PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS DA JHSF CAPITAL LTDA.

I. OBJETO

Este plano de contingência e continuidade dos negócios ("**Plano**") visa estabelecer os princípios e critérios que norteiam as decisões da JHSF Capital Ltda. ("**JHSF Capital**") a serem observados nos casos em que eventualmente se materialize qualquer evento que possa causar indisponibilidade de recursos essenciais a fim de mitigar impactos financeiros, operacionais, legais e regulatórios.

Assim, em uma situação de crise e durante um período definido, os Colaboradores deverão observar o presente Plano para que os processos essenciais e críticos sejam mantidos de maneira adequada, preservando, desta forma, a continuidade das operações da JHSF Capital. O Plano também fundamenta o processo decisório em situações emergenciais, traçando medidas preventivas e corretivas para assegurar a integral operação da JHSF Capital em tais situações, de modo a mitigar os danos aos Colaboradores e a infraestrutura.

II. APLICAÇÃO

O conteúdo deste Plano é aplicável à JHSF Capital e deverá ser observado por todos os administradores, empregados, colaboradores, prestadores de serviço ou qualquer pessoa agindo em nome ou em benefício da JHSF Capital, tanto interna quanto externamente ("**Colaboradores**").

III. REGULAMENTAÇÃO

Este Plano foi elaborado de acordo com as leis e regulamentos aplicáveis, em especial a Resolução da Comissão de Valores Mobiliários ("**CVM**") nº 21, de 25 de fevereiro de 2021 ("**Resolução CVM 21**") e as diretrizes do Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("**ANBIMA**") de Administração de Recursos de Terceiros ("**Código ANBIMA de ART**").

IV. RESPONSABILIDADES

A responsabilidade em relação a este Plano é dividida entre a equipe de *Compliance* e Risco e a Diretor de Gestão de Recursos da JHSF Capital, conforme descrito a seguir.

Diretor de Gestão de Recursos da JHSF Capital:

(a) promover a conscientização e o entendimento entre os Colaboradores da necessidade estratégica de manter um processo eficiente e eficaz de continuidade de negócios;

(b) garantir a integridade e a confiabilidade da JHSF Capital perante o mercado e minimizar impactos de eventuais incidentes financeiros, de segurança ou de imagem que possam se materializar em crises ou desastres; e

(c) contratar e suportar a equipe de *Compliance* e risco para assegurar a sua capacidade de gerir, coordenar, definir, controlar e endereçar as principais questões relacionadas à continuidade de negócios da JHSF Capital.

Diretor de *Compliance*, Risco e PLD e equipe de *Compliance* e risco:

(a) analisar os potenciais impactos e incidentes e o seu nível de severidade;

(b) coordenar a estimação da probabilidade de ocorrência dos incidentes baseado em avaliações periódicas e pontuais;

(c) desenvolver procedimentos de contingência, recuperação de desastre, gestão de crise, análise e atualização de documentos, gestão de incidentes e suporte;

(d) coordenar, supervisionar e suportar as equipes que executam procedimentos de contingência e recuperação de desastres no caso de incidentes;

(e) coordenar a realização de procedimentos anuais de testes deste Plano para todos os ativos mapeados para suportar os processos críticos; e

(f) disseminar e oferecer treinamentos e campanhas para todos os Colaboradores de conscientização sobre a importância de manter atualizadas as estratégias, planos de contingência e de recuperação de desastres e ferramentas (*software, hardware* e outros) necessários para a execução dos procedimentos.

Além disso, todos os Colaboradores devem estar cientes de suas responsabilidades, de acordo com o seu respectivo escopo de sua atividade, para facilitar a execução deste Plano. Para tanto, todos os

Colaboradores da JHSF Capital serão preparados para exercerem suas funções em situações de contingência.

Incidentes comuns que os Colaboradores podem notar no cotidiano de suas atividades incluem, sem prejuízo de outros:

(a) acesso não autorizado, dano ou furto de ativos de informação (i.e. perda de documentos confidenciais, arquivos de log faltantes etc.);

(b) fraude em processos ou controles internos;

(c) comportamento anormal dos sistemas (e.g. reinicializações de sistema não planejadas, mensagens de log não esperadas);

(d) notificações de eventos de segurança (e.g. alertas físicos de segurança, alertas de identificação);

(e) evidências de brechas físicas (e.g. portas ou fechaduras abertas, alertas físicos de entrada não autorizada); e

(f) outros eventuais sinais de uma potencial brecha ou incidente de segurança.

V. MAPEAMENTOS DE ÁREAS E ATIVIDADES

Para garantir a continuidade dos negócios da JHSF Capital em situações adversas, foram identificados os seguintes elementos:

(a) Área de Tecnologia da Informação (TI): trata-se de área fundamental para o funcionamento da JHSF Capital, visto que todas as comunicações com corretoras, administradores de fundos e demais parceiros são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios). A continuidade das atividades da equipe de TI é fundamental para a realização de registros de operações (e.g. compra e venda de títulos e valores mobiliários, aplicações e resgates em fundos de investimento, transferência de recursos e pagamento de despesas da JHSF Capital);

(b) Escritório: trata-se do espaço físico onde são realizadas as operações da JHSF Capital. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução das atividades da JHSF Capital; e

(c) Pessoal: são os Colaboradores responsáveis pelas atividades exercidas pela JHSF Capital (e.g. análise e decisão para realização ou não de investimentos, equipe de *Compliance* e Risco).

Conhecendo aspectos da JHSF Capital que devem ser abrangidos por este Plano, conforme listados acima, a JHSF Capital traçou os seguintes riscos:

(a) Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falha e/ou interrupção no fornecimento de serviços essenciais como a falta de energia elétrica, falta de água, falha nas conexões de rede, indisponibilidade de internet, indisponibilidade de telefonia, incêndios, falhas nos sites das empresas que fornecem sistemas de uso da JHSF Capital;

(b) Problemas de acesso ao local/recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibilidade pode ser causada por eventos como greves dos transportes públicos, interdições pelas autoridades do prédio ou do entorno do escritório da JHSF; e

(c) Problemas de Segurança da Informação: os problemas dessa ordem são, dentro outros, o acesso não autorizado, dano ou roubo de informações ou ativos (e.g. login não autorizado, perda de documento confidenciais), violações físicas (e.g. portas ou fechaduras danificadas, alertas de intrusão física).

VI. CONTROLES PREVENTIVOS

VI.1. Efetiva Contingência

A JHSF Capital conta com acesso remoto aos seus bancos de dados virtuais disponíveis a todos os Colaboradores, nos termos das autorizações do Diretor de *Compliance*, Risco e PLD.

Além disso, cada Colaborador possui notebooks devidamente autorizados e com acesso à internet móvel para qualquer eventualidade, além de formas de conexão à internet banda larga. Ainda, a JHSF Capital possui sistema de rede sem fio em todos os seus departamentos.

O serviço de e-mail da JHSF Capital é garantido por provedor parceiro que provém suporte 24/7 (i.e. 24 horas por dia, durante 7 dias na semana), serviço de anti-spam, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. Adicionalmente, como sistema de comunicações internas e externas, a JHSF Capital utiliza o Microsoft Office 365, que possibilita o acesso remoto de todas as mensagens pelos Colaboradores.

O serviço de e-mail da JHSF Capital é garantido por dispositivo de segurança Fortinet que executa funções de firewall e antivírus. Além disso, o firewall de software é ativado corporativamente na rede do escritório.

Não obstante, as informações do portfólio estão armanezadas em sistemas internos da JHSF Capital e são disponibilizadas diariamente pelo administrador ou pela JHSF Capital, conforme previsto no regulamento do Fundo, que também serão os responsáveis por comunicar qualquer movimentação no passivo dos Fundos para seja possível a adequação do caixa dos Fundo às respectivas movimentações.

Como forma de assegurar a continuidade de seus serviços, em caso de falha de fornecimento de energia, a JHSF Capital possui *nobreak* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de outras quatro estações de trabalho (*desktops*) para a efetiva continuidade dos negócios. Ainda, os Colaboradores da JHSF Capital contam com telefones celulares, utilizados para substituir a telefonia fixa diante de eventuais falhas nas linhas telefônicas da JHSF Capital.

A Política de Segurança da Informação da JHSF Capital apresenta, de forma mais detalhada os procedimentos a serem adotados diante das contingências atinentes à Segurança da Informação. Em caso de dúvida quanto a esses procedimentos, a Política de Segurança da Informação está inserida no Manual de *Complicance* da JHSF Capital e pode ser consultada em http://www.jhsfcapital.com.br.

VI.2. Procedimentos de *backup*

A JHSF Capital possui procedimentos de *backup* específicos. Diariamente, sempre às 23h00 (vinte e três horas), todos os arquivos localizados da rede interna da JHSF Capital são copiados, de maneira automática, para um *Hard Drive* externo. Esses arquivos poderão ser armazenados em fitas magnéticas e/ou em um *Datacenter* externo.

Sempre que possível o software de *backup* será configurado para efetuar, de forma automática, a verificação do *backup*. Essa verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados armazenados no disco, de modo a mitigar possíveis falhas no *backup* dos arquivos da JHSF Capital.

Nesse sentido, por meio dos procedimentos de *backup* externo e, conforme exposto no item VI.1., do acesso remoto pelos Colaboradores da JHSF Capital aos e-mails, não será necessário que a JHSF Capital paralise suas atividades diante de eventual impossibilidade de acesso físico ao escritório.

VII. OCORRÊNCIA DE CONTINGÊNCIAS

Este Plano deverá ser acionado, em caráter imediato, mediante deliberação do Diretor de *Compliance*, Risco e PLD, em face da impossibilidade ou dificuldade em manter o funcionamento normal da JHSF Capital devido a problemas de ordem técnica (*hardware*), física, pessoal e de infraestrutura.

Acionado o Plano, o Diretor de *Compliance*, Risco e PLD deverá iniciar imediatamente a avaliação das causas que geraram a contingência, com o objetivo de solucionar o problema o mais rápido, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

(a) comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada Colaborador de acordo com a contingência ocorrida; e

(b) diante da impossibilidade de se utilizar o espaço físico do escritório, a JHSF Capital poderá continuar a funcionar através de Home Office, através de notebooks autorizados.

O Diretor de *Compliance*, Risco e PLD da JHSF Capital deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela JHSF Capital e reportar eventuais alterações e atualizações da contingência aos demais Colaboradores.

VIII. AÇÕES CORRETIVAS

Sem prejuízo de outras ações corretivas a serem adotada pela JHSF Capital em decorrência de uma contingência, diante de (i) falhas no sistema de telefonia, (ii) indisponibilidade de internet, (iii) impossibilidade de acesso ao escritório, ou (iv) falha na energia elétrica, após a solicitação do estabelecimento dos serviços ou solução do problema de infraestrutura, a JHSF Capital poderá continuar a funcionar através de *home office*, por meio de notebooks autorizados.

IX. TESTES PERIÓDICOS, AVALIAÇÃO E REVISÃO

O Diretor de *Compliance*, Risco e PLD realizará a testes periódicos com o objetivo de avaliar se a metodologia desenvolvida neste Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da JHSF Capital e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se tais planos podem ser ativados tempestivamente.

X. VIGÊNCIA

O presente Plano entrará em vigor na data de sua aprovação pela JHSF Capital e deverá ser atualizado, no mínimo, a cada 1 (um) ano, sendo que somente poderá ser modificado por deliberação expressa da Diretoria da JHSF Capital.

O Diretor de *Compliance*, Risco e PLD é responsável por manter este Plano atualizado, bem como validar os procedimentos aqui estabelecidos anualmente.

Este Plano pode ser consultado em http://www.jhsfcapital.com.br.

XI. SANÇÕES DA COMPANHIA AO DESCUMPRIMENTO DESTE PLANO

O descumprimento deste Plano sujeita os infratores às sanções disciplinares aplicáveis de acordo com as normas internas da JHSF Capital.

XII. HISTÓRICO DE REVISÕES

Revisão	Data	Motivo	Responsável
V1.0	Fev/23	Versão Inicial	Jurídico

XIII. VALIDAÇÃO

Descrição	Nome / Cargo
ELABORAÇÃO	Giovanna Araujo Pacheco – Gerente Jurídico Marcelo Mckenzie – *Head* de Finanças
REVISÃO E APROVAÇÃO	Diretoria Executiva e Diretor de *Compliance*, Risco e PLD

--*-*