POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

PORTOGALLO INVESTIMENTOS LTDA.

Janeiro-2023
Versão 03

ÍNDICE

INTRODUÇÃO E OBJETIVO

A presente Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética da Portogallo Investimentos Ltda. ("Portogallo Investimentos" ou "Gestora") tem por objetivo descrever os procedimentos observados pela Gestora para garantir a devida segregação, confidencialidade e segurança das informações, para fins de atendimento ao disposto na regulamentação vigente.

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética se aplica aos sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Portogallo Investimentos ("Colaboradores").

CONFIDENCIALIDADE

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Portogallo Investimentos são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na Portogallo Investimentos e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes da Portogallo Investimentos deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, por escrito, salvo na hipótese de decisão judicial específica que determine à Portogallo Investimentos a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da Comissão de Valores Mobiliários ("CVM"). Caso a Portogallo Investimentos ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser comunicado aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Portogallo Investimentos, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Portogallo Investimentos. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da Portogallo Investimentos, para que sejam tomadas as medidas cabíveis.

A Portogallo Investimentos exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Portogallo Investimentos, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

O material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Portogallo Investimentos, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa, por escrito, da diretoria. Ainda, os arquivos eletrônicos recebidos ou gerados pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo da área, do cliente ou do projeto a que se refere tal arquivo eletrônico.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade da Gestora, presente no Anexo II à presente Política de *Compliance*, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Gestora e durante certo período após terem deixado a Portogallo Investimentos.

Para fins de manutenção das informações confidenciais, a Portogallo Investimentos recomenda que seus Colaboradores (i) bloqueiem o computador quando o mesmo não tiver sendo utilizado ou estiverem ausentes da sua estação de trabalho; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha pessoal de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora ("Informações" ou "Informação"), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de *Compliance*, Risco e PLDFT deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de *Compliance*, Risco e PLDFT, primeiramente, identificará se a Informação vazada refere-se ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de *Compliance*, Risco e PLDFT procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. No caso de vazamento de Informações relativas aos cotistas:

Neste caso, ao Diretor de *Compliance*, Risco e PLDFT procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de *Compliance*, Risco e PLDFT ficará à inteira disposição para auxiliar na solução da questão.

SEGURANÇA DA INFORMAÇÃO

A. Aspectos Gerais

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas fisicamente na sede da Gestora, com back-up de dados. O acesso aos arquivos é permitido apenas aos diretores da Portogallo Investimentos, ou aos Colaboradores previamente por eles autorizados.

Todo software disponibilizado aos Colaboradores deverá ser utilizado somente para os negócios da Portogallo Investimentos, em consonância com os acordos de licenciamento firmados.

Conforme mencionado acima, a realização de *back up* de todas as informações armazenadas no CPD físico da gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O acesso aos sistemas de informação da Portogallo Investimentos é feito por meio de um par "usuário/senha". O acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Gestora. O controle desses dados é de domínio da Portogallo Investimentos, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

Para acessar informações nos sistemas da Gestora deverão ser utilizadas somente ferramentas e tecnologias autorizadas e previamente estabelecidas pela Portogallo Investimentos, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas).

Adicionalmente, informamos que a rede da Portogallo Investimentos é composta por diretórios de dois níveis: (i) diretórios de informações públicas, aos quais todos os Colaboradores têm acesso, contendo tão somente informações de natureza administrativa; e (ii) diretórios de acesso restrito, cujo acesso é somente pré-autorizado pelo Diretor de *Compliance*, Risco e PLDFT aos membros de alguns departamentos específicos, em todos os casos sendo necessário o log-in e senha de cada integrante.

Todo Colaborador que tiver acesso aos sistemas de informação da Portogallo Investimentos é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Colaborador da Gestora.

A Portogallo Investimentos se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Portogallo Investimentos ou utilizados em nome dela, a fim de assegurar o fiel cumprimento desta política de Segurança da Informação, bem como da legislação em vigor.

B. Testes Periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Verificação semestral do login dos Colaboradores;
(ii) Anualmente, altera-se a senha de acesso dos Colaboradores;
(iii) Testes trimestrais no firewall;
(iv) Testes semestrais nas restrições impostas aos diretórios;
(v) Manutenção semestral de todo o "hardware" por empresa especializada em consultoria de tecnologia de informação;
(vi) Testes no "back-up" (salvamento de informações) semanal, realizado na nuvem.

SEGREGAÇÃO DE ATIVIDADES

A Portogallo Investimentos é uma Gestora de Investimentos independente com autorização de funcionamento em conformidade com a Resolução CVM n° 21, de 25 de fevereiro de 2021, conforme alterada ("Res. CVM 21").

Visando atribuir o mais elevado grau de transparência, salienta-se que a Portogallo Investimentos possui como controladora a empresa Maracajú Comércio Empreendimentos e Participações S/A ("Maracajú"), sociedade que não exerce atividades de cunho operacional. A Maracajú, por sua vez, exerce controle na MP Associados Consultoria de Investimentos LTDA, inscrita no CNPJ sob o n° 08.234.053/0001-89 ("MP Associados"), sendo a MP Associados, portanto, empresa sob controle comum. As atividades centrais desenvolvidas pela MP Associados são: confecção de relatórios gerenciais ou de controle que mostram a rentabilidade, composição e enquadramento de uma carteira de investimento de acordo com

as políticas de investimentos traçadas e informadas pelo próprio cliente, seja no mercado doméstico ou estrangeiro; planejamento financeiro; planejamento sucessório; consultoria acerca de questões atinentes aos produtos previdenciários existentes; e administração de finanças em geral.

A. Ausência de conflitos de interesses

No tocante à sociedade Maracajú, não há que se falar em qualquer forma de conflito de interesses, haja vista que tal sociedade não exercer atividades de cunho operacional. A MP Associados, por sua vez, exerce atividades fora do mercado financeiro e de capitais, não suscitando, portanto, conflitos de interesses. Em razão da inexistência de conflitos de interesses, a Portogallo Investimentos e a MP Associados Consultoria não adotam segregação física e funcional.
Sem prejuízo, cumpre salientar que para salvaguardar eventuais conflitos de interesse entre as áreas a Gestora se utiliza das seguintes regras: (i) em primeiro lugar, existe a segregação lógica das áreas, em especial operacional e de negócios, sendo os acessos aos diretórios completamente segregados, com controle individual de acesso, de forma a garantir o máximo nível de confidencialidade das informações e manter o sigilo devido das operações realizadas pela Gestora; (ii) todo e qualquer benefício recebido pela Gestora diretamente ou indiretamente, serão integralmente revertidos aos seus clientes, conforme estabelecido na regulamentação em vigor. Ademais, eventuais rebates recebidos por investimentos feitos pelos fundos e/ou carteiras administradas geridos pela Gestora serão devolvidos aos próprios fundos investidores e/ou às carteiras, exceto nos casos de investimentos feitos por (a) investidores profissionais que tenham assinado o Termo de Ciência previsto na Instrução CVM nº 555/2014, ou (b) fundo de investimento em cotas de fundo de investimento que invista mais de 95% (noventa e cinco por cento) de seu patrimônio em um único fundo de investimento.

Não obstante, a Gestora atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros e exercendo a distribuição de cotas dos fundos sob a sua gestão, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito dentro da Gestora. Não obstante, a Portogallo Investimentos manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

O primeiro nível de segregação dentro das atividades da Portogallo Investimentos refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de gestor, analistas, *compliance*, risco e administrativo. Perfis de acesso, e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade ("*as-needed basis*") nos comitês instituídos pela Gestora, sendo que os participantes se responsabilizam pelo sigilo das informações.

O acesso de pessoas que não fazem parte do quadro de Colaboradores da Portogallo Investimentos será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração da Portogallo Investimentos, e desde que acompanhadas de Colaboradores da Portogallo Investimentos. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da Portogallo Investimentos, com exceção dos casos em que tenha sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a clientes nas dependências da Portogallo Investimentos deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

As diferentes áreas da Gestora terão suas estruturas de armazenamento de informações logicamente segregada das demais, de modo a garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

Sem prejuízo, as regras destacadas na política de Segurança da Informação, tratada neste documento, sobretudo no que tange às segregações eletrônicas e de funções, se aplicam para fins da presente política de Segregação das Atividades, e devem ser observadas pelos Colaboradores da Gestora.

PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Responsável: Diretor de *Compliance*, Risco e PLDFT

A. Identificação e avaliação de riscos (*risk assessment*)

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:

a) Malware (vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;
d) Phishing scam;
e) Vishing;
f) Smishing;
g) Acesso pessoal;
h) Ataques de DDoS e botnets;
i) Invasões (advanced persistent threats).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Gestora definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento,

criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A Gestora levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

B. Ações de prevenção e proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a Gestora adota, conforme já detalhado nas regras internas que tratam de Segurança da Informação e Segregação de Atividades.

A Gestora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis. A Gestora deve criar logs e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela Segurança Cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A Gestora conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais. A Gestora deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de *Compliance*, Risco e PLDFT.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Gestora, bem como avisar prontamente o Diretor de *Compliance*, Risco e PLDFT.

Não obstante o disposto no parágrafo anterior, todos os anexos dos e-mails recebidos pelos Colaboradores da Gestora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A Gestora adota também backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da Gestora.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 18 da Res. CVM 21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da Gestora e devem ser observadas integralmente.

A Gestora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A Gestora mantém inventários atualizados de hardware e software, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da Gestora deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A área responsável deve também monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

Deve-se, ademais, realizar testes de invasão externa, phishing, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados na forma definida no item anterior devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

C. Plano de resposta

A área de *compliance* e risco deve, conjuntamente com os profissionais de cybersecurity e segurança da informação, elaborar um plano formal de resposta a ataques virtuais. A Gestora deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.
O plano de resposta deverá levar em conta os cenários de ameaças previstos no risk assessment. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

D. Reciclagem e revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da Gestora sobre a matéria, deverá ser revisto e atualizado semestralmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A Gestora deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

A. Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal em suas instalações principais, a Portogallo Investimentos possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada Colaborador na execução do Plano de Continuidade de Negócio ("PCN").

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela Portogallo Investimentos, de forma que os interesses dos clientes da Portogallo Investimentos não sejam prejudicados.

O PCN estabelecido e sua ativação é responsabilidade da sócia Magda Maria Malvão Portugal. Periodicamente, o plano será revisado pela Diretoria de *Compliance* e Risco com a finalidade de: (i) verificar que o PCN esteja em concordância com as leis e normas dos órgãos reguladores e (ii) zelar por sua atualização e cumprimento do cronograma de treinamento previsto.

B. Principais riscos potenciais mapeados

A análise do impacto do negócio foi resumida para refletir os potenciais riscos que podem causar desastres, incidentes e consequentes possíveis perdas ao negócio da Gestora. São eles:

1. Queda de energia.
No-break para até 1 (uma) hora.

2. Queda do link para acesso à internet.

Links redundantes de operadoras diferentes e utilização de modens de operadoras de Celular.

Caso nenhuma das contingências funcionem, é possível fazer o acesso remoto aos emails, que podem ser acessados através de outros provedores.

3. Contingências para e-mail e rede de arquivos.

Indisponibilidade do serviço de e-mail e rede de arquivos.

4. Invasão da intranet por hackers.

Firewall com monitoramento e alertas de segurança.

5. Impossibilidade de acessar o escritório

Algum desastre ou outro fato de força maior impede os funcionários de acessarem o escritório.

C. Respostas do PCN

Para os pontos "1" e "2", a Gestora entende que a solução mais rápida é a utilização de outro computador de fora do escritório com acesso a internet.

Para o item "3", o serviço de e-mail é poderá ser acessado remotamente, garantindo a continuidade. Há possibilidade de comunicação nos celulares dos funcionários.

No item "4" e "5" o recomendado é utilizar a estação em nuvem, que possui acesso direto ao backup dos arquivos.

A implementação dos planos de contingência deverá ser realizada em até quatro horas e será de responsabilidade da sócia Magda Maria Malvão Portugal.

O reestabelecimento da operação poderá ser realizado por terceiros contratados pela Administradora da Gestora e o prazo de ajuste será estimado pelo prestador de serviço em questão.

Adicionalmente, se necessário, a Gestora adotará soluções para:

(a) Substituir equipamentos danificados;
(b) Efetuar despesas contingenciais, incluindo a compra de equipamentos ou contratação de serviços que se fizerem necessários;
(c) Avaliar os prejuízos decorrentes da interrupção das atividades regulares.

D. Medidas de Prevenção

A Gestora realiza o backup de seus dados, diariamente, possibilitando o acesso às últimas versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Os principais executivos da Gestora possuem acesso remoto aos seus e-mails, de modo que possam acessá-los de fora do escritório, se necessário.

Os registros contábeis da Gestora ficarão com o contador responsável (terceirizado) e as informações sobre os fundos de investimento cujas carteiras serão geridas pela empresa ficarão com a respectiva instituição administradora.

A equipe de gestão da Gestora tem acesso a softwares que permitem a consulta do mercado financeiro em qualquer lugar do mundo.

E. Teste de Contingência

Será planejada a realização de testes de contingências anualmente, sob responsabilidade do Diretor de *Compliance*, Risco e PLDFT, sem prejuízo da implementação de testes que se façam necessários em uma menor periodicidade, de modo a possibilitar que a Gestora esteja preparada para a continuação de suas atividades. Tais testes devem ser realizados com o objetivo de verificar as condições para:

a) Acesso aos sistemas;
b) Acesso ao e-mail corporativo;
c) Acesso aos dados armazenados em procedimento de backup; e
d) Outros necessários à continuidade das atividades da Gestora.

O resultado de cada teste anual será registrado em relatório próprio obedecendo o disposto na regulamentação aplicável e as orientações das entidades responsáveis pela supervisão das atividades, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do presente PCN.

O PCN foi elaborado tendo em vista a possibilidade de realização de todos os trabalhos prestados pela Gestora sem dependência do acesso à sua localidade física.