos web em Ruby. Ele é projetado para facilitar o desenvolvimento de aplicativos web de alta qualidade e escaláveis, permitindo que os desenvolvedores se concentrem na lógica de negócios em vez de na infraestrutura subjacente. O RoR é baseado no padrão de arquitetura MVC (Model-View-Controller), que separa a lógica de negócios (Model), a apresentação de informações ao usuário (View) e o fluxo de controle da aplicação (Controller). Isso permite que os desenvolvedores criem aplicativos web de maneira mais organizada e estruturada. Além disso, o RoR é altamente modular e oferece muitas bibliotecas e plugins que podem ser adicionados aos aplicativos para aumentar sua funcionalidade. Isso torna o RoR uma escolha popular para o desenvolvimento de aplicativos web de alta qualidade e escaláveis.

  - **APIs:** conjunto de regras, protocolos e ferramentas que permitem que diferentes aplicativos se comuniquem e compartilhem informações entre si de maneira eficiente e escalável e são amplamente usadas no desenvolvimento de software. Possuímos endpoints para cada necessidade de registro do ativo, sendo o consumo e saída em formato JSON.

  - **Banco de dados:** Banco de dados relacional utilizando o PostgreSQL (servido pelo AWS RDS) e um banco de dados NoSQL utilizando o Redis (servido pelo AWS Elasticache). Sendo o primeiro transacional (dados dos participantes e registros dos ativos) e o segundo processamento assíncrono (agendamento de dados a serem processados e enfileiramento de rotinas).


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

#pública

## 7.3. PROCESSOS DE TESTES DE SOFTWARE

Os procedimentos aplicáveis para as atividades relacionadas a testes de Software, contemplando os processos de testes unitários, funcionais, performance, segurança e homologação, estão descritos no **Manual de Procedimentos de Garantia de Qualidade de Software**.

O processo de testes busca realizar as seguintes ações:

- Encontrar Defeitos no *Software*, permitindo a correção o quanto antes;
- Avaliar a qualidade do *Software* e das funcionalidades entregues;
- Comprovar que o *Software* foi desenvolvido conforme o projetado;
- Garantir que os requisitos foram implementados corretamente;
- Garantir a eficiência e segurança do *Software*.

**Testes funcionais:** Consiste em realizar testes manuais em uma versão de software que contenha as alterações solicitadas para o projeto. Nesse tipo de teste, o software é avaliado em relação às funcionalidades, requisitos e regras de negócios. Os testes funcionais são essenciais para garantir que o sistema atende às especificações e que todas as funcionalidades operam conforme o esperado.

**Testes de Homologação:** São realizados pelo PO ou PM, podendo ter a participação de empresas externas (reguladores ou órgãos externos), responsável pelo software a ser disponibilizado em ambiente de produção. O foco destes testes é garantir que o software funcione de acordo com os critérios de aceitação definidos para o projeto.

**Testes de Performance:** São aplicados quando é necessário avaliar a eficiência da aplicação e disponibilizar informações para que sejam tomadas ações corretivas em relação aos problemas de desempenho do sistema.

**Testes de Segurança:** São aplicados para avaliar se existem brechas, vulnerabilidades, ameaças e riscos que podem gerar perdas de dados para a SPC Grafeno. Como parte da estratégia contínua de gestão de vulnerabilidades, os scans de segurança são realizados mensalmente, com foco em conjuntos distinto de ativo a cada ciclo. Essa abordagem permite uma cobertura mais ampla e eficiente da infraestrutura de TI, distribuindo a análise ao longo do tempo sem sobrecarregar os sistemas ou as equipes responsáveis. No mínimo anualmente, são realizados testes de penetração (Pentest), conforme cronograma da área de SI/Cyber.

**Testes com Órgãos Reguladores:** Tem a finalidade de orientar sobre todas as etapas que precisam ser cumpridas para a SPC Grafeno estar preparada para a homologação (testes funcionais) dos nossos sistemas com os órgãos reguladores, como por exemplo, o Banco Central do Brasil.


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

#pública

## 7.4. GESTÃO DE MUDANÇAS

O principal objetivo do processo de Gestão de Mudanças é assegurar que todas as alterações no ambiente de TI sejam realizadas de forma controlada e coordenada, minimizando os riscos de interrupções nos serviços e garantindo a continuidade das operações. Este processo visa identificar, avaliar e autorizar mudanças, garantindo que elas sejam implementadas com eficiência e eficácia, e que qualquer impacto negativo seja mitigado. A gestão adequada de mudanças contribui para a estabilidade e a confiabilidade dos sistemas de TI, promovendo um ambiente tecnológico seguro e resiliente.

O procedimento detalhado para a Gestão de Mudanças está descrito no **Manual de Gestão de Mudanças da SPC Grafeno**, que define as etapas, responsabilidades e critérios de aprovação de mudanças. Este manual estabelece diretrizes claras para a solicitação, avaliação, aprovação e implementação de mudanças, incluindo a comunicação adequada aos stakeholders e a documentação completa de cada alteração. Além disso, o manual descreve os mecanismos de monitoramento e revisão pós-implementação para assegurar que os objetivos da mudança foram alcançados e para identificar oportunidades de melhoria contínua no processo.

De forma objetiva, em toda mudança na infraestrutura que por algum motivo possa gerar um incidente e consequentemente um *downtime* na operação para o usuário final, é extremamente necessário a gestão das mudanças que serão implementadas. Sejam elas de cunho preventivo, corretivo ou de melhoria sistêmica.

As GMUDs podem ser gerenciadas por *software* de mercado ou por documentos assinados e validados pelas pessoas responsáveis ou que interagem no processo.

De forma resumida, uma GMUD precisa ter:

- A data prevista para operação;
- A razão da operação (correção, melhoria, manutenção de rotina);
- A janela de tempo necessária para tal procedimento;
- O risco (alto, médio, baixo) da operação. Ex.: mudança de regra de firewall vs migração de banco de dados;
- O procedimento de rollback contemplando os passos necessários, caso a ação principal falhe: execução de restauração de backup, scripts etc.;
- Os responsáveis pela operação;
- O revisor;
- O solicitante.

Em caso de falha no procedimento de rollback, devemos iniciar o procedimento de gestão de incidentes de TI definido pelo item 7.9 desta Política.


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

#pública

## 7.5. IMPLEMENTAÇÃO EM PRODUÇÃO

Sempre que forem necessárias novas funcionalidades ou correções de defeitos, a demanda irá ser registrada no Jira pelo responsável do Produto, a demanda pode ser iniciada tanto por impacto a clientes, por adequação a novas resoluções divulgadas pelos Órgãos Reguladores e novas leis ou funcionalidades que irão facilitar a utilização da plataforma pelo cliente.

No que tange a gestão de mudanças no fluxo de *deploy*, implementamos o conceito de *blue-green deployment*, possibilitando mais agilidade, porém sem perder a rastreabilidade, logs e a possibilidade de *rollback* em caso de falhas na implementação de novas versões da aplicação.

O fluxo do *deploy* no ambiente de produção envolve primariamente o *deploy* no ambiente de homologação, com o intuito de detectar possíveis problemas de software, arquitetura ou infraestrutura sem que gere prejuízo à plataforma em ambiente produtivo.

Etapas:

- Desenvolvimento (Code review, pair programming);
- Testes Integrados;
- Geração de imagem para ser colocado em produção;
- *Health Checks* que validam se a nova versão do servidor está de acordo com o esperado;
- Transbordo de conexões do servidor antigo (blue) para o novo (green);
- Após a estabilização do novo servidor, o antigo é automaticamente deletado;
- Em caso de detecção de falhas no momento do transbordo de conexões, é possível fazer o rollback para o estado anterior.

## 7.6. MONITORAMENTO DE SERVIÇOS

O monitoramento de serviços de TI é essencial para garantir a disponibilidade contínua e a operação eficiente dos serviços críticos, em especial o serviço de Registro de Ativos Financeiros. O objetivo principal deste monitoramento é assegurar que o sistema esteja sempre disponível para os participantes, permitindo o registro, a consulta e a gestão dos ativos financeiros de maneira confiável e segura. A manutenção da disponibilidade do serviço é vital para a integridade do mercado financeiro e para a confiança dos participantes no sistema.

Para alcançar esses objetivos, a SPC Grafeno adota um conjunto de ferramentas e práticas de monitoramento que cobrem todos os aspectos do serviço de Registro de Ativos Financeiros. Isso inclui a supervisão em tempo real dos componentes de hardware e software, o acompanhamento dos indicadores chave de desempenho (KPIs) e a detecção proativa de falhas ou anomalias que possam comprometer a disponibilidade do serviço. O monitoramento contínuo permite identificar e resolver problemas antes que eles afetem os usuários finais, garantindo assim a continuidade das operações.


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

#pública

Além disso, o monitoramento de serviços é complementado pelo processo de resposta a incidentes, que garantem uma reação rápida e eficaz a qualquer interrupção ou degradação do serviço. As equipes de TI são treinadas para seguir procedimentos de escalonamento e resolução, minimizando o tempo de inatividade e restaurando a funcionalidade normal o mais rápido possível. A Companhia também realiza revisões regulares do desempenho do serviço e implementa melhorias contínuas baseadas nas análises de dados de monitoramento, assegurando que o serviço de Registro de Ativos Financeiros esteja sempre alinhado com as necessidades dos participantes e as melhores práticas do setor.

Os principais KPIs monitorados são:

- Disponibilidade e saúde da aplicação: são monitoradas as requisições por segundo, latência e erros;
- Recursos: se estão operando de forma saudável, se estão estáveis e estão suportando devidamente às requisições;
- Logs da aplicação, infraestrutura e usuários;
- Endpoints de parceiros-chave da aplicação;
- Custos de infraestrutura.

### 7.6.1. Centro de Operações de Segurança (SOC)

O Centro de Operações de Segurança (SOC) desempenha um papel essencial no monitoramento contínuo das plataformas de segurança da informação da Companhia.

O monitoramento realizado pelo SOC abrange eventos suspeitos e comportamentos anômalos, garantindo uma vigilância constante sobre redes, sistemas e aplicações. A identificação e análise de vulnerabilidades cibernéticas são conduzidas com base em varreduras periódicas e análises técnicas, tais como Pentest (no mínimo anual) e Scan Mensal, conforme citado no capítulo: 7.3. desta Política.

**Escopo e Responsabilidades**

O serviço contratado com o SOC é de primeiro nível (N1), o que significa que sua atuação está focada nas seguintes atividades:

- Monitoramento 24x7 de alertas e eventos de segurança;
- Análise inicial e triagem dos eventos com base em regras pré-definidas;
- Classificação e priorização dos eventos conforme criticidade;
- Abertura de tickets e encaminhamento para os responsáveis da SPC Grafeno;
- Criação de Casos de Uso e Playbooks Sob Demanda, conforme necessidade da área de Segurança;
- Geração de relatórios e dashboards com indicadores de segurança.

**Escalonamento de Incidentes**


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

#pública

- Telefone (24x7): Para incidentes críticos que exigem resposta imediata;
- E-mail: Para incidentes de média/baixa criticidade ou atualizações.

O SOC de N1 não realiza investigações profundas nem correções técnicas diretas, mas garante a detecção precoce de ameaças e a resposta rápida a incidentes, funcionando como a primeira linha de defesa da Companhia.

## 7.7. ANÁLISE DE CAPACIDADE, EXPANSÃO E PERFORMANCE DE TI

O processo de análise de capacidade, expansão e performance de TI é fundamental para garantir que a infraestrutura tecnológica da Companhia suporte de maneira eficaz o crescimento e as demandas variáveis dos serviços, especialmente o serviço crítico de Registro de Ativos Financeiros.

A análise de capacidade envolve a avaliação contínua dos recursos de TI, como servidores, armazenamento, rede e sistemas, para assegurar que eles atendam às necessidades operacionais atuais e futuras. Isso inclui a identificação de possíveis gargalos, a previsão de necessidades de recursos e a implementação de medidas preventivas para evitar a sobrecarga do sistema.

A expansão e a performance de TI são gerenciadas através de um processo estruturado que inclui planejamento, monitoramento e otimização contínua. A expansão é planejada com base nas análises de capacidade e nas projeções de crescimento, garantindo que os recursos de TI possam ser escalados de forma eficiente e econômica.

A performance é monitorada continuamente, utilizando ferramentas avançadas de análise e relatórios, para identificar áreas de melhoria e otimizar o desempenho dos sistemas. Este processo assegura que a empresa possa manter a alta disponibilidade e a performance ideal do serviço de Registro de Ativos Financeiros, atendendo às expectativas dos participantes e cumprindo os requisitos regulatórios.

## 7.8. ATENDIMENTO A USUÁRIOS

Os acessos dos usuários aos sistemas da SPC Grafeno acontecem através de abertura de chamados na plataforma de abertura de chamados (Service Desk). Após a recepção do chamado, a área de Service Desk verifica se a solicitação de acesso é para um sistema de acesso restrito, caso positivo, solicita-se a aprovação do gestor responsável do usuário solicitante.

O processo de atendimento do Service Desk para a concessão de acesso aos usuários internos dos sistemas da SPC Grafeno, define como 3 (três) horas para a resposta inicial e 3 (três) dias para a solução total do atendimento.


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

#pública

## 7.9. RESPOSTA A INCIDENTES

Todos os incidentes do ambiente de produção devem ser registrados no Portal de Incidentes, conforme descrito na **Política de Gerenciamento de Incidentes.**

A partir de uma triagem a equipe de Sustentação avalia a solicitação e toma as seguintes ações:

- Impedimento para a utilização do serviço, não tem contingência e precisa de solução imediata;
- Impedimento para a utilização do serviço, mas tem solução de contorno satisfatória;
- Ocorrência de lentidão ou intermitência do ambiente de produção;
- Ocorrência de falhas e/ou bugs internos de fácil resolução sem a necessidade de contingência.

### 7.9.1. Monitoramento Técnico

A metodologia utilizada para gestão de controle de tecnologia e infraestrutura consiste em priorizar o monitoramento dos sistemas da SPC Grafeno e de seus fornecedores, com o apoio de ferramentas, de modo a detectar alertas de possíveis incidentes antes mesmo que venham a impactar o funcionamento normal, possibilitando ações preventivas e proativas, de modo a garantir os SLAs regulatórios compromissados com os clientes.

A equipe de Tecnologia da Informação, por meio de sistema para coleta de logs da aplicação e checagem do ambiente, monitora os recursos e a aplicação para assegurar que ambos estão performando de acordo com os SLAs esperados para a operação. Caso algum item passe a operar de maneira inesperada, são enviados alertas com condições específicas, tais como quantidade de erros e latência.

### 7.9.2. Fluxo Operacional

- Através do Monitoramento Técnico realizado pelas áreas de Tecnologia da Informação, da comunicação do cliente/participante sobre a dificuldade encontrada na plataforma ou alguma inconsistência em suas operações, das verificações e monitoramentos de Segurança da Informação e Cyber, bem como outras comunicações de incidentes identificados pelas áreas internas da Companhia, realiza-se o registro através de ferramenta interna de registro de incidentes;

- Para qualquer tipo de incidente registrado, a equipe de Sustentação realiza a triagem da comunicação realizada, verificando o impacto ao negócio e tratativas de solução;

- Se o incidente tiver impacto em um processo crítico da Companhia, impossibilitando a operação pelos clientes / participantes ou pela área de Operações, com a previsão de contorno superior a 2 (duas) horas, o Comitê de Gerenciamento de Crises e Risco Operacional deve ser acionado;


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

#pública

- O CGCRO quando acionado, avaliará o impacto e decidirá sobre a ativação do Estado de Contingência, conforme descrito no Plano de Continuidade de Negócios Corporativo;
- Após o tratamento do incidente, a área de Tecnologia atualiza o registro informando a causa raiz, o plano de contenção de incidente e através da revisão de lições aprendidas, estabelece em conjunto com as equipes de resposta a incidentes, os planos de ação estruturais para evitar recorrência.

O objetivo da tabela abaixo é fornecer 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, e ajuda a priorizar recursos e ações para minimizar a interrupção das operações e atender aos níveis de serviço estabelecidos.

| Estimativa de tempo de Interrupção e Recuperação | Grau de Gravidade | Classificação |
|---|---|---|
| Menos de 1 hora | Baixo | Incidente |
| 1 a 2 horas | Moderado | Incidente |
| 2 a 4 horas | Alto | **Crise** |
| Mais de 4 horas | Crítico | **Crise** |

**Tabela de Classificação de Incidentes**

- **Grau de Gravidade:**
  - **Baixo:** Impacto mínimo nas operações, sem afetar a funcionalidade essencial ou a conformidade regulatória.
  - **Moderado:** Impacto limitado, pode afetar parcialmente as operações, mas dentro do SLA regulatório.
  - **Alto:** Impacto significativo nas operações, pode levar a violações do SLA regulatório.
  - **Crítico:** Impacto severo e abrangente, comprometendo operações e conformidade regulatória de forma grave.
- **Classificação:**
  - **Incidente:** Problemas que podem ser resolvidos rapidamente com impacto limitado nas operações.
  - **Crise:** Problemas graves que exigem uma resposta imediata e coordenada para mitigar impactos severos nas operações e conformidade regulatória, incluindo o acionamento do Comitê de Gerenciamento de Crises e Risco Operacional.


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

#pública

## 7.10. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

O objetivo do **Plano de Recuperação de Desastres (PRD)** da Companhia é garantir a continuidade dos serviços críticos e a rápida recuperação das operações em caso de eventos adversos que possam causar interrupções significativas. Este plano abrange estratégias e procedimentos detalhados para responder a diversos tipos de desastres, desde falhas técnicas até desastres naturais, garantindo que o serviço de Registro de Ativos Financeiros continue a operar ou seja rapidamente restaurado para minimizar impactos negativos aos participantes.

O PRD inclui uma análise abrangente de riscos e vulnerabilidades, identificando os principais ativos e sistemas críticos que precisam ser protegidos. Procedimentos específicos são descritos para a preparação e resposta a incidentes, incluindo a ativação do plano, comunicação com stakeholders, e coordenação das equipes de resposta. O plano também detalha os recursos necessários para a recuperação, como backups de dados, sistemas redundantes, e locais alternativos de operação, assegurando que a empresa esteja pronta para enfrentar qualquer contingência com eficácia.

Além disso, o PRD define procedimentos para testes e simulações regulares, a fim de validar a eficácia do plano e treinar as equipes envolvidas. Esses testes permitem identificar e corrigir possíveis falhas no plano, garantindo que todos os membros da organização estejam familiarizados com suas responsabilidades e ações em caso de desastre. A Companhia realiza revisões periódicas do PRD para incorporar novas ameaças e mudanças no ambiente de TI, assegurando que o plano permaneça atualizado e alinhado com as melhores práticas do setor e as exigências regulatórias.

## 7.11. GESTÃO DE DADOS E INOVAÇÃO

### 7.11.1. Gestão de Dados

A Diretoria de Tecnologia, Dados e Inovação adota a abordagem abrangente para a gestão de dados, buscando assegurar que todas as informações da Companhia sejam tratadas como recursos estratégicos. Isso inclui a definição de papéis, responsabilidades e processos claros para a coleta, armazenamento, processamento e uso dos dados. A gestão eficaz de dados deve abranger a proteção da privacidade dos dados pessoais, alinhada às regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil. Adicionalmente, a qualidade e a integridade dos dados devem ser mantidas através de processos rigorosos de validação e correção, garantindo que todas as informações sejam precisas, completas e confiáveis.

O gerenciamento deste processo busca oferecer uma estrutura abrangente para a governança de dados, cobrindo áreas como arquitetura de dados, modelagem de dados, qualidade de dados, segurança de dados e gestão de metadados, alinhando a estratégia de dados aos objetivos de negócios e estabelecendo métricas de desempenho para monitorar a eficácia da governança.


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

#pública

### 7.11.2. Inovação

A Diretoria de Tecnologia, Dados e Inovação promove um ambiente que incentiva a criatividade e a experimentação, adotando práticas ágeis e metodologias de *design thinking* para impulsionar o desenvolvimento de soluções inovadoras. A inovação é tratada como um processo contínuo, integrado à estratégia corporativa, permitindo a identificação e exploração de novas tecnologias e tendências de mercado. A gestão de inovação coloca o usuário no centro do processo de desenvolvimento, promovendo uma abordagem iterativa de prototipagem e teste para soluções criativas.

Para testar rapidamente hipóteses de mercado e ajustar as estratégias, a gestão de inovação enfatiza a construção de produtos mínimos viáveis (MVPs) para testar rapidamente hipóteses de mercado e ajustar as estratégias com base no feedback dos usuários, permitindo uma adaptação ágil e eficiente às mudanças e demandas dos clientes.

## 7.12. TREINAMENTO E CAPACITAÇÃO

A Diretoria de Tecnologia, Dados e Inovação deve garantir que todas as equipes internas de TI possuam as habilidades e conhecimentos necessários para desempenhar suas funções de maneira eficaz e segura, bem como assegurar que os colaboradores estejam preparados para manter a continuidade dos serviços críticos, como o Registro de Ativos Financeiros.

Os programas de capacitação devem ser adaptados às necessidades específicas de cada equipe e função dentro da TI, garantindo que todos os colaboradores recebam a formação adequada às suas responsabilidades. A Diretoria também promove uma cultura de aprendizado colaborativo, incentivando o compartilhamento de conhecimento e experiências entre as equipes internas de TI, o que fortalece a capacidade geral da organização de lidar com desafios e inovar continuamente.

# 8. DISPOSIÇÕES GERAIS

## 8.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

## 8.2. CASOS OMISSOS

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

## 8.3. DIVISIBILIDADE

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


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

#pública

## 8.4. DIVULGAÇÃO E COMUNICAÇÃO

A Companhia promoverá a divulgação e comunicação contínuas das políticas para todos os funcionários, diretores, membros do conselho e demais partes interessadas e quando aplicável, publicadas no website da Companhia.

## 9. REVISÃO DA POLÍTICA

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

## 10. VIOLAÇÕES

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

## 11. CONTROLE DE VERSÕES

| Versão | Data | Responsável | Ocorrência |
|---|---|---|---|
| 1.0 | 30/07/2024 | Área de Tecnologia da Informação | Elaboração do documento (em substituição ao documento “Manual de Governança de Serviços de TI” |
| 1.0 | 27/08/2024 | Comitê de Riscos, Compliance e SI | Revisão e Aprovação do documento. |
| 1.0 | 03/10/2024 | Conselho de Administração | Aprovação final do documento |
| 2.0 | 14/07/2025 | Áreas de Riscos e Segurança da Informação | Revisão do documento:<br>Item 7.2 – Reforço na necessidade de testes da infraestrutura;<br>Item 7.3 – Ajuste no texto sobre os testes de segurança;<br>Item 7.6 – Melhor descrição sobre a atuação do SOC 24x7. |
| 2.0 | 08/08/2025 | Diretoria de Tecnologia, Dados e Inovação | Revisão do documento |
| 2.0 | 13/08/2025 | Comitê de Riscos, Compliance e SI | Revisão e aprovação do documento |
| 2.0 | 13/08/2025 | Conselho de Administração | Aprovação final do documento. |

***



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

#pública