

---

---

**PLANO DE CONTINUIDADE DOS NEGÓCIOS**

**DA**

**SCAI GESTORA DE RECURSOS LTDA.**

\_\_\_\_\_

**28 DE SETEMBRO DE 2022**

\_\_\_\_\_

---

---

## ÍNDICE GERAL

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>3</b>
<b>2</b>	<b>COMPLIANCE .....</b>	<b>3</b>
<b>3</b>	<b>PLANOS DE CONTINGÊNCIA .....</b>	<b>4</b>
<b>4</b>	<b>ATUALIZAÇÃO E REVISÃO .....</b>	<b>6</b>
	<b>ANEXO I – MODELO DE TERMO DE COMPROMISSO.....</b>	<b>7</b>

## 1 INTRODUÇÃO

Esta Política descreve os planos de contingência implantados na SCAI Gestora de Recursos Ltda. (“SCAI”) para responder com rapidez a um evento que possa impossibilitar a continuidade dos negócios da empresa. Estes planos indicam como a SCAI responderá a um evento de forma a garantir que as funções críticas do negócio retornem a um nível de operação aceitável dentro de um prazo desejável.

Esta Política também indica as principais responsabilidades da área de *Compliance* da SCAI bem como a disposição de sua infraestrutura.

A SCAI mantém um conjunto de procedimentos alternativos a serem adotados pelas áreas de suporte técnico quando da inoperância de um recurso técnico (sistemas, comunicações, componentes etc.), objetivando a sua recuperação após o evento. A SCAI também estabeleceu um conjunto de cenários de inoperância previamente definidos e respectivos procedimentos, destinados a manter a continuidade dos processos e/ou serviços.

As instruções aqui expostas devem ser observadas pelos sócios, diretores, empregados, funcionários, *trainees* e estagiários da SCAI (conjuntamente referidos como "Colaboradores", e individual e indistintamente como "Colaborador")

## 2 COMPLIANCE

As principais funções desempenhadas pela área de *Compliance*, cujo diretor responsável é o Diretor de *Compliance* (“Diretor de Compliance”), são:

- (i) fiscalizar o tratamento dado a informações privilegiadas;
- (ii) realizar o controle de arquivos físicos e eletrônicos;
- (iii) impor restrições na negociação de valores mobiliários com o uso de informações privilegiadas;
- (iv) impor restrições na divulgação de informações privilegiadas, opiniões e recomendações;
- (v) garantir a divulgação, educação e treinamento de Colaboradores;
- (vi) garantir que política de combate e prevenção à lavagem de dinheiro seja observada; e
- (vii) aplicar sanções ao descumprimento das políticas e procedimentos regulados pelo Manual de *Compliance* da SCAI.

### 3 PLANOS DE CONTINGÊNCIA

#### 3.1 Infraestrutura e Tecnologia da Informação

A área de Tecnologia da Informação (“TI”) da SCAI está sob responsabilidade de sua equipe de tecnologia da informação, sob supervisão do Diretor de *Compliance*. Todas as normas de segurança estão formalizadas na Política de Segurança da Informação.

#### 3.2 Data Center

Data Center, ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e sistemas de ativos de rede (“Data Center”).

O Data Center principal está localizado na Rua Voluntários da Pátria, 360, Botafogo - Rio de Janeiro, o secundário, por sua vez, situa-se na Avenida Rio Branco, 1, sala 2009 – Rio de Janeiro, o terceiro localiza-se na própria empresa e possui acesso restrito (“Data Center”). Os Data Centers podem ser acessados por Diretores, Profissionais da TI orgânica e Colaboradores contratados do próprio Data Center. Os Data Centers também poderão ser acessados pela equipe de TI, para fins de manutenção.

#### 3.3 Back Up e Restore de Arquivos

A SCAI dispõe de 5 tipos de *backups* para suprir a falha do servidor:

- (i) *Backup* diário das informações em fita (unidade LTO) hospedado nos Data Centers da empresa, onde o acesso é restrito;
- (ii) *Backup* dos logs dos bancos de dados em períodos de hora em hora em disco;
- (iii) Replicação de dados entre os discos através de Raid em todos os servidores;
- (iv) Replicação de máquinas virtuais entre ambientes clusterizados; e
- (v) Replicação de banco de dados para o Data Center redundante.

#### 3.4 Disaster Recovery e “Site Espelho”

Em caso de indisponibilidade do Data Center Primário, contamos com um Data Center Redundante na SCAI, onde os dados do nosso ERP, JDEdwards são replicados para a AMT - Agência Moderna Tecnologia Ltda, situada à Rio Branco nº 1, Centro, Rio de Janeiro – RJ. Está previsto no contrato de serviços que a AMT fornecerá outros servidores sob demanda em caso de impossibilidade de usar o Data Center Principal. Todos os integrantes da SCAI possuem

computadores com acesso à internet podendo acessar o *web-mail* da SCAI e celulares disponibilizados pela empresa para comunicação.

### **3.5 Internet, Email, Dados e Telefonia**

A SCAI possui 2 *links* redundantes de internet que, somados, possuem uma capacidade total de 200MB de fornecedores distintos. Todos os links são providos por um firewall ativo e passivo que, além de protegerem o perímetro, fazem o *load balance* entre os *links* com o objetivo de garantir disponibilidade de *performance*. O *firewall* em questão segregava ambientes que disponibilizam internet pública para visitantes daqueles ambientes privados para colaboradores, nos quais a rede é integrada com o Active Directory.

Ainda, a SCAI utiliza o serviço da Google, denominado Google for Workspace, o qual garante a disponibilidade de 99,99% e conta com o seu serviço de Archive por 10 anos. Os usuários têm acesso a essas informações no navegador Web.

O serviço de telefonia não possui *backup*, sendo que, havendo falha, serão utilizados os celulares da SCAI.

Os computadores da SCAI são *notebooks*, e, portanto, não necessitam de *No Breaks*.

A SCAI também possui notebooks com capacidade total de operação, acesso remoto ao servidor e, ainda, internet via celular.

### **3.6 Testes de Segurança e Integridade do Sistema**

O sistema é frequentemente testado pela provedora, sendo garantido o suporte 24 horas por dia. Nos termos do que dispõe o Plano de Continuidade de Negócios, o sistema de antivírus dos servidores e estações de trabalho é gerenciado pela equipe interna de infraestrutura e auxiliados por um suporte de 3º nível do fabricante. Ainda, os equipamentos são monitorados diariamente para verificações de atualizações automáticas e monitoramento de pragas. Nossos back ups são armazenados por um prazo superior aos cinco anos exigidos pela CVM, sendo feitos para durarem o maior tempo possível. O responsável pela ativação do plano de continuidade é o Gerente de infraestrutura na empresa Ancar Ivanhoe Shopping Centers. Os nossos testes de continuidade são realizados com frequência pela Ancar Ivanhoe e são armazenados em um relatório.

#### **4 ATUALIZAÇÃO E REVISÃO**

Este plano deve ser revisado na ocorrência de alterações materiais nas atividades, infraestrutura ou operações da SCAI. Entretanto, uma revisão mínima deve ocorrer a cada 2 (dois) anos, ou em período inferior, se houver alterações regulatórias e autorregulatórias, com o intuito de verificar a eventual necessidade de produzir uma versão atualizada, a ser aprovada pela Diretoria da SCAI.

#### **5 ACESSO AO PLANO DE CONTINUIDADE DOS NEGÓCIOS**

Uma cópia do Plano de Continuidade dos Negócios deve ser entregue a cada Colaborador da SCAI quando da sua contratação, nos termos do Modelo de Termo de Compromisso constante do Anexo I. A cada atualização do plano, uma nova versão deve ser encaminhada para todos. Cada Colaborador deve armazenar uma cópia atualizada desse documento fora das dependências da SCAI (residência ou veículo, por exemplo). Uma versão eletrônica atualizada do documento é disponibilizada no diretório da rede da SCAI.

**ANEXO I – MODELO DE TERMO DE COMPROMISSO**

**TERMO DE ADESÃO À POLÍTICA DE CONTINUIDADE DOS NEGÓCIOS  
DA SCAI GESTORA DE RECURSOS LTDA.**

Eu, [nome], [qualificação], declaro que tomei conhecimento dos termos e condições da Política de Continuidade dos Negócios da SCAI Gestora de Recursos Ltda. (“Política” e “SCAI”), por meio de treinamento realizado em [●] de [●] de [●] na sede da SCAI, tendo, ao final, recebido uma cópia da Política.

Subscrevendo o presente formalizo a minha adesão à presente Política, comprometendo-me a cumprir com todos os seus termos e condições, adotando, nas situações de dúvida, a posição mais conservadora possível, submetendo as dúvidas a respeito do cumprimento da Política e da legislação e regulamentação em vigor ao Diretor de *Compliance*.

Rio de Janeiro, [●] de [●] de [●].

---

[●]

Testemunhas:

1. \_\_\_\_\_

Nome:

RG:

CPF:

2. \_\_\_\_\_

Nome:

RG:

CPF: