Manual de Regras, Procedimentos e Controles Internos

Atualizado: 02/06/2020

I - Objetivo

O objetivo deste documento é descrever e divulgar quais são os princípios e procedimentos que a Paineiras Investimentos utiliza para assegurar que está em conformidade com as leis e regulamentos internos e externos voltados à área de gestão de recursos. As políticas apresentadas neste manual são complementares e cumulativas às demais políticas e diretrizes da Paineiras Investimentos, segregadas entre documentos públicos e restritos.

II – Pessoas Sujeitas ao Manual

Todos os sócios, administradores, funcionários e estagiários ("Colaboradores") da Paineiras Investimentos estão sujeitos às regras contidas neste manual e devem assinar um termo de adesão ao mesmo (o detalhamento desse procedimento está descrito no item IV). Também ficam sujeitos às regras deste manual, eventuais terceirizados que possuem acesso às informações reservadas ou privilegiadas no âmbito de suas atividades.

III – Responsabilidades

A responsabilidade pela elaboração, manutenção e cumprimento das normas descritas neste manual é da Área de Cumprimento de Normas e do Comitê de Cumprimento de Normas da Paineiras Investimentos.

O Comitê de Cumprimento de Normas é composto pelos membros da Área de Cumprimento de Normas, incluindo o Diretor de Cumprimento de Normas e da ICVM558, e pelos membros do Comitê Estratégico.

O Comitê de Cumprimento de Normas tem como suas principais atribuições e responsabilidades:

- Revisão e aprovação do Código de Ética, Manual de Regras, Procedimentos e Controles Internos, e de todas as demais políticas desenvolvidas pela empresa;
- Avaliação e aprovação do Relatório Anual de Conformidade (Art. 22 da ICVM 558);
- Indicação do diretor responsável pelo cumprimento de normas relativas à prevenção da lavagem de dinheiro, de acordo com a Instrução CVM 617 ou regulamentação que venha a substituir;
- Apreciação e definição das ações a serem tomadas em relação a eventuais denúncias de infrações e violações ao Código de Ética e demais políticas da empresa, especialmente aos casos relacionados à PLDFT e Política de Procedimentos Anticorrupção.

A Área de Cumprimento de Normas da Paineiras Investimentos é composta pelo Diretor de Cumprimento de Regras, Políticas, Procedimentos e Controles Internos e da ICVM558 e pelo gerente responsável pelo cumprimento de normas. Esta área opera de forma independente uma vez que seu diretor, além de sócio, não está subordinado funcionalmente a nenhum outro diretor.

As responsabilidades da Área de Cumprimento de Normas são:

- Elaboração, manutenção e adequação das normas descritas no Manual de Regras, Procedimentos e Controles Internos, no Código de Ética e de todas as políticas desenvolvidas pela empresa;
- Esclarecimentos de dúvidas em relação às políticas, normas e regulamentações vigentes;

- Apresentação do Código de Ética e demais normas e políticas da empresa no momento da contratação de novos Colaboradores e, recolhimento das assinaturas nos Termos de Adesão;
- Implementar e manter programas de treinamento aos Colaboradores, incluindo, mas não se limitando aos treinamentos de PLDFT, Segurança e Sigilo das Informações;
- Monitorar e avaliar a eficácia operacional dos controles internos implementados, através da fiscalização e acompanhamento periódico das atividades realizadas na empresa;
- Assegurar o cumprimento das normas descritas nas políticas da empresa;
- Monitorar, junto ao(s) responsável(is) por TI, das medidas adotadas na Área de Segurança da Informação;
- Aprovação e monitoramento dos terceiros contratados;
- Desenvolver projetos de melhoria contínua e adequação às normas técnicas.

IV- Procedimento de Aderência dos Colaboradores ao Manual de Regras, Procedimentos e Controles Internos, Código de Ética e demais Políticas

Ao ser contratado um funcionário/estagiário, ou no momento de entrada de um novo sócio na empresa, este receberá cópia e assinará termo de adesão aos seguintes documentos: Manual de Regras, Procedimentos e Controles Internos; Código de Ética; Política de Negociação de Valores Mobiliários (Investimentos Pessoais); Plano de Continuidade de Negócios; Política de Prevenção à Lavagem de Dinheiro; Política de Procedimentos Anticorrupção e Política de Certificação. Cópias dos documentos acima ficam disponíveis na rede da empresa, com acesso a todos os Colaboradores.

Caso seja feita alguma alteração/atualização relevante nos documentos acima, um novo termo de adesão deverá ser assinado pelo Colaborador.

Ao assinar o termo de adesão estarão todos cientes e comprometidos com as regras e princípios que regem a Paineiras Investimentos. Portanto, qualquer transgressão destas será considerada infração contratual e as ações a serem tomadas serão decididas pelo Comitê de Cumprimento de Normas. Cabe destacar que os profissionais terceirizados que possuem acesso as informações reservadas ou privilegiadas, também devem assinar ao termo de adesão supracitado.

O Manual de Regras, Procedimentos e Controles Internos, Código de Ética e demais políticas existentes, devem ser atualizados anualmente ou sempre que for necessário, e todos os Colaboradores devem assinar um novo termo de adesão.

V - Procedimento de Tratamento de Exceções e Violações

Exceções

Ao ler o presente Manual, o Código de Ética e as demais políticas da empresa, os Colaboradores terão pleno conhecimento dos princípios éticos e das regras que regem a Paineiras Investimentos. Se em algum momento existir a necessidade de aprovação de alguma exceção em qualquer das normas citadas acima, essa exceção deverá ser endereçada ao Diretor de Cumprimento de Regras, Políticas, Procedimentos e Controles Internos e da ICVM558 e será julgada pelo Comitê de Cumprimento de Normas.

Comunicação e Tratamento de Violações

Através do Código de Ética, Manual de Regras, Procedimentos e Controles Internos e demais políticas existentes da Paineiras Investimentos, todos os seus Colaboradores tomam ciência dos princípios éticos e das regras que regem a empresa. Dessa forma, fica determinado que qualquer violação ou indício de violação de legislação ou políticas da empresa, deve ser comunicada imediatamente ao Diretor de Cumprimento de Regras, Políticas, Procedimentos e Controles Internos e da ICVM558. O episódio será avaliado pelo Comitê de Cumprimento de Normas e resultará em ações internas visando à resolução do problema.

No caso de violações das normas e regulamentações sujeitas à fiscalização da CVM, a Paineiras Investimentos, através do seu Diretor de Cumprimento de Normas, no exercício de suas atribuições deverá informar a CVM no prazo máximo de 10 (dez) dias úteis da ocorrência ou identificação da violação.

É importante ressaltar que os integrantes do Comitê de Investimento e os Colaboradores que tomam decisões relativas à gestão de recursos têm o dever de reportar a ocorrência ou indício de violações, principalmente, mas não se limitando a atos ilícitos tais como: manipulação de preços, operação fraudulenta, prática não equitativa e uso de informações privilegiadas. Após a comunicação ao Diretor de Cumprimento de Normas e ao Comitê de Cumprimento de Normas, os Colaboradores que identificaram a ocorrência devem acompanhar o andamento e consequências dessa comunicação, a fim de assegurarem o cumprimento do prazo de comunicação à CVM.

O não cumprimento das normas do presente manual e do Código de Ética, ou ainda o exercício de conduta inapropriada, será julgado pelo Comitê de Cumprimento de Normas e resultará em ações internas ao infrator, que poderão ir desde uma simples advertência até o seu desligamento da empresa.

VI - Política de Treinamento

Além dos Manuais, Códigos Internos e Políticas, é importante ter uma rotina de treinamento interno. O treinamento é necessário para que os Colaboradores se mantenham atualizados e conheçam as normas contidas nos manuais e as leis aplicáveis. Todos os Colaboradores devem receber anualmente este treinamento, que é desenvolvido e ministrado pela Área de Cumprimento de Normas. As principais matérias do treinamento são:

Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT)

No treinamento de PLDFT, apresentamos a Política de PLDFT da Paineiras Investimentos e os principais pontos da Lei 9.613/98 e da Instrução CVM617 (ou Lei/regulamentação que venha a substituir) com a finalidade de estabelecer um canal informativo aos seus Colaboradores, capacitando-os quanto ao entendimento e alinhamento com a cultura e política interna relativas à PLDFT. Também são destacadas no treinamento as principais práticas ilícitas observadas no mercado de capitais (*Spoofing*, *Insider Trading*, *Front Running*, dentre outras) com o objetivo de manter os Colaboradores atualizados sobre os aspectos relevantes da regulamentação brasileira pertinente ao assunto e sobre as melhores práticas adotadas no mercado nacional e internacional.

Confidencialidade e Segurança da Informação

O respectivo treinamento engloba a importância da confidencialidade das informações detidas por todos os Colaboradores da empresa, sejam elas no meio digital ou não, além de reforçar o compromisso do cumprimento das normas estabelecidas no Código de Ética da Paineiras Investimentos. São também apresentados os principais pontos de atenção que devem ser observados por cada colaborador em relação a segurança das informações armazenadas em ambiente digital, destacando as ações de prevenção que devem ser seguidas no dia a dia das atividades realizadas, além de destacar as diretrizes de navegação na internet, a fim de manter a integridade das informações e da rede da empresa.

Anticorrupção

Devem ser apresentados os principais pontos da Lei 12.846 de 2013, os procedimentos internos de combate à corrupção e estratégias para identificação de situações de risco, além de um canal de denúncia junto à Área de Cumprimento de Normas.

VII – Regras e Procedimentos para Administração de Conflitos de Interesse

Conceitos gerais

Conflitos de interesse, potenciais ou efetivos em decorrência de investimentos, participações ou qualquer atividade desempenhada fora da empresa, detidos por qualquer dos Colaboradores, deverão ser evitados ou comunicados ao Diretor de Cumprimento de Normas para avaliação.

Conflitos de interesse reais e potenciais podem ocorrer envolvendo os Colaboradores da empresa, clientes, fornecedores e a própria empresa. Identificar, evitar ou administrar tais conflitos é crucial para o bom funcionamento da empresa. No nosso entendimento, o alinhamento de interesses entre Colaboradores e clientes é condição fundamental para o sucesso da empresa.

Alinhamento de interesses entre sócios e clientes

O alinhamento de interesses entre sócios e clientes está intimamente ligado ao motivo da criação da empresa, que surgiu com o objetivo de oferecer aos clientes o mesmo tipo de gestão que era feito com os recursos próprios dos sócios. Há um acordo societário onde os sócios devem obrigatoriamente estar investidos nos mesmos fundos e estratégias de investimento que os clientes, de acordo com regras pré-estabelecidas. Basicamente, todos os sócios devem possuir investimentos nos fundos da empresa em montante que seja proporcional à sua participação societária na empresa de gestão e com condições de liquidez mais restritas do que as oferecidas aos clientes. Dessa forma, quanto maior a participação acionária do sócio na empresa, maior deve ser seu volume de investimentos pessoais nos fundos geridos pela empresa. Nos casos onde o sócio não possua recursos suficientes para fazer frente à essa obrigação, ele deverá obrigatoriamente reinvestir parcela pré-definida da remuneração e dividendos recebidos da empresa nos fundos, até que cumpra com sua obrigação de alinhamento de interesses.

Com esta regra, buscamos minimizar qualquer potencial conflito entre clientes e tomadores de decisão, pois estes últimos possuem investimentos idênticos aos dos clientes e, em proporção de seu capital

financeiro, provavelmente muito superior ao dos clientes. O dever fiduciário de preservação de capital do cliente é incentivado pela preservação de capital do próprio gestor.

Administração dos conflitos de interesse

Regras específicas para compra e venda de valores mobiliários e para recebimento de presentes estão descritas em políticas próprias (além do próprio Código de Ética) e servem para orientar a identificação e mitigação de potenciais conflitos.

Contudo, quaisquer conflitos de interesse, sejam decorrentes de investimentos pessoais, benefícios recebidos, atividades fora da empresa ou qualquer outro assunto que possa afetar a independência e objetividade, ou interferir com os deveres fiduciários para com os clientes, deverão imediatamente ser comunicados com clareza e detalhes ao Diretor de Cumprimento de Normas, que poderá levar o assunto ao Comitê de Cumprimento de Normas para deliberação de medidas mitigatórias ou de transparência.

VIII – Política de Segregação de Atividades

Pelo foco da empresa ser exclusivo na gestão de recursos, sem atuação em outras atividades, não há necessidade de segregação física entre os Colaboradores da empresa, com exceção da área que contém os servidores e equipamentos de telecomunicações, que fica em ambiente separado com acesso monitorado por câmeras.

IX – Política de Segurança e Sigilo das Informações

Descrevemos abaixo os procedimentos adotados pela Paineiras Investimentos com o objetivo de garantir a segurança e a confidencialidade das informações geradas, armazenadas, processadas e disponibilizadas pela empresa.

Confidencialidade

Faz parte da política da empresa exigir que todos os Colaboradores, e eventuais terceirizados, mantenham a total confidencialidade das informações dos clientes (inclusive clientes indiretos, ou seja, os cotistas dos fundos geridos pela empresa) com as seguintes exceções: informações que digam respeito a atividades ilegais, informações cuja divulgação seja obrigatória por Lei ou informações cuja divulgação seja autorizada pelo cliente.

A empresa tem como premissa, proteger as informações em relação aos cotistas dos fundos geridos, que porventura tenha acesso. Também se exige dos Colaboradores, confidencialidade com relação a quaisquer informações ou análises relativas aos investimentos dos fundos geridos pela empresa a que tiverem acesso, que tenham obtido ou tomado conhecimento em função das atividades que desempenham ou desempenharam na Paineiras Investimentos.

Informação eletrônica e Segurança da Informação

Embora seja permitido o uso de comunicação digital pelos Colaboradores da empresa, inclusive redes sociais, sobretudo pela facilidade que hoje representam no acesso a informações relevantes para a gestão das carteiras, os Colaboradores devem ter domínio sobre os aspectos de segurança de suas estações e dispositivos e devem empregar todo o cuidado possível para evitar vazamentos acidentais de informações. A empresa possui procedimentos rotineiros de segurança e realiza treinamentos sobre confidencialidade e segurança das informações (conforme descrito no item VI).

Contudo, a maneira mais simples, conservadora e eficaz de proteger as informações digitais é o estabelecimento de controle de acesso às pastas e arquivos de tal sorte que as informações mais sigilosas, sobretudo aquelas referentes aos clientes, sejam acessadas somente por um grupo restrito de Colaboradores autorizados. Cabe pontuar que, por não desempenharmos a atividade de distribuição de cotas de fundos de investimento, inclusive dos fundos que gerimos, temos um contato limitado com as informações referentes aos clientes/investidores dos fundos sob gestão da Paineiras Investimentos.

A Paineiras Investimentos entende que deve garantir que as informações geradas, armazenadas, processadas e disponibilizadas pela empresa sejam confiáveis e seguras. Para que isso ocorra são adotadas as regras descritas abaixo:

1) <u>Regras de controle de acesso a informações</u>

a. Acessos a servidores, máquinas, diretórios de trabalho, são controlados por *logins* individuais;
b. Todos os controles e regras de acesso permitido são guardados num arquivo em Excel e somente têm acesso a esse arquivo os membros da Área de Cumprimento de Normas;
c. Nesse arquivo são listados todos os diretórios existentes, os grupos de trabalho que têm acesso a cada diretório e as pessoas que fazem parte de cada grupo;
d. O controle de acesso garante a segregação das informações;
e. São feitos testes de permissão de acesso para todos os usuários a fim de garantir que as regras estabelecidas sejam cumpridas;
f. Alterações, inclusões e exclusões são feitas da seguinte forma:

    i. A solicitação é feita ao Diretor de Cumprimento de Regras, Políticas, Procedimentos e Controles internos e da ICVM558, ou ao gerente da Área de Cumprimento de Normas, e estes estando de acordo com a solicitação, realizam a alteração do arquivo de regras de permissão de acesso e encaminham por e-mail ao setor de suporte (TI), que por sua vez efetua as alterações contidas no arquivo e e-mail enviados;

    ii. Para os casos de desligamentos, a Área de Cumprimento de Normas solicita imediatamente através de e-mail para o setor de suporte (TI) a troca de senha para posterior exclusão do usuário da rede e de todos os eventuais sistemas em que o mesmo tenha obtido acesso.

g. Utilização de senhas de acesso

Além dos procedimentos descritos acima, todos os arquivos importantes e confidenciais são bloqueados por senhas de acesso nos próprios arquivos. Este procedimento é realizado pelo próprio colaborador/usuário.

h. Segurança física e do ambiente

A empresa possui acesso físico controlado por seguranças 24 horas por dia, com monitoramento por câmeras com gravação de imagens e controle de acesso com identificação individual. Todos os acessos à empresa são registrados e guardados.

i. Armazenamento e recuperação de dados

O Plano de Contingência e Continuidade de negócios descreve em detalhes o parque tecnológico, os mecanismos de armazenamento e recuperação de dados e arquivos da empresa, incluindo os mecanismos de armazenamento externos e em nuvem, bem como os procedimentos adotados na gestão de incidentes.

j. Tratativa em casos de vazamentos de informações confidenciais

Nos casos de vazamento de informações consideradas confidenciais, ainda que ocorridos como consequência de ações involuntárias, o Comitê de Cumprimento de Normas deverá se reunir e avaliar os procedimentos mais adequados, incluindo a possibilidade de comunicação a reguladores bem como parceiros e clientes afetados.

X - Política de Uso de Informações Privilegiadas

Conceitos gerais

Os Colaboradores da empresa que tenham posse de informações que sejam simultaneamente materiais e não públicas e que possam afetar o valor dos investimentos deverão manter confidencialidade em relação a elas e não poderão agir ou influenciar outros a agirem com base nestas informações.

a) Conceito de informação "material"

Uma informação é considerada material se sua divulgação provavelmente tivesse um impacto no preço de algum ativo ou instrumento financeiro ou mesmo se investidores razoáveis gostariam de ter acesso a esta informação antes de tomar decisões de investimento. A especificidade, substância e a confiabilidade

da sua fonte são fatores determinantes para a caracterização de uma informação como material. Por outro lado, a passagem do tempo pode tornar uma informação, que originariamente era considerada material, em imaterial.

b) Conceito de informação "não pública"

Uma informação é considerada não pública até que seja disseminada ou esteja disponível para o mercado em geral (em oposição a um seleto grupo de investidores). Logo, especial atenção deve ser dada a informações que são abertas a pequenos grupos de investidores e que são consideradas não-públicas até que se tornem disponíveis ao público do mercado em geral.

Teoria do Mosaico

Os Colaboradores da empresa, em especial os gestores, podem usar combinações de informações que sejam públicas com outras que sejam não públicas, porém não materiais, para chegar a conclusões que tenham caráter não público e material.

Particularidades do foco da empresa

Os fundos geridos pela Paineiras Investimentos são focados na estratégia macro, utilizando principalmente posições direcionais, através de operações nos mercados de títulos públicos e derivativos de renda fixa, bolsas e moedas. Como os fundos não investem em ações ou títulos de dívidas de empresas, estamos muito menos sujeitos à possibilidade de usar informações materiais e não-públicas. Estas normalmente estão relacionadas a aspectos corporativos, como resultados e projetos de empresas, e muito raramente estão associadas aos mercados influenciados primordialmente por fatores macroeconômicos como os de taxas de juros e de câmbio.

Comunicação Interna

Independentemente da vedação à utilização de informações materiais e não-públicas e, sobretudo quando houver dúvidas em relação a natureza de informações obtidas, os Colaboradores da empresa deverão informar ao Diretor de Cumprimento de Normas sobre a posse de tais informações.

XI - Política de Segurança Cibernética

Esta política apresenta as diretrizes traçadas para a segurança cibernética da Paineiras Investimentos. As ameaças cibernéticas podem comprometer a confidencialidade, integridade e disponibilidade dos dados e sistemas da empresa. Existem inúmeras razões para que os ataques dessa natureza sejam realizados, tendo como principais motivos:

- Obter ganho financeiro;
- Roubar, manipular ou adulterar informações;
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes;
- Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança;
- Promover ideias políticas e/ou sociais;

- Praticar o terror e disseminar pânico e caos;
- Enfrentar desafios e/ou ter adoração por hackers famosos.

São utilizados diversos métodos para ataques cibernéticos, onde destacamos abaixo os mais comuns:

- Malware – softwares desenvolvidos para corromper computadores e redes:

  Vírus: software que causa danos a máquinas, redes, softwares e banco de dados;

  Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;

  Spyware: software malicioso para coletar e monitorar o uso de informações; e

  Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

  Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

  Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

  Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

  Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e

  Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Estrutura e Diretrizes de Navegação na Internet

O acesso a rede mundial de computadores (internet) é permitido para fins pessoais, uma vez que não tenha impacto nas atividades profissionais dos Colaboradores, e não comprometa o tráfego de rede da empresa. Os diretores, em conjunto com a Área de Cumprimento de Normas, realizam o monitoramento

das condições descritas. Os computadores corporativos efetuam a comunicação com a internet através de rede Ethernet ou Wi-Fi, passando por um Firewall de última geração (NGFW FortiGate 60E, com *features* de antivírus, *webfilter* e *Intrusion Prevention* habilitadas), que realiza filtro das informações transitadas. Além do Firewall, o computador dos Colaboradores está equipado com antivírus McAfee, que é mais uma barreira para as possíveis ameaças cibernéticas. A empresa conta também com rede Wi-Fi para visitantes (também filtrado pelo Firewall), na qual possui o acesso segregado da rede corporativa, reduzindo as chances de invasão ou contaminação da rede por eventuais indivíduos que não fazem parte do quadro de Colaboradores da empresa.

Em relação as regras de uso dos computadores e de navegação na internet, citamos abaixo as principais características:

- Os usuários não possuem perfil de administrador, portanto, a alteração e instalação de programas/softwares só é permitido após consulta com a Área de Cumprimento de Normas, que avalia junto a área de TI o programa em questão e sua respectiva fonte, para assegurar que não apresente ameaças a rede interna e esteja dentro dos requisitos legais para aquisição;
- Não são permitidos acesso a softwares peer-to-peer (Kazaa, BitTorrent, etc);
- Os computadores estão configurados para não permitir o acesso de qualquer dispositivo de armazenamento externo (pendrives, HD's, etc);
- Em relação aos serviços de streaming (canais de broadcast, rádios on-line, etc), os mesmos são permitidos, porém podem ser bloqueados caso prejudique a performance dos profissionais em suas atividades diárias;
- São proibidos o uso, instalação, cópia e a distribuição não autorizada de softwares que possuam direitos autorais, marca registrada ou patente na internet, assim como não licenciados.

Anualmente, a Área de Cumprimento de Normas realiza treinamento dos Colaboradores, conforme descrito no item VI, onde apresenta diretrizes para navegação em rede no ambiente de trabalho, destacando os principais pontos de atenção que devem ser observados ao acessar a internet.

A responsabilidade pelo tratamento de questões de segurança cibernética é do analista de TI, supervisionado pela Área de Cumprimento de Normas.

<u>Programa de Segurança Cibernética</u>

A seguir descrevemos o programa desenvolvido pela empresa com o objetivo de prevenir as ameaças cibernéticas. É importante ressaltar que os controles e procedimentos descritos nesta política são complementares aos apresentados na Política de Segurança e Sigilo da Informação (item IX), assim como do Plano de Continuidade de Negócios. Estes são os três pilares que compõe o funcionamento operacional da empresa.

1- Foi elaborada uma matriz onde identificamos os principais riscos internos e externos, os ativos de hardware e software, assim como dos dados e processos que necessitam de proteção. Através deste mapeamento é realizada uma avaliação dos potenciais riscos identificados e os seus possíveis impactos, sejam eles financeiros, operacionais ou reputacionais;

2- De acordo com a matriz descrita no item anterior, são estabelecidas as medidas de prevenção com objetivo de mitigar a ocorrência de ataques através dos riscos identificados. Tais medidas

podem vir pela aquisição de novos equipamentos e softwares, ou pela implementação de novas rotinas e controles internos. Citamos a seguir algumas medidas adotadas:

a. Alteração de Login

Foi estabelecida a troca periódica da senha de acesso aos computadores individuais de todos os Colaboradores, abrangendo sua periodicidade e complexidade.

b. Firewall

A empresa conta com Firewall NGFW Fortigate 60E, que faz controle de acesso à Internet através de perfis UTM avançados, acesso por VPN e balanceamento de links de internet.

c. Sistema Antivírus

O Antivírus utilizado é o McAfee, que realiza varredura ativa a fim de identificar e prevenir o acesso de elementos estranhos na rede da empresa.

3- Com o intuito de monitorar as ações de prevenção, e detectar possíveis irregularidades no ambiente cibernético, a empresa conta com algumas atividades e controles internos que buscam assegurar o ambiente de rede seguro que se é esperado. Dentre os mecanismos de prevenção e monitoramento implementados, cabe destacar:

a. Inventário de ativos

É realizado inventário anual de hardware e software, sendo possível identificar computadores não autorizados ou softwares não licenciados.

b. Monitoramento dos Controles Internos

A Área de Cumprimento de Normas é responsável pelo monitoramento da execução dos controles internos, acompanhando os resultados e a necessidade de novos planos de ação;

4- Ao detectar qualquer tipo de ameaça, esta deve ser levada ao conhecimento da Área de Cumprimento de Normas, que em conjunto com os diretores estatutários e a Área de Tecnologia da Informação, compõem o grupo responsável pela estrutura de segurança cibernética da empresa. Após as devidas tratativas, os responsáveis se reúnem com objetivo de desenhar os planos de ação que devem ser implementados. As ameaças são classificadas de acordo com os riscos que apresentarem, pois podem exigir soluções simples ou mais complexas, a depender do impacto que podem causar para a empresa.

5- Anualmente, a respectiva política é revisada pelos membros responsáveis pela estrutura de segurança cibernética da empresa. São reavaliados os riscos estabelecidos, desenhados os planos de ação e testada a eficácia do monitoramento realizado ao longo do período. Os membros expõem também os conhecimentos obtidos em relação a novas ameaças cibernéticas, a fim de debater sobre possíveis novos procedimentos ou controles a serem implementados.

XII - Procedimento de Testes Periódicos

A Paineiras Investimentos possui rotinas de controles internos com o objetivo de assegurar aderência às normas e diretrizes internas e externas. Todos os testes realizados ficam armazenados em diretório reservado aos membros do Comitê de Cumprimento de Normas, apresentados em *templates* descrevendo os procedimentos realizados, assim como suas respectivas evidências de execução. Cabe destacar, que após os responsáveis pelos testes efetuarem os devidos procedimentos, o Gerente ou Diretor da Área de Cumprimento de Normas valida as informações, garantindo a efetividade dos controles internos. Seguem abaixo resumo dos testes citados:

1. **Testes de vulnerabilidade e segurança cibernética:**

    a. Periodicidade: mensal;

    b. Descrição: é gerado um relatório de atividade do firewall existente na Paineiras Investimentos. Este relatório é extraído através de software que grava todas as transações que ocorrem através do firewall. O técnico da área de TI realiza a análise dos dados do relatório, verificando se ocorreu alguma anormalidade que deva ser investigada e tratada;

2. **Testes do controle de acesso:**

    a. Periodicidade: mensal;

    b. Descrição: o técnico da Área de Informática gera um relatório do sistema que apresenta a relação de todos os diretórios existentes na rede e os grupos de trabalho que possuem acesso às respectivas pastas. Esses dados são confrontados com a planilha de permissionamento de acesso, garantindo a segurança da informação e as regras pré-estabelecidas;

3. **Testes do Plano de Continuidade de negócios:**

    3.1 Teste de back-up site:

        a. Periodicidade anual;

        b. Descrição: a Paineiras Investimentos possui locação permanente de um site de contingência (back-up site). É realizada visita presencial no back-up site com testes de rede elétrica e de links de internet, além de testes de acesso aos sistemas de back-up de arquivos de forma remota.

    3.2. Teste de funcionamento de sistemas críticos a partir de fora da empresa

        a. Periodicidade anual;

        a. Descrição: os sistemas críticos utilizados para o processamento das ordens, apuração de resultados gerenciais, checagem de carteiras e gerenciamento de

riscos serão testados a partir de estações fora da empresa sem acesso ao servidor local.

3.3 Teste de funcionamento de links de internet:

a. Periodicidade: diária;

b. Descrição: por conta de divisão das estações de trabalho entre os principais links da empresa, temos condição de acompanhar constantemente se os links de internet estão funcionando adequadamente. Eventuais quedas dos serviços de provedores de links ficam registradas através dos chamados efetuados junto às próprias provedoras.

3.4 Teste do servidor secundário

a. Periodicidade: sob demanda;

b. Descrição: todos os arquivos utilizados para as atividades do dia a dia ficam armazenados no servidor, portanto, é possível monitorar seu funcionamento a todo momento. Em caso de queda, é possível utilizar os arquivos armazenados na nuvem (através do DropBox) ou do servidor secundário, que mantém cópia de todos os arquivos do servidor primário.

3.5 Teste do Nobreak:

a. Periodicidade: anual;

b. Descrição: anualmente é selecionado um dia no qual é forçada a queda de energia do site, a fim de garantir o correto funcionamento do Nobreak. É verificado se após a queda de energia, o Nobreak assumiu como fonte de energia e se todos os equipamentos permaneceram em correto funcionamento.

4. Teste de Backup de Arquivos

a. Periodicidade: mensal;

b. Descrição: o técnico da área de TI verifica se os arquivos obtidos pelo serviço de backup DropBox estão em conformidade com os arquivos armazenados no servidor principal, assegurando a totalidade das informações.

5. Teste dos procedimentos de Rateio e divisão de ordens:

a. Periodicidade: anual

b. Descrição: é gerado um relatório em Excel, através do sistema da corretora responsável pelo *clearing*, onde são escolhidos dias em que tenham ocorrido operações em mais de

um fundo, para que seja verificado se as ordens foram divididas de acordo com as regras previamente estabelecidas nas políticas.

6. Teste de Soft-Dollar

a. Periodicidade: anual

b. Descrição: as informações referentes às taxas operacionais pagas às corretoras com as quais possuímos vínculo são extraídas do sistema da *clearing* responsável, onde posteriormente os valores pagos àquelas com Soft Dollar são comparados as demais corretoras, a fim de demonstrar que não foram dadas vantagens indevidas.

7. Teste de Corretagem

a. Periodicidade: mensal

b. Descrição: é selecionado um dia dentro de cada mês onde são verificadas as taxas pagas às corretoras, para cada tipo de operação, comparando com os valores estabelecidos nos contratos firmados.