# PLANO DE CONTINUIDADE DE NEGÓCIOS E CONTINGÊNCIA

**SECURITY ADMINISTRADORA DE RECURSOS LTDA.**

**Rio de Janeiro/RJ**

**Maio de 2026**

# PLANO DE CONTINUIDADE DE NEGÓCIOS E CONTINGÊNCIA

## 1. INTRODUÇÃO E OBJETIVOS

1.1. O presente Plano de Continuidade de Negócios e Contingência (“PCN”) tem por finalidade estabelecer, consolidar e descrever as diretrizes, procedimentos e medidas que deverão ser adotados para assegurar a continuidade das atividades da SECURITY ADMINISTRADORA DE RECURSOS Ltda. diante da ocorrência de eventos adversos, tais como falhas operacionais, atos de vandalismo, acidentes, desastres naturais ou quaisquer outros distúrbios que possam comprometer suas instalações físicas, sistemas, infraestrutura tecnológica ou a possibilidade de utilização destes por período superior a 24 (vinte e quatro) horas consecutivas.

1.2. O PCN busca garantir que, mesmo em situações de contingência, a SECURITY mantenha sua capacidade operacional mínima necessária para a continuidade de seus fluxos de negócios, o cumprimento tempestivo das obrigações regulatórias e legais, o envio de informações aos órgãos competentes, bem como a adequada execução das liquidações financeiras relacionadas aos fundos de investimento sob sua gestão, mitigando impactos operacionais, financeiros, reputacionais e regulatórios decorrentes de eventuais interrupções.

1.3. A SECURITY entende que a implementação parcial das medidas previstas neste Plano poderá ser necessária em situações de contingência de menor duração, especialmente em eventos que comprometam a capacidade operacional regular da companhia por período superior a 4 (quatro) horas consecutivas e inferior a 24 (vinte e quatro) horas. Nessas hipóteses, os impactos operacionais são administrados no curso ordinário dos negócios, mediante a adoção de procedimentos alternativos e mecanismos de contingência previamente estabelecidos, incluindo, mas não se limitando, à utilização de dispositivos móveis, acesso remoto aos sistemas corporativos e envio de instruções operacionais em modo contingencial.

1.4. Dentro dessas premissas, o presente Plano descreve os procedimentos, responsabilidades e medidas que deverão ser observados pelos colaboradores da SECURITY em caso de ocorrência de eventos que demandem sua ativação, total ou parcial, com o objetivo de assegurar a continuidade das operações essenciais da companhia e minimizar eventuais impactos operacionais, regulatórios e financeiros.

1.5. A responsabilidade pela estruturação, atualização, coordenação e ativação deste Plano caberá ao Diretor de Risco e Compliance, que deverá avaliar a gravidade do evento ocorrido, determinar as medidas contingenciais aplicáveis e acompanhar a execução dos procedimentos necessários até o restabelecimento integral das atividades da SECURITY.

## 2. ESCOPO E DISSEMINAÇÃO DO PLANO

2.1. Todos os Colaboradores da SECURITY deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não), os planos de evacuação das instalações físicas e as melhores práticas de saúde e segurança no ambiente de trabalho.

2.2. Todo e qualquer colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da empresa, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Plano, deverá informar o Coordenador ou algum dos Diretores, para que sejam tomadas as providências cabíveis. São atribuições dos Diretores relacionada a este Plano:

- definir os princípios éticos a serem observados por todos os colaboradores, constantes deste Plano ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos deste Plano e também apreciar e analisar situações não previstas;
- garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;
- tratar todos os assuntos que chegue ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da Sociedade, como também dos colaboradores envolvidos; e
- definir e aplicar eventuais sanções aos colaboradores.

## 3. CRITÉRIOS E PROCEDIMENTOS PARA ATIVAÇÃO DO PCN

3.1. O PCN da SECURITY é ativado por um dos sócios-gestores em situações em que a capacidade da empresa de conduzir seus negócios em seu curso normal for severamente comprometida.

3.2. São exemplos de casos de comprometimento qualquer situação que torne inviável aos sócios e funcionários acessarem fisicamente o escritório da SECURITY.

3.3. Ao tomar conhecimento da situação, o sócio gestor enviará mensagem por dispositivo de comunicação remota (telefones celulares) que for de funcionamento independente da rede interna da empresa a todos os contemplados neste PCN para assim iniciar sua implementação.

## 4. SERVIÇOS ESSENCIAIS, ESTRUTURA DE CONTINGÊNCIA E MOBILIZAÇÃO DE RECURSOS EXTERNOS

4.1. A estrutura tecnológica e de telefonia da SECURITY foi estruturada para permitir mobilidade, sem a perda do controle e segurança.

4.2. Independentemente da localização, os colaboradores poderão utilizar os serviços telefônicos da SECURITY através de aplicativo instalado em seus aparelhos de celular, bem como conseguirão acessar o servidor de arquivos da companhia, conforme delimitação de seus acessos, utilizando qualquer conexão de internet disponível, uma vez que os servidores de arquivos da SECURITY situam-se em ambiente de nuvem.

**Acesso Aos Servidores de Arquivos**

4.3. A infraestrutura da SECURITY não possui servidor de arquivos físico, todos os documentos, planilhas e informações utilizadas pelos seus colaboradores e sócios estão disponíveis no OneDrive for Business, conforme contrato vigente desde sua constituição com a Microsoft , sendo necessária apenas a existência de conexão de cada colaborador com a internet, para poder acessar normalmente seus arquivos, planilhas e demais documentos necessários para o dia a dia de trabalho.

## 5. PROCEDIMENTOS PARA SOLUÇÕES DE DETALHES OPERACIONAIS

5.1. Os principais sistemas utilizados pela SECURITY são acessados por meio de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com conexão à internet. A comunicação poderá continuar sendo realizada por meio de telefones celulares dos Colaboradores. Para tanto, os Colaboradores deverão ser comunicados, com a maior brevidade possível, acerca do estado de contingência, e estejam aptos a adequar a condução das suas atividades ao cenário aplicável.

## 6. ASPECTOS GERAIS

6.1. Este Plano é de uso restrito dos Colaboradores da SECURITY e não poderá ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

6.2. É responsabilidade do Coordenador de Contingência manter este Plano atualizado, bem como a realização de validação anual dos procedimentos estabelecidos neste Plano. Ainda, o Coordenador de Contingência realizará testes de contingências que possibilitem que a SECURITY esteja preparada para eventos desta natureza, proporcionando à SECURITY condições adequadas para continuar suas operações. Sendo assim, anualmente, deverá ser

realizado teste de contingência para verificar:

(i) Acesso aos sistemas;

(ii) Acesso ao e-mail corporativo;

(iii) Acesso aos dados armazenados;

(iv) Verificação do treinamento aos colaboradores para atuarem como back-up; e

(v) Qualquer outra atividade necessária para continuidade do negócio.