Plano de Continuidade de Negócios (“PCN”)

23 de agosto

2024

Este documento estabelece as bases, princípios e regras para continuidade de negócios (“PCN”) da JPP Gestão de Recursos Ltda. (“denominada neste documento como “JPP”) na sua atuação interna, com o mercado e demais terceiros.

Plano de Continuidade de Negócios

Sumário

1. Objetivo

Este Plano de Continuidade de Negócios da JPP Gestão de Recursos Ltda. (“denominada neste documento como “JPP”), tem por objetivo estabelecer diretrizes e define o Plano de Continuidade do Negócio (“PCN”) que estabelece estratégias e procedimentos a serem observados na eventualidade de incidentes ou emergências que envolvam a da JPP.

2. Regulamentação Aplicável

- Resolução CVM nº 21/21;
- Código ANBIMA de Administração e Gestão de Recursos Terceiros,
- Regras e Procedimentos de Deveres Básicos;
- Guia Anbima de Cibersegurança;
- Lei nº 13.709/18 - Lei de Proteção de Dados Pessoais (LGPD) e alterações dadas pela Lei nº 13.853/19.

3. Abrangência

São abrangidos por este PCN todos os diretores e colaboradores da JPP, bem como os prestadores de serviços que realizarem atividades em seu nome.

4. Vigência e Atualização

O presente Plano entra em vigor na data de sua publicação e deverá ser revisto e, se necessário, atualizado pelo Compliance no mínimo a cada 24 (vinte e quatro meses), serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.

5. Da Gestão da Continuidade

A Continuidade de Negócios é um processo abrangente, que identifica ameaças potenciais inerentes aos negócios da JPP e os possíveis impactos nas operações provenientes de tais ameaças. Fornece uma estrutura para que se desenvolva um nível de resiliência organizacional que seja capaz de responder efetivamente e proteger os interesses das partes envolvidas, a reputação e as atividades de valor agregado da gestora.

A Continuidade de Negócios contempla o gerenciamento da recuperação em caso de interrupção e gestão de todo o Programa de Continuidade por meio de treinamentos, planos, testes, revisões e manutenções, a fim de garantir sua operacionalização e atualização.

A presente política leva em consideração o cenário de negócios no qual a JPP está inserida e as

disposições legais aplicáveis e a Lei Geral de Proteção de Dados Pessoais Lei 13.709/18 e alterações dadas pela Lei nº 13.853/19.

6. Objetivos Gerais Específicos

Como estratégia para atingir nosso objetivo principal, definimos como objetivos específicos:

a) Realizar backup diário de todo o banco de dados, envolvendo todas as operações diárias, incluindo os arquivos de programas;

b) Assegurar a integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;

c) Manter os sistemas operacionais disponíveis;

d) Manter rede eletrônica em funcionamento e em boas condições operacionais. Para redução e controle de eventuais perdas com contingências, todos os colaboradores da JPP deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho;

e) Manter uma estrutura específica de recursos em nuvem, para os acessos aos recursos necessários para execução das atividades da JPP.

7. Etapas e Procedimentos Para o Plano de Continuidade

A JPP possui uma estrutura que possibilita aos seus colaboradores desempenharem suas atividades de suas residências, inclusive o atendimento ao cliente (quando aplicável). Neste sentido, a instituição está devidamente preparada para a realização de atividades de maneira emergencial por este meio, em caso de indisponibilidade de sua sede.

O desenvolvimento do PCN é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

- Análise de Riscos de TI;
- Estratégia de recuperação.

Desta forma, simular situações de emergências, definir responsabilidades de atuação para cada colaborador na execução do PCN, e acima de tudo mantê-lo atualizado, são fatores críticos de sucesso.

São fatores que integram o PCN da JPP:

- **Estrutura Operacional**

a) manutenção no quadro funcional da JPP de profissionais experientes com dedicação exclusiva à gestora;

b) a existência do Diretor de Compliance, que, dentre outras funções, concentra a responsabilidade pelo suporte à JPP no que concerne a esclarecimentos de todos os controles e regulamentos internos (Compliance), bem como no acompanhamento de conformidade das operações e atividades da JPP com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos;

c) a existência de tecnologia da informação, sendo esta fundamental para o funcionamento da JPP, no sentido de que todas as comunicações com corretoras, administradores de fundos etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios), sendo também fundamental para a realização de registros das operações;

d) a manutenção da plena capacidade operacional do escritório, sendo este espaço físico onde são realizadas as operações da JPP e onde encontra-se instalada toda a infraestrutura, interna ou externa, necessária para a execução de suas atividades; e

e) Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem.

Tais fatores colaboram não só para melhor direcionar a aplicação de recursos pela JPP, mas também para incrementar o gerenciamento de riscos, conferir melhor fluidez ao fluxo de informações e ao processo decisório da JPP e para atendimento às necessidades mínimas de manutenção dos seus serviços/atividades.

Tendo identificado os fatores principais que integram seu Plano de Contingência do ponto de vista da estrutura da JPP e dos processos sob sua responsabilidade, os riscos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

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, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso da JPP, etc.;

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, por exemplo, de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório da JPP, vendaval, incêndio, etc.;

c) **Problemas Humanos:** Manipulação indevida de dados e sistemas, distúrbio civil, vírus de computador, falha de prestador de serviços/parceiro, roubo e/ou furto de recursos, sequestro de dados e informações, acesso indevido às instalações e erro humano (não intencional).

Com base no levantamento da estrutura da JPP e no mapeamento de riscos, a JPP tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações.

Com base no processo de gestão e avaliação de riscos (conforme a Política de Segurança da Informação, Cibernética e LGPD), o foco em continuidade levará em consideração os seguintes requisitos:

- A identificação dos riscos que afetem processos de negócio a serem cobertos pela PCN;
- A identificação da probabilidade de ocorrência do referido risco e o impacto para a gestora;
- A identificação dos tempos objetivados de recuperação.

Neste sentido, conforme avaliação de risco da JPP, foram definidos 2 (dois) ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação deste PCN. Esses ambientes são: Físico e o Tecnológico.

(i) Ambiente Físico: O ambiente físico é definido como o espaço onde as operações diárias da JPP são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e equipamentos necessários a essa operação, como também o acesso seguro a esses recursos.

As situações de problemas de acesso às suas dependências, os colaboradores da gestora devem continuar a desempenhar suas atividades a partir do plano de contingência. O plano contempla acesso remoto ao ambiente JPP através de recursos em nuvem, no qual os usuários para continuidade dos negócios tem seu login único e individual de usuário, acesso a todos os sistemas e arquivos necessários para realizar suas atividades. Em caso de equipamentos utilizados de propriedade do colaborador, para o ambiente de trabalho remoto, o mesmo deverá seguir os mesmos padrões de configurações e segurança utilizados pela JPP, além de autorização dos acessos a documentos e sistemas da gestora pelo Compliance.

(ii) Ambiente Tecnológico: O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a JPP possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela empresa em seu dia a dia e a garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da empresa, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

iii) Análise de Impacto no Negócio: O presente Plano foi elaborado após análise criteriosa pela JPP dos seguintes fatores:

- eventos que podem impactar as atividades desenvolvidas;
- estimativa da probabilidade de ocorrência de cada um dos eventos;
- relevância do impacto no negócio no caso de ocorrência de cada uma das circunstâncias analisadas.

O resultado da análise acima encontra-se no Anexo I: Análise de Impacto no Negócio. A presente análise foi definida de acordo com a estratégia de continuidade de negócios adotada pela JPP.

Todos os sistemas utilizados pela JPP no ambiente da gestão são acessados através de sites dos próprios provedores desses sistemas, como também através de recursos em nuvem, no qual viabiliza o acesso de qualquer local desde que se disponha de um computador com um link de internet. A comunicação com corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da JPP.

Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência, de forma que também estes tenham conhecimento da situação, de forma a impactar o mínimo possível a operação.

As informações relativas a backup, hardware, firewall, servidores, telefonia, rede, e-mails etc.

- **Equipe de Contingência**

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 JPP, foram definidos os seguintes responsáveis pela Equipe de Contingência:

a) Diretor de Compliance (Coordenador de Contingência); e

b) Diretor de Gestão de Recursos (Responsável pela definição de prioridades da área de gestão e operações a ser operada em modo de contingência);

c) Tecnologia e Segurança de Informação (responsável pela coordenação dos trabalhos de contingência do âmbito tecnológico).

Essa equipe deverá tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, na ausência de um dos diretores, isoladamente e deve ser comunicada imediatamente a todos os colaboradores da JPP.

O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com os Colaboradores que prestam serviço de Tecnologia da Informação para a Gestora, para comunicar o modo contingencial e tratar do acesso aos dados/sistemas, bem como efetuar o desvio das ligações dos telefones do escritório para linhas alternativas.

8. Cenários e Contingência

A ocorrência de eventos de contingência deverá ser avaliada pela Equipe de Contingência da JPP e, com base nas informações disponíveis, deverá ser tomada uma decisão quanto ao acionamento do Plano de Contingência.

Com base na decisão tomada pela Equipe de Contingência, a JPP deverá adotar os procedimentos a seguir listados.

- **Situação de Contingência**

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

Nessa situação, o Diretor de Compliance deverá acionar este Plano de Contingência, 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, quais sejam:

a) Comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da JPP 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) Caso seja verificada a necessidade de sair do escritório físico da JPP, os colaboradores poderão continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos podem ser acessados no servidor em nuvem. A continuidade das operações da JPP 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.

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

9. Testes

Serão realizados testes efetivos de utilização do site de contingência, verificando se tudo está funcionando como deveria.

Ademais, é responsabilidade do Diretor de Compliance manter este Plano de Contingência atualizado, bem como a realização de validação dos procedimentos estabelecidos neste Plano de Contingência.

Neste sentido, o Diretor de Compliance realizará testes de contingências (além do teste relativo ao site de contingência) que possibilitem que a JPP esteja preparada para eventos desta natureza, proporcionando à JPP condições adequadas para continuar suas operações.

Sendo assim, anualmente, é realizado um 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.

O resultado do teste deve ser registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

10. Divulgação

Um dos fatores de primordial importância para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a gestora definiu que serão realizadas sessões de divulgação a todos os colaboradores e envolvidos na continuidade de negócios.

A divulgação será organizada pelo Compliance, sempre que necessário, visando manter os colaboradores da equipe de contingência atualizados sobre os conceitos de continuidade, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação dos negócios vigente.

11. Considerações Finais

Todas as dúvidas sobre as diretrizes deste PCN podem ser esclarecidas com o Compliance da JPP.

12. Manutenção Dos Arquivos

A JPP manterá armazenado todos os arquivos eletronicamente, pertinente ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

ANEXO I

Evento Potencial	Probabilidade de Ocorrência	Análise de Risco	Impacto	Ações Mitigatórias de Respostas ao Evento
Impedimento do acesso físico à sede (desastres naturais, incêndio, interdição, etc.)	Baixa	Impossibilidade de acesso às estações de trabalho na sede	Alto	Sistemas rodam em servidores em "nuvem" Método de trabalho Home Office
Problemas com a Infraestrutura de comunicação da sede	Baixa	Falta de acesso ao telefone fixo ou ao e-mail corporativo	Médio	Uso de telefones celulares Comunicação aos clientes e prestadores de serviços quanto a comunicação de contingência
Problemas com infraestrutura de sistemas e rede (nuvem)	Baixa	Incapacidade de acessar o sistema ou outras ferramentas e documentos nos diretórios da rede (nuvem)	Médio	Sistemas rodam em servidores em "nuvem" Arquivos de dados com backup diário
Perda de fornecimento de energia elétrica (serviço público)	Média	Incapacidade de acesso aos sistemas ou ferramentas e documentos nos diretórios de rede (nuvem)	Alto	Computadores com nobreaks próprios que suportam de 15 (quinze) minutos a 2 (duas) horas.
Perda de fornecimento de internet (serviço	Média	Incapacidade de acesso aos sistemas ou ferramentas e	Alto	Uso de Internet de celulares.

privado)		documentos nos diretórios de rede (nuvem)		Método de trabalho Home Office.
Falha de Equipamento	Baixa	Problema de continuidade de alguns processos	Alto	Acionamento da empresa terceirizada prestadora de serviços de tecnologia da informação.
Perda de pessoas chaves na organização	Baixa	Perda de conhecimento específico e potencial problema de continuidade de alguns processos	Médio	Políticas e Procedimentos escritos. Treinamentos internos. Ausência nas férias, em que comprova a contingência por no mínimo duas semanas.