STEN GESTÃO PATRIMONIAL LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

JUNHO / 2023

Sumário

1. OBJETO

1.1. O presente Plano de Contingência e Continuidade dos Negócios ("Plano de Contingência") tem como objetivo definir os procedimentos que serão seguidos pela **STEN GESTÃO PATRIMONIAL LTDA.** ("Gestora"), no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados planos de ação e estratégias para garantir que os serviços essenciais da Gestora sejam devidamente identificados e preservados após a ocorrência de imprevisto ou desastre.

1.2. O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da Gestora dentro do contexto de seu negócio.

1.3. O Plano de Contingência identifica duas variáveis para o funcionamento adequado da empresa: Infraestrutura e Processos.

1.4. A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática e sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.

1.5. Os Processos são as ações realizadas na operação do negócio e são diretamente dependentes do funcionamento adequado da infraestrutura.

2. ESTRUTURA OPERACIONAL

2.1. A Gestora é uma gestora de recursos de terceiros, e conta com uma estrutura operacional desenvolvida e preparada para eventuais emergências. O suporte para essa estrutura é formado por um corpo funcional com a competência necessária para a sua adequada atuação e por empresa responsável pela tecnologia de informação, devidamente contratada pela Gestora ("Empresa de TI").

3. POLÍTICA E PROCEDIMENTOS PARA BACK-UP

3.1. A Empresa de TI disponibilizará aos servidores da Gestora o serviço de *backup* e *restore* de arquivos, com o objetivo de garantir a segurança das informações, a recuperação dos mesmos em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

3.2. Diariamente, às 23h00 min, os arquivos armazenados em um servidor seguro, localizado na sede da Gestora, são criptografados e copiados de maneira automática por meio de ferramenta de backup do Windows 2018 Server e Cloud, sendo salvos em disco externo e cloud.

3.2.1. O processo de *back-up* será conduzido, sistematicamente, da seguinte forma:

(i) os arquivos relativos à operação são armazenados no servidor da rede.

(ii) o *back-up* de dados armazenados nos servidores da rede corporativa é realizado de forma automatizada 1 vez por dia às 23:00 horas, de acordo com os procedimentos de *back-up* e *restore* definidos pela Empresa de TI; e

(iii) o *restore* de dados deve ser solicitado à Empresa de TI, sendo realizado de acordo com os procedimentos específicos.

3.3. Verificação e teste de restauração: mensalmente o *software* será configurado para verificar automaticamente o *back-up*. A verificação será realizada por meio da verificação do log do software de *backup*.

4. EQUIPE DE CONTINGÊNCIA

4.1. Para coordenar todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da Gestora, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance e Risco (Coordenador de Contingência); e
- Diretor de Gestão.

4.2. Os membros dessa equipe tomarão as medidas cabíveis para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, na ausência de um dos diretores, isoladamente. Todos os colaboradores da Gestora serão comunicados imediatamente sobre essa decisão.

4.3. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com a Empresa de TI para comunicar o acionamento do Plano de Contingência e tratar do acesso aos dados/sistemas, bem como efetuar o desvio das ligações dos telefones do escritório para linhas alternativas.

5. EFETIVA CONTINGÊNCIA

5.1. O Plano de Contingência será acionado quando for identificada qualquer ocorrência ou situação que dificulte ou impeça a rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, aos clientes da Gestora e à Gestora propriamente dita.

5.2. Neste cenário, considera-se basicamente a impossibilidade ou dificuldade de manter o funcionamento normal da Gestora devido a problemas de ordem técnica (*hardware*), física (acesso ao escritório), pessoal (ausência significativa de funcionários) e de infraestrutura (falta de energia).

5.3. Nessa situação, o Diretor de Compliance e Risco da Gestora deverá acionar este plano, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência para

providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo:

(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;

(b) Caso seja verificada a necessidade de sair do escritório da Gestora, os colaboradores poderão continuar a desempenhar suas atividades através de H*ome Office*, uma vez que todos os arquivos podem ser acessados pela nuvem. A continuidade das operações da Gestora deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

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

5.5. O serviço de e-mail da Gestora é garantido pela Microsoft, que provém suporte 24/7, serviço de *antispam*, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

5.6. A Gestora conta com 3 (três) operadoras de telefone, i.e., Algar, Vivo e Mundivox. Em caso de falhas nas linhas telefônicas, os colaboradores da Gestora ainda possuem celulares que podem substituir a telefonia fixa.

5.7. As informações do portfólio, além de estarem nos sistemas internos da Gestora, são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos.

5.8. Em caso de falha de fornecimento de energia, a Gestora possui *nobreak* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de outras duas estações de trabalho (*desktops*) na Empresa de TI para a efetiva continuidade dos negócios.

6. ASPECTOS GERAIS

6.1. O serviço de e-mail da Gestora está hospedado nos servidores da Microsoft. O serviço possui suporte 24/7, serviço de *antispam*, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A Gestora detém uma conta corporativa, que é garantida com todos os serviços de segurança e *back-up*, sendo executadas funções de *firewall* e antivírus no nível do roteador. Além disso, o antivírus (*software*) é ativado em cada computador individual na rede do escritório da Gestora.

6.2. Com seus procedimentos de *back-up* externo e acesso remoto a e-mails, a Gestora continuará a funcionar, mesmo se não for possível ter acesso físico ao escritório. Além disso, todos os colaboradores têm acesso imediato a todas as informações contidas nos seus e-mails em qualquer situação de emergência.

6.3. Deverá ser mantida no servidor remoto uma lista com as informações de todos os integrantes da Gestora, das corretoras com as quais se realizam negócios, dos clientes e dos prestadores de serviço contratados.

7. DOCUMENTAÇÃO

7.1. O Diretor de Compliance e Risco tem por obrigação manter este Plano de Contingência atualizado, bem como realizar a validação a cada **12 (doze) meses** dos procedimentos estabelecidos neste Plano de Contingência.

7.2. O Diretor de Compliance e Risco também é responsável por realizar testes de contingências que possibilitem que a Gestora esteja preparada para eventos dessa natureza, proporcionando-lhe condições adequadas de continuidade de suas operações.

7.3. Anualmente, é realizado um teste de contingência para verificar:

a) Acesso aos sistemas;
b) Acesso ao e-mail corporativo;
c) Acesso aos dados armazenados; e
d) Qualquer outra atividade necessária para continuidade do negócio.

7.4. O resultado do teste é registrado em relatório, que serve como indicador para regularização das possíveis falhas identificadas, e como apoio para o constante aprimoramento deste Plano de Contingência.

7.5. Para realização dos testes de contingências mencionados no item 7.2. acima, o Diretor de Compliance e Risco contará com o apoio da Empresa de TI no que couber, podendo, inclusive, solicitar que a própria Empresa de TI realize e, adicionalmente, comprove a realização dos controles e procedimentos acima estabelecidos que lhe competem, respectivamente, monitorar e executar.

8. CONTROLE DE VERSÕES

Histórico das atualizações		
Data	**Versão**	**Responsável**
Abril de 2019	1ª	Diretor de Compliance e Risco
Fevereiro de 2022	2ª	Diretor de Compliance e Risco
Junho de 2023	3ª e Atual	Diretor de Compliance e Risco