ZAVIT GESTÃO DE RECURSOS LTDA.

Política de *Compliance*, Controles Internos e Segregação de Atividades

SUMÁRIO

1. APRESENTAÇÃO

A presente Política de *Compliance*, Controles Internos e Segregação de Atividades ("Política") tem como objetivo estabelecer os conceitos, regras e procedimentos dos controles internos da **Zavit Gestão de Recursos LTDA** ("Zavit") na condução de suas atividades inerentes à administração de carteiras de valores mobiliários, conforme estabelecido pela Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021 ("RCVM 21"), no Código de Melhores Práticas para Administração de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("ANBIMA") ("Código ANBIMA"), e demais regulamentações aplicáveis. Este documento faz parte do compromisso da Zavit em manter altos padrões de compliance, ética e boa conduta no decorrer de suas atividades.

Responsável: Diretor de *Compliance*, Gestão de Risco e Prevenção da Lavagem de Dinheiro e do Financiamento ao Terrorismo ("Diretor de *Compliance*, Risco e PLD/FTP")

2. ABRANGÊNCIA

A presente Política aplica-se a todos os sócios, administradores, diretores, funcionários, estagiários, consultores e colaboradores terceirizados e demais pessoas que possuam cargo, função, posição e/ou relação de natureza societária, empregatícia, comercial, profissional, contratual ou de confiança com a Zavit, em razão da qual poderá ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras ("Colaboradores").

Todos os Colaboradores devem assegurar o total entendimento das leis e normas aplicáveis à Zavit e do completo conteúdo desta Política, aderindo formalmente a presente Política por meio da assinatura do Termo de Compromisso ("Termo de Compromisso"), anexo ao Código de Ética e Conduta ("Código de Ética").

A Zavit não assume a responsabilidade por Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Zavit venha a ser responsabilizada ou sofra prejuízos de qualquer natureza em razão de atos ilícitos praticados por seus Colaboradores, a Zavit exercerá seu direito de regresso contra os responsáveis.

3. ESTRUTURA DE COMPLIANCE

A presente Política possui como princípios: (i) assegurar que todos os Colabores atuem com imparcialidade e conheçam o Código de Ética, bem como as normas aplicáveis ao exercício de suas atividades; (ii) garantir a confidencialidade de informações que a Zavit e seus Colaboradores têm acesso no exercício de suas atividades; e (iii) implementar e manter programa de treinamento dos sócios e Colaboradores.

A estrutura de *Compliance* atua com plena autonomia e independência no exercício de suas funções em relação

a outros departamentos da Zavit e poderá exercer seus poderes em relação a qualquer Colaborador, tendo plena autoridade e independência para implementação das medidas necessárias, o que lhe garante total independência e autonomia

3.1. Comitê de Risco e Compliance

O Comitê de Risco e *Compliance* possui as seguintes atribuições:

Nas questões de *Compliance*: é o orgão responsável por monitorar o cumprimento de normas regulatórias e autorregulatórias, controles internos, além de questões operacionais e éticas nas atividades da gestora, e por avaliar, do ponto de vista normativo, a atividade da Zavit e dos veículos de investimento sob sua responsabilidade, a fim de garantir a aderência à legislação e normas regulatórias e autorregulatórias em vigor, bem como aprovar ações de correção nestas matérias.

Nas questões de Risco: é o orgão responsável por (i) aprovar novos instrumentos, produtos e parâmetros de uma forma geral, sob aspectos de risco, e monitorar os enquadramentos aos parâmetros estabelecidos e regulamentos de fundo; (ii) monitoramento a apresentação técnica dos riscos dos fundos de investimento sob responsabilidade da Zavit, bem como de seus ativos, em linha com as boas práticas de mercado, normas e regulamentações aplicáveis; (iii) análise dos níveis de risco dos fundos de investimento sob responsabilidade da Zavit em relação a seus limites e estratégias propostos e o uso destes limites; (iv) avaliar os riscos envolvidos no processo de gestão de recursos da Zavit, que afetam ou que podem a vir afetar os investimentos por ela geridos; (v) analisar eventuais situações de desenquadramento ocorridas no mês anterior, risco operacional, e discussão de mitigantes e melhorias; (vi) recomendar e fazer implementar medidas corretivas sempre que identificados desenquadramentos aos parâmetros aprovados.

O Comitê de Risco e *Compliance* é composto pelo Diretor de Compliance, Risco e PLD/FTP e pelo Diretor de Gestão de Recursos, pelo qual se reúne mensalmente, em conjunto com o Comitê de Investimento. No entanto, dada a estrutura enxuta da Zavit, discussões sobre os riscos dos portfólios podem acontecer com mais frequência, em particular em momentos de maior agitação nos mercados e seus respectivos ativos.

As decisões do Comitê de Risco e *Compliance* em matéria de gestão de risco deverão ser tomadas preferencialmente de forma colegiada e deverão ter obrigatoriamente o voto favorável do Diretor de *Compliance*, Risco e PLD/FTP

Em relação a medidas corretivas e medidas emergenciais, o Diretor de Risco e *Compliance* poderá decidir monocraticamente e todas as decisões serão formalizadas.

O Comitê de Risco e *Compliance* exerce suas funções de forma completamente independete das outras áreas da Zavit e poderão exercer seus poderes e autoridade com relação a qualquer Colaborador.

O Diretor de *Compliance*, Risco e PLD/FTP deverá elaborar o "Relatório de *Compliance* e Controles Internos", conforme regulamentação expedida pela CVM, para encaminhar aos órgãos de administração da Zavit até o último dia útil do mês de abril de cada ano.

O Relatório de *Compliance* e Controles Internos faz referência às operações do ano anterior ao de sua elaboração e contém: (a) os resultados dos testes periódicos de controle e aderência executados; (b) recomendações para solucionar quaisquer deficiências e cronogramas de plano relevante para soluciona-las; e (c) comentários do Diretor de *Compliance*, Risco e PLD/FTP com relação a essas deficiências ou quaisquer deficiências encontradas em verificações anteriores, se houver, bem como o plano de solução do problema ou as atuais medidas tomadas para resolver tais deficiências de acordo com o cronograma de plano estabelecido para tal propósito.

O Relatório de *Compliance* e Controles Internos ficará disponível na sede da Zavit.

4. CONTROLES INTERNOS

O Comitê de Risco e *Compliance* é responsável, quanto aos controles internos, em elaborar os planos de ação necessários a eventuais falhas de execução identificadas nos processos ou controles. Ao mesmo tempo, deve mitigar as ocorrências de ilícitos ou atividades contrárias à regulação.

A Zavit possui controles internos adequados para garantir o permanente atendimento às normas e regulamentações vigentes aplicáveis às atividades por ela desempenhadas, de forma a:

(i) Estabelecer o conceito de controles internos através do estabelecimento de cultura de *Compliance*, visando melhoria nos controles;

(ii) Realizar os reportes regulatórios periódicos exigidos pelas regulamentações aplicáveis;

(iii) Assegurar que todos os Colaboradores atuem com imparcialidade e conheçam as Políticas e normas aplicáveis às atividades desempenhadas; e

(iv) Identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores que desempenhem funções ligadas à administração de carteiras de valores mobiliários.

4.1. Procedimentos

O Diretor de *Compliance*, Risco e PLD/FTP pode a qualquer momento requisitar a estação de trabalho de um Colaborador com o propósito de efetuar exames e análises quando houver suspeitas de descumprimento dos

regulamentos internos ou atividades ilegais. A solicitação é válida apenas com a finalidade de averiguar a correta observância das normas internas e utilização adequada dos recursos disponibilizados pela Zavit.

Anualmente o Diretor de *Compliance*, Risco e PLD/FTP deverá preparar um relatório, nos moldes do item 1 acima, contendo a conclusão dos exames efetuados e recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando necessário.

4.2. Reportes Regulatórios

O Comitê de Risco e *Compliance* é o órgão responsável em cumprir as obrigações regulatórias da Zavit perante CVM, ANBIMA, Conselho de Controle de Atividades Financeiras ("COAF"), dentre outras eventualmente exigidas.

Além disso, a Zavit deve manter todos os seus dados e registros atualizados em todos os órgãos regulatórios e autorregulatórios.

Todas as políticas e códigos exigidos estão disponíveis no site da Zavit.

5. SEGREGAÇÃO DE ATIVIDADES

A política de segregação de atividades tem como objetivo garantir a segregação física das instalações entre a área responsável pela administração de carteiras de valores mobiliários e as demais atividades exercidas pela Zavit, conforme aplicável e nos termos da legislação vigente.

Os equipamentos, rede e arquivos utilizados pela Zavit são organizados de modo a garantir atuação independente pelas diferentes áreas e segregação total de suas atividades. Tal organização consiste na utilização de um sistema operacional de tecnologia da informação para o controle e bloqueio de informações, a fim de preservar as informações confidenciais e permitir a identificação de pessoas que tenham acesso.

O acesso aos sistemas utilizados pela Zavit é restrito, regido por perfis de acesso e controlado por senhas e registros de log. Da mesma forma, toda a informação em guardada em nuvem através do Dropbox, com controle de acesso pelos colaboradores.

O Comitê de Risco e *Compliance* deverá monitorar os acessos concedidos aos Colaboradores, e cabe ao supervisor a responsabilidade pela análise da necessidade e verificação da correta utilização dos acessos e ferramentas concedidas.

A Zavit não realiza nenhuma outra atividade para além da atuação como gestora de recursos. Entretanto, caso a gestora decida iniciar outras atividades, a presente Política será revisitada e atualizada, sob responsabilidade do Diretor de *Compliance*, Risco e PLD/FTP.

6. TREINAMENTO

Como parte de seu programa de controles internos, o Comitê de Risco e *Compliance* procederá com os treinamentos sobre esta Política e todas as demais políticas e códigos da Zavit a todos os Colaboradores.

O treinamento ministrado pelo Comitê de Risco e *Compliance* aborda as atividades da Zavit, assim como sua cultura, observação das leis e normas que abarcam sua atividade e sobre o conteúdo de todas as Políticas e Códigos da Zavit. Serão ministrados treinamentos com o objetivo de comunicar atualizações às Políticas ou ao Manual, bem como reforçar na equipe a compreensão e a necessidade de observância das normas e regras acima mencionadas.

O treinamento será ministrado bianual a todos os Colaboradores da Zavit e aplicado quando no ingresso de novos Colaboradores na gestora. Sua frequência dependerá da necessidade identificada no dia a dia da Zavit, em especial, quando de sua alteração e em decorrência de mudanças na legislação ou fato relevante.

O treinamento se dará, preferencialmente, online mas também com a possibilidade de ser por meio de reuniões em toda a gestora, distribuição de materiais escritos ou orientação fornecida por e-mail.

O Diretor de *Compliance*, Risco e PLD/FTP será responsável por manter um registro em aquivo interno, de quaisquer orientações ou materiais escritos fornecidos durante os treinamentos.

7. POLÍTICA DE CERTIFICAÇÃO CONTINUADA

A Zavit está sujeita as disposições do Código de Certificação e o Código ANBIMA de Regulação e Melhores Práticas Programa de Certificação Continuada ("Código ANBIMA de Certificação"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

Apesar da Zavit não realizar a distribuição das cotas dos fundos por ela geridos, sua atuação como gestora de recursos de terceiros torna-se obrigatória a obtenção da Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE"), aplicável aos Colaboradores que atuem efetivamente na Gestão de Recursos de Terceiros e tenham alçada/poder discricionário de investimento (compra e venda) dos ativos dos fundos de investimentos sob gestão ("Atividade Elegível").

O profissional contratado (não certificado) receberá, no momento da contratação, as instruções sobre a necessidade de certificação, a depender da atividade que exercerá dentro da Zavit. O Comitê de Risco e *Compliance* efetuará os devidos registros junto às entidades pertinentes.

O profissional que não apresentar a certificação necessária, deve ser impedido de iniciar as suas atividades. Se completado o prazo estabelecido pelo Comitê de Risco e *Compliance* para a retirada da certificação e o profissional não tiver apresentado, cabe ao Comitê de Risco e *Compliance* a comunicação ao responsável da área

de que o profissional ainda não está habilitado a exercer as atividades pelas quais foi contratado.

Cabe ao responsável pela área que fez a contratação do novo Colaborador, a definição sobre o eventual remanejamento para uma outra área ou a sua manutenção em atividades não elegíveis, devidamente supervisionado por funcionários que possuam a certificação.

Caso o Colaborador esteja exercendo Atividade Elegível e a certificação não esteja vencida a partir do vínculo do Colaborador com a Zavit, o prazo de validade da certificação CGE será indeterminado, enquanto perdurar o seu vínculo com a Zavit. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGE na Gestora, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a Atividade Elegível.

Desse modo, o Comitê de Risco e *Compliance* assegurará que os Colaboradores que atuem na Atividade Elegível participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos nesta Política e nos termos previstos no Código ANBIMA de Certificação

8. PLANO DE CONTINUIDADE DE NEGÓCIOS

O objetivo do "**Plano de Contingência**" da Zavit é garantir a linearidade das operações, por meio de medidas a serem tomadas para evitar ou diminuir o impacto negativo que um "Evento de Contingência", como crises econômicas, pandemias, falhas operacionais, desastres naturais, por exemplo, podem causar.

Caso ocorra um Evento de Contingência, a estratégia de continuidade a ser adotada pela Zavit poderá conter, entre outras, as seguintes soluções para viabilizar a manutenção de seus negócios:

(i) controle de acesso as dependências por meio do uso de crachás e/ou chaves;
(ii) controle de acesso aos sistemas da Zavit por meio de login e senha;
(iii) revezamento de colaboradores com a aplicação do modelo híbrido de trabalho (presencial e *home office*);
(iv) planejamento de sucessão das atribuições dos colaboradores;
(v) uso de recursos humanos terceirizados;
(vi) contratação de novas tecnologias da informação e segurança da informação; serviços de assinatura eletrônica; e serviços de guarda de documentação;
(vii) manutenção dos sistemas por meio de notebooks com bateria interna para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da Zavit; e
(viii) prédio onde se localizam os provedores em nuvem da Zavit (azure microsoft e Drop box) contam com geradores próprios.

Além disso, para garantir a continuidade das atividades, a Zavit realiza o *backup* das informações digitais e dos sistemas existentes no escritório armazenados em (i) disco externo ao servidor de produção; ou (ii) em sistemas de armazenamento em nuvem.

Por fim, convém ressaltar que a Zavit conta com uma estrutura de tecnologia da informação compatível com o volume e complexidade de suas operações, bem como com sistemas contratados de terceiros que asseguram proteção integral contra adulterações e permitem a realização de auditorias e inspeções ,para arquivamento, *firewall* e VOIP centralizado em servidor com controle total de monitoramento e bloqueio de acesso.

Na hipótese de ocorrência do vazamento de algum dado confidencial interno da Zavit, o Comitê de Risco e *Compliance* deverá verificar a potencial extensão dos danos, bem como avaliar a necessidade de comunicação privada ou pública do vazamento das informações, a reavaliação das medidas de segurança da informação e, caso necessário, comunicar o vazamento aos órgãos competentes.

Após a ocorrência de qualquer Evento de Contingência, o Comitê de *Compliance* deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

8.1. Testes de Contingência

Os "Testes de Contingência" da Zavit têm como objetivo avaliar o presente Plano e se ele é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Zavit, de modo a manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotado pelo Plano, bem como se o Plano pode ser ativado tempestivamente considerando o Evento de Contingência.

Os Testes de Contingência serão realizados no mínimo a cada 12 (doze) meses, ou em prazo inferior se exigido pela regulação em vigor e/ou se constatada necessidade pela Zavit.

Os testes serão:

(i) Testes das baterias dos notebooks, para verificar o status de funcionamento e do tempo de suporte das baterias com carga;
(ii) Acesso aos sistemas e aos e-mails remotamente;
(iii) Acesso aos dados armazenados externamente e/ou em nuvens; e
(iv) Testes e atualizações nos equipamentos dos Colaboradores assegurando seu bom funcionamento.

9. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A presente Política de Segurança da Informação, visa garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual, quanto a confidencialidade, disponibilidade e integridade das

informações da Zavit, dos Colaboradores, dos clientes e do público em geral.

Nos termos desta Política de Segurança da Informação:

(i) A confidencialidade garante que as informações tratadas pela Zavit e seus Colaboradores sejam restritas a um grupo restrito de usuários autorizados, impedindo a exposição de dados restritos e acessos não autorizados;
(ii) A disponibilidade das informações aos usuários autorizados sempre que necessário; e
(iii) A integridade garante a veracidade e completude das informações, de forma que elas sejam íntegras e sem alterações à dados por pessoas não autorizadas que possam efetuar modificações não aprovadas.

Para garantir a segurança da informação na Zavit o Comitê de Risco e *Compliance* realiza o monitoramento das atividades de gestão e identificação de eventuais inconformidades por meio do acesso à relatórios elaborados pelas demais áreas da gestora para rastrear a atividade de investimento da Zavit.

O Comitê de Risco e *Compliance* tem acesso a todas as mensagens trocadas via e-mail e deve ficar atento quanto aqueles contendo anexos de arquivos de grandes tamanhos. Em observância a segurança da informação, toda rede computacional da Zavit está protegida por firewalls, antivírus e filtros de spans. Testes periódicos são feitos com propósito de avaliar possíveis vulnerabilidades e falhas nos sistemas operacionais, softwares e rede. São feitos (i) testes de penetração, de modo a identificar possíveis falhas sistêmicas e (ii) armazenamento de informações confidenciais protegidas por criptografia.

O Comitê de Risco e *Compliance* possui acesso irrestrito aos arquivos do servidor da Zavit, contudo, cada Colaborador possui acesso apenas no que se referem às pastas e aos arquivos relacionados à sua atividade. Além disso, o Comitê de Risco e *Compliance* deve apurar se os acessos estão adequados e sendo respeitados pelos Colaboradores, assim como investigar os acessos não autorizados.

As senhas, os acessos pessoais e as informações confidenciais devem ser guardadas e utilizadas adequadamente pela Zavit e pelos Colaboradores .e podem ser requisitados pelo Comitê de Risco e *Compliance* quando da necessidade de alguma inspeção.

O Comitê de Risco e *Compliance* é responsável por divulgar amplamente a presente Política de Segurança da Informação e garantir que os Colaboradores entendam e sigam suas diretrizes. Toda violação ou desvio, intencional ou não, como instalação de vírus de informática, uso de software ilegal e tentativas de acesso a informações restritas, por exemplo, é investigada pelo Comitê de Risco e *Compliance* para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.

10. POLÍTICA DE SEGURANÇA CIBERNÉTICA

Em linha com a Política de Segurança da Informação, a presente Política de Segurança Cibernética visa garantir a aplicação de um efetivo programa contra os ataques cibernéticos que ameaçam a confidencialidade, a integridade e a disponibilidade de dados ou dos sistemas da Zavit pelos quais acarretam riscos, significativos, a imagem, dano financeiro, vantagem concorrencial, riscos operacionais, dentre outros ("Ameaças Cibernéticas").

O programa para garantir a cibersegurança na Zavit busca: (i) a identificação e avaliação de riscos; (ii) estabelecer as ações de prevenção e proteção dos riscos previamente identificados; (iii) estabelecer monitoramentos e testes internos de segurança para a identificação de Ameaças Cibernéticas em tempo hábil; e (iv) a criação de um plano de respostas às Ameaças Cibernéticas, eventualmente, sofridas pela Zavit.

10.1. Avaliação de Riscos

A avaliação de riscos deverá ser realizada com base nas premissas de ameaças abaixo identificadas:

(i) Malware – software projetado na intenção de corromper tanto computadores quanto redes:

- **a)** Vírus: Software que causa danos diretos à máquina, à rede, ao software ou até o banco de dados;
- **b)** Cavalo de Tróia: vem oculto dentro de outros softwares, criando uma porta de invasão aos sistemas;
- **c)** Espiões: software que coleta e monitora o uso de informações, repassando-as a terceiros; e
- **d)** Ranomware: software que bloqueia acesso aos bancos de dados, normalmente sendo solicitado um valor de resgate para nova concessão do acesso aos próprios sistemas.

(ii) Engenharia Social – métodos de manipulação para obter quasiquer informações sensíveis, como senhas ou até dados pessoais e bancários.

- **a)** Pharming: direciona para um site fraudulento, sem que se perceba o teor mal-intencionadodo site;
- **b)** Phishing: links de e-mail, fingindo ser uma pessoa ou empresa confiável, enviando e-mails oficiais de modo a tentar obter informações confidenciais;
- **c)** Smishing: finge ser uma pessoa ou empresa confiável, tentando obter informações confidenciais através de mensagens de texto;

(iii) Acesso pessoal: pessoas localizadas em locais públicos como bares, cafés e restaurantes que recolhem qualquer tipo de informação que possa ser utilizada posteriormente para um ataque cibernético

(iv) DDoS (ataque de negação de serviços) e ataques de botnet – ataques destinados a negar ou atrasar o acesso aos serviços e sistemas da instituição. O ataque de botnet consiste em muitos computadores infectados

usados para criar e enviar vírus ou spam, inundando uma rede com mensagens que resultam em uma sobrecarga do sistema, resultando em uma lentidão ou queda total dos sistemas.

10.2. <u>Ações de Prevenção e Proteção</u>

Em busca da mitigação das Ameaças Cibernéticas, a Zavit adota as seguintes diretrizes:

(i) As informações da Zavit, dos Colaboradores, dos clientes e do público em geral devem ser tratadas de forma ética, sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

(ii) A senha e login para acesso aos dados contidos em todos os computadores e equipamentos da Zavit, bem como nos e-mails que possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do equipamento ou do sistema e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. O Colaborador se responsabiliza pessoalmente por qualquer conduta realizada por meio de suas credenciais de acesso aos equipamentos e sistemas da Zavit.

(iii) Acesso a dados confidenciais são restritos a determinados usuários e bloqueados com base no login de usuário. Acessos indevidos devem ser comunicados imediatamente ao Comitê de Risco e *Compliance*;

(iv) Cada usuário é responsável pelo uso dos recursos que lhe foram entregues e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas de *softwares* instalados;

(v) Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na Zavit ou para outras situações formalmente permitidas;

(vi) É proibida a conexão de equipamentos na rede da Zavit que não estejam previamente autorizados.;

(vii) Equipamentos eletrônicos corporativos ou nos quais circulem informações internas ou confidenciais da Zavit devem ter seu acesso protegido por, no mínimo, login e senha;

(viii) Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade;

(ix) A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função;

(x) Apenas os equipamentos e softwares disponibilizados e/ou homologados autorizados pela Zavit

podem ser instalados e conectados à rede;

(xi) Solicitar alterações de senha sempre que exista a possibilidade de ter sido comprometida;

(xii) Em caso de não funcionamento do *software* antivírus instalado em cada computador, deverá o usuário notificar prontamente a equipe de Tecnologia da Informação ("TI");

(xiii) Equipamentos particulares e/ou privados dos Colaboradores não devem ser usados para armazenar ou processar informações relacionadas aos negócios da Zavit, e só podem ser conectados à rede Wi-Fi de visitantes, exceto em casos em que o Plano de Contingência requeira essa prática e em que exista autorização explícita do Comitê de Risco e *Compliance*;

(xiv) Os Colaboradores deverão manter arquivada na rede da Zavit toda e qualquer informação, bem como documentos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos regulatórios em torno de possíveis atuações da Zavit em relação à esta Política e as atividades desenvolvidas pela Zavit;

(xv) A senha da rede de internet principal da Zavit e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários; e

(xvi) Diariamente são feitos *backups* dos arquivos salvos em nuvem em um local diferente do escritório da Zavit.

10.3. <u>Monitoramento e Testes</u>

Além das ações de prevenção e proteção estabelecidas, para garanir a segurança cibrnética a Zavit realiza os seguintes monitoramentos periódicos e testes internos de segurança para a identificação de Ameaças Cibernéticas em tempo hábil:

(i) Atualização de inventários dos hardwares e *softwares* da Zavit, junta a verificação frequente para a identificação elementos estranhos à instituição, inclusive em relação ao momento de acesso aos sistemas e/ou trabalho remoto prolongado, bem como computadores não autorizados ou *softwares* não licenciados;

(ii) Atualização constante dos sistemas operacionais e *softwares* utilizados para as atividades da Zavit;

(iii) Monitoramento diário das rotinas de *backup* com testes regulares da restauração dos dados;

(iv) Testes de invasão externa e *phishing*;

(v) Análises periódicas das vulnerabilidades na estrutura tecnológica da Zavit, ou sempre que houverem mudanças significativas em tal estrutura.

(vi) Testes periódicos do plano de resposta a incidentes, na forma como mencionado abaixo, simulando os cenários especificados durante sua criação; e

(vii) Analise regular dos logs e trilhas de auditoria criadas, de forma a permitir a rápida identificação de ataques, internos e externos, bem como o uso de ferramentas de centralização e correlação de logs.

10.4. Resposta a incidentes

A Zavit estabelece que o Diretor de *Compliance*, Risco e PLD/FTP e o Comitê de Risco e *Compliance* são responsáveis pelo plano de ação quanto às respostas aos incidentes, contudo atuam com o envolvimento das demais áreas da gestora, incluindo a alta gestão, vez que se trata de um risco operacional ("Governança Cibernética").

A Governança Cibernética (i) conduzirá, ou designará terceiro para conduzir, avaliações periódicas dos riscos e identificação das Ameaças Cibernéticas, vulnerabilidades e potenciais consequências comerciais, além da segurança física dos sistemas; (ii) realizar testes periódicos de seus procedimentos de detectação de Ameaças Cibernéticas e respostas a incidentes; (iii) monitoramento dos principais prestadores de serviços terceirizados da gestora que tenham acesso a dados confidenciais e sensíveis.

Os Colaboradores são responsáveis por informar qualquer suspeita de invasão, atividade ou comportamento adverso do sistema, perda, roubo ou revelação/desvio involuntário de informação confidencial à Governança Cibernética, que na forma do item 8, deverá verificar a potencial extensão dos danos e avaliar a necessidade de comunicação aos órgãos competentes, além da reavaliação das medidas de segurança.

Imediatamente a qualquer incidente ou violação da rede da Zavit, a área de Governança Cibernética deverá se reunir e avaliar o risco, determinar quais eventos requerem notificação ou alertas aos seus profissionais, prestadores de serviços terceirizados ou reguladores.

No caso de prejuízo real aos ativos sob gestão da Zavit, serão documentados os fatos pertinentes acerca do prejuízo, o montante da perda e o reembolso pela cobertura de seguro de cibersegurança, caso este seja contratado pela Zavit para cobertura de eventuais ataques cibernéticos.

11. POLÍTICA DE CONTRATAÇÃO DE TERCEIROS

A presente Política de Contratação de Terceiros em nome dos Fundos de Investimentos geridos pela Zavit visa estabelecer as regras e critérios pelos quais a Zavit, como gestora de recursos irá realizar a contratação de

corretoras de títulos e valores mobiliários e as corretoras de câmbio ("Terceiro") ("Contratação de Terceiros").

O Comitê de Risco e *Compliance* poderá delimitar a quais Colaboradores a presente Política de Contratação de Terceiros se aplica, observando as atividades cotidianas de cada um e a coerência com seu conteúdo.

Para terceiros, prestadores de serviços, pelo qual sua contratação não tenha sido realizada em nome dos Fundos de Investimentos geridos pela Zavit, a aplicação das seguintes diretrizes é facultativa.

11.1. Procedimento para a Contratação

O Comitê de Risco e *Compliance* deverá realizar, preliminarmente a Contratação de Terceiros, processo de *due diligence* que consiste na verificação da idoneidade da empresa com consultas em sites de busca, bem como em órgãos governamentais e reguladores, assim como, a avaliação da capacidade de atendimento do Terceiro em cumprir a demanda solicitada, com o devido preenchimento do questionário de *due diligence* modelo ANBIMA.

Após devida análise, o Comitê de Risco e *Compliance* informará suas conclusões com a devida classificação de risco do Terceiro e possíveis situações de conflitos de interesses com a Zavit ou com os fundos de investimentos sob sua responsabilidade de gestão, ao Diretor de *Compliance*, Risco e PLD/FTP, que será responsável pela decisão da contratação.

Aprovada a contratação pelo Diretor de Risco e *Compliance*, e observada eventual aprovação em assembleia geral de cotistas, a área contratante poderá ceberar o respectivo contrato, obedecendo as diretrizes das políticas e códigos da Zavit.

Após a contratação, a Zavit fornecerá cópias de todas suas políticas para que o Colaborador recém contratado tenha conhecimento de suas diretrizes e, caso aplicável, monitorará sua atividade com os fundos geridos. Ainda, caso aplicável, informará aos cotistas e, ao mercado da contratação efetuada.

12. REVISÃO DA POLÍTICA

A presente Política será revisada a cada 2 (dois) anos, ou a qualquer momento, sempre que se observarem mudanças relevantes nas normas, regras, formato das atividades ou em qualquer outro aspecto intrínseco ao dia a dia da Zavit, nos termos da regulamentação e diretrizes aplicáveis.

Versão	Data de Atualização
1ª	Junho/2022
2ª	Agosto/2023

* * *