PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Versão Atualizada: Outubro/2024

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Objetivo

Definir as bases, princípios e regras para contingências e continuidade de negócios da HORIZONTE CAPITAL GESTÃO DE INVESTIMENTOS LTDA. e na PEAK WEALTH ADVISORY GESTORA DE RECURSOS LTDA. (ambas, doravante, em conjunto, as "GESTORAS", e, individualmente, a "GESTORA").

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, gestores, consultores e demais pessoas físicas ou jurídicas contratadas, ou outras entidades que participem, de forma direta, das atividades diárias e negócios, representando qualquer das GESTORAS (doravante, "Colaboradores").

Revisão e Atualização

Este Plano de Contingência e Continuidade de Negócios ("PCN") deverá ser revisado e atualizado cada 2 (dois) anos, ou em prazo inferior, caso necessário em função de mudanças legais, regulatórias, autorregulatórias ou estruturais de qualquer das GESTORAS.

Responsabilidades

Caberá ao Diretor de Compliance e PLD a avaliação das ocorrências.

Contexto Operacional e de Negócios

Este PCN foi elaborado considerando as seguintes premissas e particularidades do modelo operacional e de negócio das GESTORAS:

- os fornecedores dos sistemas utilizados pelas GESTORAS se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades das GESTORAS;

- os Colaboradores das GESTORAS estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;
- as GESTORAS alocam recursos sob gestão, e têm seus produtos distribuídos, mediante a utilização de corretoras/plataformas de investimento acessíveis pela web e disponíveis para qualquer dispositivo eletrônico (laptops, smartphones, tablets ou computadores de mesa);
- os sistemas de consolidação de carteiras utilizados pelas GESTORAS identificam os clientes por meio de siglas, dispensando a identificação mediante o preenchimento de cadastro com informações pessoais;
- os arquivos contendo informações pessoais e financeiras dos clientes das GESTORAS são armazenados em nuvem, com *backups* periódicos não superiores a 7 (sete) dias corridos, podendo ser recompostos solicitando tais informações aos próprios clientes;
- os dispositivos eletrônicos (*laptops*, *smartphones*, *tablets*) utilizados no exercício das atividades das GESTORAS possuem senhas de acesso e criptografia;
- as GESTORAS utilizam redes sem fio para fornecer acesso à web para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à web, os Colaboradores utilizam redes/roteadores de redundância. Neste caso, e em caso de trabalho remoto, os Colaboradores das GESTORAS comprometem-se a utilizar redes sem fio seguras para desempenhar suas atividades;
- o espaço físico/escritório das GESTORAS é o local preferencialmente utilizado para as suas respectivas atividades, reuniões com clientes, comitês e reuniões comerciais com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas das GESTORAS estão parametrizados para serem passíveis de desempenhado remoto.

Princípios e Obrigações

O PCN é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los em prazo previamente estabelecido.

Para identificação dos ativos críticos,[1] devem ser considerados os riscos a seguir, no caso de interrupção repentina da rotina usual das GESTORAS:

a) **impacto financeiro** – situações em que a descontinuidade de negócios possa atingir os veículos sob gestão, ou a situação financeira e patrimonial de qualquer das GESTORAS;

[1] Todo e qualquer sistema, equipamento, arquivo etc., em suma, todo ativo essencial para o mínimo funcionamento das GESTIRAS, atendendo a suas obrigações legais críticas.

b) **impacto legal** – descontinuidade de negócios passível de gerar consequências legais aos veículos sob gestão, seus cotistas, ou mesmo às próprias GESTORAS;

c) **impacto de imagem** – risco de a descontinuidade de negócios impactar a reputação e confiabilidade das GESTORAS perante seus clientes e/ou o público investidor;

d) **acidentes, casos fortuitos e força maior** – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle das GESTORAS, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

As posições, áreas e sistemas considerados críticos constam do Anexo I a este PCN.

Classificação de Riscos e Providências

As GESTORAS adotam a seguinte classificação de riscos, com as respectivas providências a serem tomadas:

Nível 1: baixa probabilidade de ocorrência e/ou de impacto nas atividades das GESTORAS, com monitoramento cotidiano para a sua prevenção;

Nível 2: riscos demandantes de atenção constante, com impacto potencial médio nas atividades das GESTORAS e necessidade de maior nível de controles preventivos;

Nível 3: riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades das GESTORAS, com adoção de rigorosos controles preventivos.

São exemplos de riscos de nível 3 as situações de indisponibilidade e inacessibilidade total[2] de pessoas a seus meios/equipamentos de trabalho. Nestes casos, medidas preventivas incluem a definição de substitutos para as posições chave devidamente treinados, habilitados e capacitados para atuar no desempenho das funções requeridas.

Também são classificados desta forma (nível 3), a título de exemplo:

- falha de segurança/manutenção/atualização dos softwares e serviços críticos utilizados pelas GESTORAS no exercício de suas operações e monitoramentos periódicos;[3]

[2] Entendendo-se como inacessibilidade e indisponibilidade de um profissional, a situação em que este está totalmente impedido de acessar as ferramentas e informações necessárias para os exercícios de suas atividades. O adequado acesso eletrônico/virtual é o ativo relevante para a adequada disponibilidade do profissional, independente se nas dependências físicas da GESTORA.

[3] Que têm como medidas preventivas a obtenção dos respectivos Planos de Contingência dos provedores de tais softwares ou serviços, bem como o acompanhamento dos resultados periódicos dos testes de contingência aplicados e dos planos de ação

- interrupção do funcionamento de equipamentos utilizados pelos Colaboradores das GESTORAS que inviabilizem sua utilização nas atividades de operação e monitoramentos periódicos;[4]
- situações de indisponibilidade dos serviços e sistemas das instituições administradoras e custodiantes dos fundos/carteiras sob responsabilidade das GESTORAS, bem como das plataformas por ela utilizadas para distribuição de tais fundos.[5]

São exemplos de riscos de nível 2 as situações de falha de segurança/manutenção das instalações das GESTORAS, que têm como medidas preventivas a verificação da manutenção de extintores, *sprinklers* e detectores de fumaça instalados nas suas dependências, além da operação/instalação de controles de acesso às suas dependências.

São exemplos de riscos de nível 1 situações não diretamente relacionadas às GESTORAS e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle.

Controles Preventivos das GESTORAS

- Identificação, treinamento e capacitação profissional de substitutos para exercer as atividades chave da operação das GESTORAS;
- Controle de acesso às dependências das GESTORAS;
- Manutenção de provedores para acesso a arquivos eletrônicos, planilhas e demais documentos de forma segura e transparente ao usuário, bem como dos respectivos backups desses materiais;
- Manutenção de sistema antivírus e *firewall* para salvaguardar os arquivos eletrônicos utilizados pelas GESTORAS;
- Servidores/provedores de serviços tecnológicos, de dados, ferramentas contratadas etc. – controles e redundâncias dos serviços de servidores e prestadores de serviço em ambiente em nuvem, com as devidas proteções antivírus, firewall, backup etc.

As GESTORAS trabalham com níveis consistentes de redundância. O *backup* é armazenado diariamente em ambiente em nuvem com redundância de provedores de internet e telefonia.

---

estabelecidos para mitigar eventuais falhas identificadas em tais testes (quer sejam nas dependências das GESTORAS ou nas dos fornecedores).

[4] Cuja medida preventiva inclui a manutenção backup dos arquivos necessários para o desempenho das atividades cotidianas, de modo a sempre possibilitar a continuidade normal de suas atividades, mesmo em eventos de crise, quer seja nas dependências das GESTORAS ou fora delas.

[5] Que tem como medidas preventivas a obtenção dos respectivos Planos de Contingência de tais parceiros de negócio.

O serviço de e-mail e servidores também são armazenados em nuvem e a interface operacional do administrador pode ser acessada de qualquer lugar via internet. Os procedimentos definidos a seguir compõem este PCN:

Procedimentos	Periodicidade	Responsável
Identificar as pessoas críticas para a operação das GESTORAS e suas respectivas atividades, e garantir que estejam capacitadas para exercer tais atividades	Sempre que necessário, no caso de novas atividades e pessoas, no mínimo anualmente.	Anualmente, o Diretor de Compliance e PLD solicita a revisão do Anexo I.
Identificar e reavaliar os sistemas críticos, e atualizar o Anexo I, bem como os telefones do plano de comunicação.	Sempre que necessário, no caso de novas atividades, pessoas e sistemas, no mínimo anualmente.	Anualmente, o Diretor de Compliance e PLD solicita a revisão do Anexo I.
Decidir pelo início da contingência. A comunicação deve ser efetuada conforme o Anexo II.	Na efetiva ocorrência de incidentes.	Dois sócios e/ou dois Diretores, ou um sócio e um Diretor em conjunto.
Acionar o plano de contingência.	Na aprovação do início da contingência.	O plano de continuidade poderá ser acionado pelas pessoas autorizadas pelas GESTORAS, conforme Anexo II.
Informação à equipe.	Após decisão pelo início da contingência na estrutura alternativa.	O plano de comunicação consta do Anexo III.
Após a contingência, verificar o que motivou o incidente/crise, e se o motivo é passível de ações de aprimoramentos, bem como aprimoramento do PCN.	Após contingência.	Gestores das áreas, com reporte e registro do Diretor de Compliance e PLD.
Realizar testes do Plano.	Anualmente.	Diretor de Compliance e PLD coordena com os gestores das respectivas áreas nas GESTORAS.

Testes de Continuidade dos Negócios

O Plano de Continuidade de Negócios será objeto de validação e testes a cada 12 (doze) meses.

ANEXO I

Atividades e Sistemas Críticos

Quadro mínimo de profissionais com acesso aos sistemas, redes etc. em situação de contingência
1 de Gestão
1 de Risco e Compliance

Sistemas críticos com acesso em situação de contingência
Sistemas de gestão
Sistemas do administrador, plataformas, corretoras etc. (ordens de compra e venda, aplicação e resgate e demais movimentações, saldos etc.)
Sistema de gerenciamento de risco
Sistema de análise de ativos, carteiras etc.
Conexão de internet
Pacote Office e demais ferramentas de apoio
E-mail
Dados e arquivos das GESTORAS

No caso de impossibilidade temporária ou definitiva de atuação do responsável junto à CVM pela administração de carteira de valores mobiliários, a respectiva GESTORA nomeará um responsável (temporário ou definitivo), devendo a CVM ser comunicada por escrito, no prazo de 1 (um) dia útil a contar da sua ocorrência, no caso de total ausência e necessidade de substituição do titular.

Se ocorrerem situações de problemas de acesso às suas dependências, as equipes das GESTORAS devem continuar a desempenhar suas atividades através de *home office*, uma vez que todos os arquivos e e-mails podem ser acessados pela nuvem pelos Colaboradores das GESTORAS. Assim, é possível permanecer trabalhando ainda que fora do escritório físico das GESTORAS.

Os sistemas utilizados pelas GESTORAS são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares das equipes das GESTORAS. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência das GESTORAS, de forma a que estes também tenham conhecimento da situação tão logo ela ocorra, buscando impactar o mínimo possível a operação de gestão de recursos das GESTORAS.

ANEXO II

Pessoas Autorizadas a Iniciar Plano de Contingência e Continuidade de Negócios na Estrutura Alternativa

---

- Diretor Responsável pela Gestão ou profissional delegado da equipe;
- Diretor Responsável por Compliance ou profissional delegado da equipe;
- Diretor Responsável por Risco ou profissional delegado da equipe;
- Demais autorizados (se aplicável): demais sócios.

Quaisquer das pessoas acima está autorizada a ativar o PCN na eventual ausência, por qualquer razão, das demais, de forma a sempre possibilitar a preservação ininterrupta das atividades das GESTORAS.

ANEXO III

Plano de Comunicação - Modelo – "*Call Tree*"

As GESTORAS utilizam primordialmente o acesso remoto (via celular ou computadores pessoais) e listas em aplicativos de mensagens via telefone celular (Whatsapp) como forma de comunicação de contingência, visando principalmente à efetividade e agilidade proporcionada por tais ferramentas em contextos dessa natureza.

A comunicação é iniciada pelos indivíduos mencionados no Anexo II, e enviada a todos os membros das respectivas equipes, os quais participam dos grupos pertinentes, de maneira a assegurar a pronta e eficiente comunicação da contingência em questão, em tempo hábil e oportuno.

Não obstante, está disponível no diretório público a lista com ramais e telefones celulares e pessoais atualizados, inclusive com telefones alternativos e endereços de contingência de seus membros.