Política de Regras, Procedimentos e Controles Internos

GTIS Partners Brasil Gestão, Consultoria em Investimentos e Participações Ltda.

outubro de 2024

Versões Anteriores:
Maio de 2022
Novembro de 2020

1 INTRODUÇÃO

Esta Política de Regras, Procedimentos e Controles Internos ("**Política**") visa a definir os princípios, conceitos, valores e procedimentos para coordenar os padrões éticos, profissionais e legais de práticas, bem como assegurar, através de um controle interno adequado, o cumprimento permanente das regras, políticas e regulamentos atuais relacionados aos diferentes tipos de investimentos e à atividade de gestão de carteiras de valores mobiliários da GTIS Partners Brasil Gestão, Consultoria em Investimentos e Participações Ltda. "("**GTIS Brasil**") no exercício de suas atividades de gestão de recursos de terceiros e/ou consultoria de valores mobiliários, de acordo com a Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("**Resolução CVM 21**").

A GTIS Brasil é uma subsidiária da GTIS Partners, LP, empresa de investimentos em ativos reais com sede em Nova York, com escritórios em São Paulo, Brasil; Los Angeles, Califórnia; São Francisco, Califórnia; Atlanta, Geórgia; Charlotte, Carolina do Norte; Phoenix, Arizona; Dallas, Texas; Houston, Texas; e Munique, Alemanha ("**Grupo GTIS**").

Esta Política será aplicável a todos os profissionais empregados da GTIS Brasil e envolvidos nas áreas de Gestão de Recursos, Controles Internos e *Compliance* da GTIS Brasil incluindo, sem limitação, qualquer sócio, diretor, conselheiro, gerente, empregados, trainees e estagiários ou outra pessoa que possua status similar ou que desempenhe funções similares ("**Pessoas Supervisionadas**").

Além dos procedimentos e ações definidos nesta Política, o cumprimento expresso e integral das leis, regras, regulamentos e políticas globais do Grupo GTIS, aplicáveis no Brasil e em outros países onde o Grupo GTIS possa estar presente é responsabilidade de todas as Pessoas Supervisionadas.

2 DEFINIÇÕES

Todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética da GTIS Brasil.

3 PROTEÇÃO DAS INFORMAÇÕES DE PROPRIEDADE EXCLUSIVA DA EMPRESA E DO INVESTIDOR

Procedimentos para a Divulgação Adequada de Informações

À luz das disposições de sigilo estabelecidas no Código de Ética, salvo se adequado no contexto de suas responsabilidades profissionais, uma Pessoa Supervisionada não poderá revelar a qualquer pessoa não associada à GTIS Brasil exceto: (i) àqueles envolvidos em uma operação ou com direito às informações em nome de um investidor; (ii) àqueles que prestem serviços jurídicos, contábeis, administrativos ou outros serviços ao respectivo fundo ou correntista; (iii) conforme exigido por lei; ou (iv) especificamente solicitado por tal investidor qualquer informação relativa aos investidores, incluindo dados pessoais fornecidos à GTIS Brasil por qualquer investidor, agente ou contratado; listas e arquivos de investidores ou outras informações do investidor; registros comerciais da GTIS Brasil, informações de empregados, informações financeiras, software, licenças, contratos, arquivos de computador e planos de negócios; modelos, pesquisa de propriedade exclusiva, direitos autorais ou outros materiais pagos por um fundo ou pela GTIS Brasil; e as análises e outros dados ou informações de propriedade exclusiva da GTIS Brasil. Todas essas informações, sejam ou não materiais, são estritamente confidenciais e não podem ser

divulgadas. As Pessoas Supervisionadas também não violarão as disposições de qualquer acordo de confidencialidade do qual a GTIS Brasil ou a Pessoa Supervisionada seja parte.

As Pessoas Supervisionadas tomarão precauções especiais para não divulgar informações relativas a recomendações ou possíveis operações que ainda não estejam fechadas ou que estejam sendo consideradas, exceto (i) conforme seja necessário ou apropriado no contexto das atribuições do seu trabalho; (ii) em conjunto com um relatório regular aos investidores; (iii) em conjunto com qualquer relatório a que as pessoas tenham direito devido a disposições de um acordo de gestão de investimentos ou outro documento similar que governe o funcionamento da GTIS Brasil; (iv) conforme exigido por lei (nesse caso, mediante notificação ao Diretor de *Compliance*); e (v) após a informação estar de outra forma disponível ao público.

A GTIS Brasil tem para com todo e qualquer investidor um dever primordial de lealdade. Esse dever inclui não se apropriar indevidamente de informações e/ou estratégias desenvolvidas para uso na administração do capital GTIS Brasil com o objetivo de utilizá-las em negociações pessoais (ou negociações para outras contas) de tais Pessoas Supervisionadas. De maneira geral, as políticas de negociações pessoais da GTIS Brasil encontradas no Código de Ética devem evitar tal apropriação indevida, mas caso qualquer Pessoa Supervisionada acredite estar em posição de lucrar com o uso de informações específicas que recebeu ou que foram geradas por conta da gestão dos investimentos da GTIS Brasil, tal Pessoa Supervisionada não deverá executar a operação em questão.

4 CLASSIFICAÇÃO DE DADOS

4.1 Categorias de Classificação de Dados

A GTIS Brasil acredita que as proteções de segurança da informação devem ser proporcionais à classificação dos dados a serem protegidos (*i.e.,* quanto mais sensíveis ou cruciais forem os dados forem para o negócio, maiores devem ser as proteções). A GTIS Brasil adotou uma política de classificação de dados que via de regra enquadra seus dados em uma das seguintes categorias:

(i) Dados Públicos (Dados da Alerta Verde): Dados públicos são dados que a GTIS Brasil pode disponibilizar ao público em geral. Isso inclui, por exemplo, informações disponíveis no website da GTIS Brasil acessíveis ao público, conteúdo acessível ao público em páginas de mídias sociais ou perfis gerenciados pela GTIS Brasil e informações acessíveis pelo público em geral sobre a GTIS Brasil através de seus arquivamentos regulamentares.

(ii) Dados Internos da Empresa (Dados da Alerta Amarelo): Esses incluem dados sobre os negócios ou operações da GTIS Brasil que, embora não necessariamente confidenciais, garantem algum certo grau de privacidade. Exemplos incluem, mas não se limitam, às informações sobre os controles internos ou procedimentos operacionais da GTIS Brasil, e informações sobre vendedores, fornecedores, contratados e investimentos ou qualquer informação cuja divulgação possa ser exigida por lei ou por autoridade competente.

(iii) Dados Confidenciais (Dados de Alerta Vermelho): Esses incluem dados do mais alto grau de sensibilidade e criticidade de ação para a GTIS Brasil e seus negócios. Exemplos incluem, mas não se limitam, a quaisquer Dados Pessoais sobre os investidores, investidores atuais e Pessoas Supervisionadas; informações de recursos humanos detidos pela GTIS Brasil (tais como nomes, data de nascimento, números de previdência social, informações de conta pessoal de corretagem, informações sobre folha de pagamento e

informações médicas); informações ou pesquisas relativas aos valores mobiliários, empresas ou investimentos feitos ou sob consideração pela GTIS Brasil; dados utilizados em controles de acesso; e informações que devam ser mantidas em sigilo por força de obrigações contratuais ou de leis ou regulamentos federais, estaduais ou locais ("**Dados Confidenciais**").

(iv) Dados Pessoais (Dados de Alerta Vermelho): qualquer informação relativa a uma pessoa identificada ou identificável ("**Dados Pessoais**").

O acesso da Pessoa Supervisionada é devidamente segmentado por classificações de dados com base em sua necessidade de conhecê-los e em suas atribuições profissionais. O Diretor de *Compliance* que trabalhar com o Diretor de Tecnologia analisará o acesso da Pessoa Supervisionada a essas categorias de classificação de dados com base na necessidade de conhecê-los, dando especial atenção àquelas que terão acesso a Dados Confidenciais, Dados Pessoais e privilégios elevados.

4.2 Titularidade de Dados

Com exceção do material claramente de propriedade de terceiros, tais como seus dados pessoais confidenciais, a GTIS Brasil é a legítima titular de todas as informações comerciais armazenadas ou transmitidas através de seus sistemas. A menos que a GTIS Brasil tenha celebrado um acordo específico por escrito, todas as informações comerciais desenvolvidas enquanto uma Pessoa Supervisionada estiver empregada pela GTIS Brasil são de propriedade da GTIS Brasil.

Pessoas Supervisionadas, fornecedores e quaisquer outros terceiros não poderão copiar software fornecido pela GTIS Brasil para qualquer meio de armazenamento, transferir tal software para outro computador ou divulgar tal software a terceiros externos sem permissão prévia do Diretor de *Compliance* e/ou Diretor Tecnologia.

4.3 Classificação e Manuseio da Informação

As informações da GTIS Brasil, e as informações que tenham sido confiadas à GTIS Brasil, devem ser protegidas de forma compatível com o seu grau de sensibilidade. Medidas de segurança devem ser empregadas independentemente do meio no qual a informação está armazenada, dos sistemas que a processam ou dos métodos através dos quais ela circula. A informação deve ser protegida de forma compatível com sua classificação, não importando o estágio do ciclo de vida desde sua criação até sua destruição. Por exemplo, documentos sensíveis em papel devem ser picotados, e os registros eletrônicos sensíveis devem ser protegidos conforme necessário. As Pessoas Supervisionadas não poderão compartilhar documentos com qualquer pessoa fora da GTIS Brasil ou conceder a qualquer delas acesso à rede GTIS Brasil sem o consentimento do Diretor de *Compliance* e/ou Diretor Tecnologia.

5 CONTROLE DE ACESSO À INFORMAÇÃO E PROTEÇÃO DE DADOS

5.1 IDs de usuário e Senhas

Para garantir que o acesso às informações e à rede da GTIS Brasil seja limitado às Pessoas Supervisionadas e afiliados externos com necessidade de acesso, a GTIS Brasil exige que cada indivíduo que acesse os sistemas de informação da GTIS Brasil tenha um ID de usuário único e uma senha exclusiva ("**Usuário"**). Esses IDs de Usuário são utilizados para restringir os privilégios do sistema com base em atribuições de trabalho, responsabilidades de projeto e outras atividades comerciais. Cada usuário é pessoalmente responsável por seu ID de usuário e senha.

Todos os computadores e dispositivos que acessem o e-mail e/ou dados da GTIS Brasil devem ter uma senha definida para todas as contas de Usuário e devem ser configurados para bloquear automaticamente a tela quando deixados sem supervisão após um determinado período. Além disso, após dez tentativas de *login*, as contas de usuário serão bloqueadas.

A GTIS Brasil poderá, a seu critério, limitar a capacidade de um empregado ou de um destinatário de imprimir, encaminhar ou salvar um documento. Quando necessário, a GTIS Brasil criptografará dados, documentos, e-mails ou anexos sensíveis, conforme o Item 5.2 abaixo.

Os computadores da GTIS Brasil são preparados com uma configuração básica padrão de hardware e software. Os empregados da GTIS Brasil devem solicitar permissão ao Diretor de *Compliance e/ou* Diretor Tecnologia para alterar essa base padrão. A GTIS Brasil reconhece que os direitos de acesso podem ser atualizados ou encerrados com base em várias mudanças de empregados ou sistemas.

5.2 Criptografia

Criptografia significa o processo de transformação de informações, utilizando um algoritmo, para tornar tais informações ilegíveis para qualquer outra pessoa que não aqueles que tenham uma necessidade específica de conhecê-las. A GTIS Brasil poderá utilizar software de criptografia que permita às Pessoas Supervisionadas garantir a segurança dos dados da GTIS Brasil através do uso de e-mail e outros métodos de transmissão, como por exemplo, através de um portal on-line. Além disso, todos os computadores, laptops, *tablets* e telefones celulares dos empregados são criptografados, tornando os dados ilegíveis em caso de perda ou roubo. Nenhum software de criptografia instalado em equipamentos fornecidos pela GTIS Brasil pode ser adulterado, desabilitado ou alterado de qualquer forma.

5.3 Acesso Remoto

Todas as Pessoas Supervisionadas têm capacidade de acessar a rede da GTIS Brasil ao trabalhar remotamente através do portal GTIS Brasil. A GTIS Brasil emprega um duplo fator de autenticação para *login* remoto na rede GTIS Brasil. Além disso, os usuários e suas credenciais são mantidos e monitorados pelo diretor de tecnologia para garantir que todos os usuários estejam atualizados e que nenhum usuário apresente risco para o sistema GTIS Brasil. As Pessoas Supervisionadas que acessem a rede GTIS Brasil remotamente estão obrigadas a instalar software de proteção contra vírus em tais computadores domésticos ou dispositivos de acesso remoto. Mediante solicitação, as Pessoas Supervisionadas podem precisar apresentar seu dispositivo ao diretor de tecnologia para inspeção como condição de acesso remoto.

Todos os smartphones/*tablets* que se conectam aos serviços de comunicações da GTIS Brasil exigem senha de no mínimo de 4 dígitos, reconhecimento de impressão digital ou reconhecimento facial para destravar o dispositivo para utilização de tais serviços. Enquanto o e-mail GTIS Brasil estiver instalado em um dispositivo de uma Pessoa Supervisionada, esta não poderá desativar a função de senha. As Pessoas Supervisionadas serão avisadas de que quando utilizarem um dispositivo pessoal para se conectar ao sistema de e-mail, a GTIS Brasil terá controle total sobre a capacidade de limpar os dados de tal dispositivo a qualquer momento para fins de segurança.

A GTIS Brasil se reserva o direito de conduzir inspeções surpresa dos usuários com privilégios de acesso remoto. Tais inspeções surpresa podem incluir visitas a sites remotos e inspeção do conteúdo de um computador utilizado para acessar os sistemas GTIS Brasil.

5.4 Detecção de Atividade Não Autorizada

Além de sólidas políticas para evitar uma ameaça à segurança cibernética de sua rede, a GTIS Brasil também adotou políticas e procedimentos destinados a detectar atividades não autorizadas em sua rede. A GTIS Brasil busca regularmente a presença de usuários, dispositivos, conexões e software não autorizados em sua rede e em dispositivos móveis de seus empregados. No âmbito dessa política, a GTIS Brasil atualizará os sistemas operacionais e software em sua rede quando necessário; tais atualizações ajudarão a reduzir as vulnerabilidades da rede, uma vez que as atualizações frequentemente abordam ameaças conhecidas ou antecipadas.

A GTIS Brasil usará programas para auxiliar na prevenção e detecção de software não aprovado e software mal-intencionado, impedindo-os de rodar na rede GTIS Brasil e nos dispositivos móveis sincronizados dos empregados. A GTIS Brasil monitorará regularmente eventos e conexões através do firewall da GTIS Brasil para detectar quaisquer violações, ataques ou acesso a informações sensíveis. A GTIS Brasil garantirá que softwares antivírus e/ou anti-malware sejam instalados em todos os computadores, que o acesso ao servidor seja definido e periodicamente auditado e que privilégios de administrador sejam implementados. A GTIS Brasil monitora sistemas de fiscalização de perímetro para detectar tentativas de *login* falhadas, tentativas de *login* não autorizadas, desativação de acesso e contas de usuários inativas.

Como parte de seus esforços para manter esta Política, GTIS Brasil realizará anualmente uma avaliação de vulnerabilidade e/ou teste de penetração, que serão realizados por um terceiro independente. Tal avaliação verificará a autenticidade da configuração do firewall e da fragmentação antivírus, analisará a segurança do dispositivo de rede e procurará evidências de atividade mal-intencionada.

5.5 Uso Aceitável de Dispositivos Pessoais

Empregados que utilizem computadores pessoais enquanto trabalham em casa deverão manter as proteções que os computadores da GTIS Brasil possuem nesses dispositivos, incluindo proteção antivírus, e senhas fortes. Embora seja permitido o uso da maioria dos dispositivos no escritório, o Diretor de *Compliance* e/ou Diretor Tecnologia se reserva o direito de negar que diversos aplicativos sejam carregados na rede da GTIS Brasil.

5.6 Plano de Destruição de Dados e Equipamentos

O Diretor Tecnologia fará o inventário dos dispositivos e sistemas físicos da GTIS Brasil; inventário dos dispositivos e sistemas de software da GTIS Brasil; criará mapas de recursos de rede, conexões e fluxos de dados (incluindo locais onde os dados do investidor estão armazenados); e catalogará as conexões à rede da GTIS Brasil a partir de fontes externas.

A GTIS Brasil manterá livros e registros por um período de 5 (cinco) anos ou mais, conforme o Item 11.7 abaixo. E-mails também são arquivados segundo a política da GTIS Brasil como livros e registros necessários e são mantidos por um período mínimo de 5 (cinco) anos. Empregados da GTIS Brasil não devem destruir documentos que ainda não estejam arquivados na rede da GTIS Brasil. Documentos impressos ou duplicados em papel contendo informações sensíveis do investidor que estão disponíveis na rede GTIS Brasil podem ser destruídos e devem ser picotados. Equipamentos da GTIS Brasil não devem ser doados, dados de presente ou destruídos, mas sim entregues ao diretor de tecnologia para descarte. Qualquer dúvida sobre destruição de dados, documentos ou equipamentos deve ser encaminhada ao diretor de tecnologia.

5.7 Equipamentos Extraviados

A GTIS Brasil instalou um programa de limpeza remota em todos os computadores portáteis e dispositivos móveis dos empregados. Caso um computador laptop ou dispositivo móvel seja extraviado ou roubado, ou esteja fora do controle de um empregado por mais de 24 (vinte e quatro) horas, o empregado deverá notificar o Diretor de Tecnologia, que tomará as devidas precauções para desativar as informações para o laptop ou dispositivo móvel. Além disso, todos os computadores, laptops, *tablets* e telefones celulares dos empregados são criptografados, tornando os dados ilegíveis em caso de perda ou roubo.

6 ACESSO À INTERNET

O acesso à Internet é fornecido para a GTIS Brasil e é considerado um recurso para a GTIS do Brasil. O acesso à Internet fornecido pela GTIS Brasil não deve ser usado para entretenimento excessivo, filmes de streaming/programas de TV ou videogames etc. Embora aparentemente corriqueiro para um usuário único, a ampla utilização desses sites não comerciais pela empresa consome uma grande quantidade de extensão de banda de Internet, que, portanto, não estará disponível para usuários responsáveis. Pessoas Supervisionadas devem entender que a GTIS Brasil se reserva o direito de monitorar o uso da Internet pelas Pessoas Supervisionadas e, se for constatado que uma Pessoa Supervisionada está gastando uma quantidade excessiva de tempo ou consumindo grande quantidade de extensão de banda para uso pessoal, poderão ser tomadas medidas disciplinares.

Os nomes e senhas das redes sem fio estão sujeitos a alterações por razões de segurança a qualquer momento, com pouca ou nenhuma notificação. Além disso, a rede interna sem fio da GTIS Brasil inclui 2 (duas) formas de identificação: (1) conhecendo a senha; e (2) filtrada por endereço *mac*.

Muitos sites da Internet já foram bloqueados por roteadores e firewalls da GTIS Brasil. Essa lista é constantemente monitorada e atualizada conforme necessário. Qualquer Pessoa Supervisionada que visite sites pornográficos ou outros sites imorais, antiéticos ou não relacionados a negócios (isto é, jogos de azar) sofrerá medidas disciplinares e poderá ser desligada. A GTIS Brasil não é responsável pelas ações de suas Pessoas Supervisionadas quando se trata de downloads e software ilegais de qualquer tipo e somente fornece software legítimo e totalmente licenciado. As Pessoas Supervisionadas são advertidas a não clicar em links que não reconheçam e não devem baixar ou instalar software da Internet sem autorização prévia. Qualquer dúvida quanto ao uso adequado da Internet deve ser encaminhada ao Diretor de *Compliance*.

7 SEGURANÇA CIBERNÉTICA (*CIBERSEGURANÇA*)

Os objetivos das iniciativas de segurança cibernética da GTIS Brasil ("**Iniciativas de Cibersegurança**") são criar um ambiente seguro onde as informações são armazenadas, proteger os Dados Confidenciais e os Dados Pessoais tratados pela GTIS Brasil incluindo, mas não se limitando, aos Dados Pessoais de investidores e de Pessoas Supervisionadas e criar um mecanismo para avaliar a conformidade da cibersegurança e a prontidão do controle na indústria de valores mobiliários.

7.1 Requisitos de Cibersegurança

As Iniciativas de Cibersegurança cobrem os seis tópicos a seguir:

(i) Governança e Avaliação do Risco;

(ii) Direitos e Controles de Acesso;

(iii) Prevenção de Perda de Dados;

(iv) Gestão de Fornecedores;

(v) Resposta a Incidentes; e

(vi) Treinamento.

7.1.1. Governança e Avaliação do Risco

(A) Governança

Como parte de seu programa de cibersegurança, o Grupo GTIS criou uma equipe de resposta a incidentes ("**IRT**"- *incident response team*), que inclui empregados da GTIS Brasil, para adequadamente monitorar e avaliar periodicamente a rede de computadores da GTIS Brasil e os riscos que ela enfrenta com relação à cibersegurança. Os procedimentos adotados e implementados pela IRT são detalhados mais adiante na seção "Resposta a Incidentes".

Conforme seja necessário, a IRT (i) apresentará à alta administração do Grupo GTIS um resumo das conclusões da IRT. Se a alta administração julgar necessário, a IRT apresentará quaisquer descobertas ao Diretor de *Compliance* da GTIS Brasil ou, se considerado necessário, a todos os investidores caso um incidente atinja um nível de elevação; e (ii) analisará os processos de avaliação de risco da GTIS Brasil para identificar potenciais ameaças à segurança cibernética e quaisquer esforços responsivos de reparação empreendidos pelo ou em nome da GTIS Brasil.

(B) Avaliação do Risco

Os avanços tecnológicos proporcionam facilidades e permitem o uso de novas ferramentas pelas instituições, permitindo agilidade na criação e disponibilidade dos serviços, aplicação no meio, entre outros avanços. Por outro lado, o uso crescente de tais ferramentas aumenta o vazamento de informações e os riscos de ciberataques, ameaçando o sigilo, a integridade e disponibilidade dos dados e/ou sistemas das instituições.

Ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informação ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, risco de imagem, danos financeiros ou perda de vantagem competitiva, podendo tais danos ser irreparáveis.

Dado esse cenário, os métodos mais comuns de ciberataques são os seguintes:

(i) Malware – software projetado para corromper computadores e redes**:**

(b) Vírus: Software que causa danos à máquina, à rede, ao software e ao banco de dados;

(c) Cavalo de Tróia: Aparece dentro de outros softwares e cria uma porta para a invasão de computadores;

(d) Espiões: Software mal-intencionado que coleta e monitora o uso de informações; e

(e) *Ransomware*: Software mal-intencionado que bloqueia o acesso a sistemas e bancos de dados, solicitando um resgate a fim de restabelecer o acesso.

(ii) Engenharia Social – métodos de manipulação para obter informações sensíveis, como senhas, dados pessoais e número de cartão de crédito:

(a) *Pharming*: direciona você para um site fraudulento sem seu conhecimento;

(b) *Phishing*: links de e-mail, fingindo ser uma pessoa ou empresa confiável, enviando e-mails oficiais tentando obter informações confidenciais;

(c) *Vishing*: finge ser uma pessoa ou empresa confiável e, através de ligações telefônicas, tenta obter informações confidenciais;

(d) *Smishing*: finge ser uma pessoa ou empresa confiável e, através de mensagens de texto, tenta obter informações confidenciais;

(e) 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.

(iii) DDoS (ataque de negação de serviços) e ataques de botnet – ataques destinados a negar ou atrasar o acesso aos serviços ou sistemas da instituição. No caso de *botnets*, o ataque vem de muitos computadores infectados, usados para criar e enviar *spam* ou vírus, inundando uma rede com mensagens que resultam em negação de serviço.

(iv) Ameaças persistentes avançadas – ataques de intrusos sofisticados usando conhecimento e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Além dos ciberataques, a GTIS Brasil pode estar sujeita a mau funcionamento dos sistemas utilizados e atos/omissões de seus empregados, o que pode resultar na perda e/ou adulteração de dados e Informações Confidenciais.

7.1.2. Prevenção da Perda de Dados

A fim de evitar a perda de dados da empresa, a GTIS Brasil determina quais dados, ativos e serviços garantem a maior proteção para ajudar a evitar que ataques cibernéticos de segurança causem danos significativos. A GTIS Brasil estabeleceu procedimentos para monitorar e evitar violações de dados (ver item 9 – Segurança da Informação – abaixo), exige criptografia ou precauções adequadas em relação à transferência de Dados Confidenciais (conforme descrito no Item 4.1(iii) acima) e estabeleceu regras relativas ao gerenciamento de dispositivos móveis. A GTIS Brasil possui proteções, como regras de negativa de *firewall*, interruptores e/ou roteadores com capacidade de limitação de uso e lista de controle de acesso, assim como atualizará regularmente seu software antivírus e/ou anti-malware. Software de proteção contra vírus ou malware será instalado em todos os computadores da empresa. Para proteger sua rede contra-ataques externos do tipo DDoS, a GTIS Brasil implementou um filtro de spam e outras proteções como regras de negativa de *firewall*, interruptores e/ou roteadores com capacidade de limitação de uso e lista de controle de acesso ou limpeza de acesso, e atualiza regularmente seu software antivírus e anti-malware. Na medida em que um empregado utilizar computadores

domésticos ou dispositivos de acesso remoto para realizar negócios, o software de proteção contra vírus e malware deverá ser instalado em tais computadores domésticos ou dispositivos de acesso remoto. Além disso, a Equipe de *Compliance* monitorará os empregados que trabalham remotamente para garantir que esses não representem um risco para a rede GTIS Brasil.

A GTIS Brasil também monitora a distribuição não autorizada de informações sensíveis fora da GTIS Brasil através de canais de distribuição alternativos, como, por exemplo, por e-mail. A GTIS Brasil adotou uma política com relação à solicitação de mudanças nas informações bancárias dos Investidores, instruções de pagamento dos fornecedores e instruções de financiamento das negociações. Especificamente, a GTIS Brasil exige que qualquer mudança nas informações de transferência via cabo ou informações bancárias que divirjam das informações constantes no contrato de subscrição inicial do investidor seja acompanhada de uma ligação telefônica confirmando tal mudança junto ao investidor. Da mesma forma, a GTIS Brasil exige que qualquer solicitação referente ao pagamento ou outras mudanças suspeitas em relação ao financiamento de investimentos ou informações de fornecedores seja verificada através de uma ligação telefônica para um ponto de contato estabelecido ou verificado.

7.1.3. Gestão de Fornecedores

A GTIS Brasil somente seleciona fornecedores externos após a devida investigação e geralmente escolhe aqueles que são bem conhecidos e estabelecidos dentro de seus segmentos. Ao contratar um fornecedor terceirizado com acesso a Dados Confidenciais, a GTIS Brasil garantirá que existam proteções adequadas para a não divulgação e a confidencialidade de tais informações. A GTIS Brasil garantirá que qualquer fornecedor terceirizado com acesso a Dados Confidenciais ao qual seja dado acesso à rede GTIS Brasil mantenha sua própria política para monitorar ameaças à segurança cibernética e a GTIS Brasil se reserva o direito de solicitar uma cópia dessa política para análise.

Além disso, a GTIS Brasil fornecerá uma cópia desta Política aos principais fornecedores terceiros que tenham acesso a Dados Confidenciais e monitorará rotineiramente a atividade dos fornecedores e o controle de acesso. A GTIS Brasil abordará quaisquer avaliações de risco, gerenciamento do risco, medições de desempenho e relatórios exigidos dos fornecedores. A GTIS Brasil solicitará que os principais fornecedores enviem à GTIS Brasil notificação no caso de quaisquer mudanças significativas nos sistemas, componentes ou serviços do fornecedor que possam potencialmente ter impacto de segurança para a GTIS Brasil ou seus dados.

7.1.4. Resposta a Incidentes

Conforme acima mencionado, a GTIS Brasil criou a IRT para monitorar adequadamente a rede GTIS Brasil e mitigar os riscos que ela enfrenta com relação à cibersegurança. A IRT inclui o Diretor de *Compliance* da GTIS Brasil, assim como vários empregados dos departamentos de tecnologia, *Compliance* e jurídico dentro do Grupo GTIS. Pelo menos uma vez por semestre, e mais frequentemente se necessário, a IRT se reunirá para identificar os riscos particulares que a GTIS Brasil enfrenta do ponto de vista da cibersegurança e analisará quaisquer incidentes ou potenciais incidentes, se houver. A GTIS Brasil manterá informações básicas sobre os eventos esperados na rede GTIS Brasil e monitorará regularmente essas expectativas.

A IRT conduz, ou designará um terceiro para conduzir, avaliações periódicas do risco para identificar ameaças à segurança cibernética, vulnerabilidades e potenciais consequências comerciais, bem como ameaças à segurança física e vulnerabilidades. Continuamente, a IRT

testará seus processos de detecção de eventos, bem como suas respostas a incidentes e quaisquer esforços de reparação realizados pela GTIS Brasil ou em seu nome. Conforme mencionado acima, a IRT também monitorará os principais fornecedores terceiros da GTIS Brasil com acesso a Dados Confidenciais para garantir que tal fornecedor seja capaz de cumprir esta Política. Qualquer ameaça, incidente ou violação de segurança cibernética deve ser comunicada imediatamente ao Diretor de *Compliance*, que informará a IRT.

É responsabilidade de cada Pessoa Supervisionada, fornecedor ou terceiro afiliado comunicar imediatamente qualquer suspeita de invasão, atividade não explicada ou comportamento errático do sistema ao Diretor de *Compliance* ou Diretor de Tecnologia, que informará a IRT. Da mesma forma, uma Pessoa Supervisionada deverá notificar o Diretor de *Compliance* caso qualquer informação sensível seja perdida, roubada ou revelada/desviada involuntariamente. Se necessário, no caso de o incidente requerer elevação adicional, a IRT envolverá a alta administração da GTIS Brasil, advogados externos ou investidores.

Ao ocorrer um incidente ou violação da rede GTIS Brasil, a IRT poderá entender que o evento exige notificação à alta administração, autoridades reguladoras, agências ou partes afetadas, conforme o caso. A IRT é responsável por determinar quais eventos requerem notificação ou alertas aos empregados, fornecedores terceiros ou reguladores. No caso de prejuízo real ao investidor, a IRT documentará os fatos pertinentes que cercam o prejuízo, o montante da perda e o reembolso pela cobertura de seguro de cibersegurança, se houver.

8 TREINAMENTO

Como parte de seu programa de Controles Internos, a GTIS Brasil dá treinamento sobre esta Política para todas as Pessoas Supervisionadas e, se necessário, para afiliados e fornecedores. O treinamento pode incluir, entre outros tópicos, instrução sobre a criação de senhas fortes, detecção de e-mails de *phishing*, dispositivos aprovados, sincronização de dispositivos pessoais e redução da exposição a e-mails. O treinamento ocorrerá periodicamente e sua frequência dependerá de uma série de fatores incluindo, mas não se limitando à evolução das ameaças à segurança. O treinamento pode se dar na forma de reuniões em toda a empresa, distribuição de materiais escritos ou orientação fornecida por e-mail. O Diretor de *Compliance* será responsável por manter um registro de quaisquer orientações ou materiais escritos fornecidos durante tal treinamento.

(i) Integração Inicial

Além disso, sempre que um empregado for contratado, e antes do início efetivo de suas atividades, ele participará de um processo de integração e treinamento onde adquirirá conhecimento sobre as atividades da empresa, regras, políticas e códigos internos, assim como informações sobre as principais leis e regulamentos que regem as atividades da GTIS Brasil. Esse é um treinamento de integração com o objetivo de demonstrar as políticas, os códigos e a filosofia da empresa. O treinamento inicial também aborda os diferentes produtos oferecidos pela GTIS Brasil.

Ao ser contratado e iniciar as atividades, o empregado receberá as seguintes políticas:

(a) Código de Ética;

(b) Política de Decisão de Investimentos, Alocação de Ativos e Divisão de Ordens;

(c) Política de Gerenciamento do Risco;

(d) Política de Prevenção à Lavagem de Dinheiro e Combate à Corrupção;

(e) Política de Segregação de Atividades;

(f) Política de Voto;

(g) Política de Investimento em Crédito Privado;

(h) Política de Investimentos Pessoais;

(i) Política de Aquisição e Monitoramento de Ativos Imobiliários;

(j) Política de Certificação Continuada; e

(k) Política de Regras, Procedimentos e Controles Internos.

(ii) Treinamento contínuo

Em conformidade com esta norma e os valores de nossa instituição, a GTIS Brasil adota um programa anual de reciclagem de seus empregados, a fim de garantir que eles estejam sempre atualizados sobre os termos e responsabilidades aqui descritos, estando todos obrigados a participar de tais programas de reciclagem.

Esse programa anual de reciclagem de empregados consiste, entre outras atividades, em uma apresentação presencial das políticas mencionadas no capítulo acima, que aborda os principais pontos das políticas em vigor no momento da apresentação, a fim de manter os empregados sempre alinhados com as regras dos órgãos reguladores e da própria empresa.

Além disso, no caso de qualquer mudança nas políticas, devido a exigências regulatórias ou outros motivos, a GTIS Brasil poderá conduzir um eventual programa de reciclagem a fim de fornecer-lhes a nova política e, também, apresentar as mudanças e novos pontos abordados por tal política.

Finalmente, deve-se observar que o processo de treinamento inicial e o programa de reciclagem contínua são desenvolvidos e controlados pelo Diretor de *Compliance* e exigem o compromisso total dos empregados com seu atendimento e dedicação.

(iii) Programas de Treinamento

Um programa de treinamento eficaz inclui disposições para garantir que: (i) o treinamento seja contínuo, incorporando eventos atuais e mudanças em códigos, políticas e produtos, bem como leis e regulamentos relativos à sua atividade; (ii) o treinamento se concentre na educação dos empregados sobre as políticas e valores da empresa; (iii) o treinamento exponha as consequências do não cumprimento da política e procedimentos estabelecidos por parte de um empregado (multa, suspensão, rescisão do contrato de trabalho no caso de empregados ou exclusão da sociedade no caso de parceiros); e (iv) o conteúdo do treinamento para cada Pessoa Supervisionada também seja específico para as atividades realizadas por cada um deles.

9 SEGURANÇA DA INFORMAÇÃO

9.1 Privacidade dos Empregados

As Pessoas Supervisionadas não devem ter qualquer expectativa de privacidade ao utilizar os sistemas de informação na GTIS Brasil. Para gerenciar sistemas e reforçar a segurança, a GTIS Brasil pode registrar, revisar e utilizar qualquer informação armazenada ou que circule através de seus sistemas. A GTIS Brasil pode capturar atividades dos usuários como tráfego de e-mail,

números de telefone discados e sites visitados. Além disso, a administração da GTIS Brasil reserva-se o direito de monitorar, inspecionar ou remover de seus sistemas de informação qualquer material que considere ofensivo ou potencialmente ilegal. Esse exame pode ocorrer com ou sem o consentimento, presença ou conhecimento das Pessoas Supervisionadas envolvidas. Os sistemas de informação sujeitos a tal exame incluem, mas não estão limitados, a sistemas de correio eletrônico, qualquer dispositivo controlado pela GTIS Brasil, arquivos de correio de voz, arquivos de *spool* de impressora, saída de fax, gavetas de mesa e áreas de armazenamento.

9.2 Uso Pessoal de Sistemas e Armazenamento de Dados Pessoais

Os sistemas de informação da GTIS Brasil são destinados à utilização somente para fins comerciais. Os arquivos pessoais de uma Pessoa Supervisionada, tais como documentos, fotos, vídeos ou música, não devem ser armazenados no disco compartilhado da GTIS Brasil. O uso pessoal acidental é permitido se não for um risco, não consumir mais do que uma quantidade trivial de recursos que poderiam ser usados para fins comerciais, não interferir na produtividade do usuário e não impedir qualquer atividade comercial. É proibido o uso dos sistemas de informação da GTIS Brasil para correspondência em cadeia, solicitações de caridade, material de campanha política, trabalho religioso, transmissão de material questionável, ou qualquer outro uso não comercial. Software pessoal não deve ser instalado nos sistemas de informação da GTIS Brasil sem a aprovação expressa do Diretor de *Compliance*. A GTIS Brasil não é responsável por quaisquer Dados Pessoais armazenados nos computadores ou servidores da empresa e poderá apagar esses dados sem aviso prévio. Além disso, a GTIS Brasil não investirá recursos da empresa na recuperação de Dados Pessoais no caso de perda deles.

10 PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

O objetivo do Plano de Contingência e Continuidade de Negócios visa estabelecer as medidas a serem tomadas para evitar um impacto negativo considerável na condução das atividades. Essas contingências incluem, por exemplo, crises econômicas, pandemias, falhas operacionais e/ou desastres naturais.

Todos os empregados possuem acesso remoto às redes GTIS Brasil como parte dos procedimentos de recuperação de desastres da GTIS Brasil. Nos casos de ocorrência de quaisquer eventos ou sinistros que possam tornar impraticável, paralisar ou comprometer temporariamente o exercício de suas atividades, a GTIS Brasil deverá seguir os procedimentos aqui definidos e trabalhar em conjunto com um Provedor de Serviços em Nuvem para retomar as atividades o mais brevemente possível.

10.1 Diretrizes de Prevenção e Tratamento de Contingências

Para a implementação efetiva deste Plano de Contingência e Continuidade de Negócios, a GTIS Brasil procurará conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para este fim, a empresa tomará medidas que lhe permitam:

(i) Conhecer e minimizar os danos no período pós-contingência;

(ii) Minimizar prejuízos para si, seus clientes e empregados decorrentes da interrupção de suas atividades; e

(iii) Normalizar as atividades de gestão o mais rapidamente possível.

De modo geral, as etapas para a execução deste plano são as seguintes:

(i) A identificação de interdependências entre as instalações, equipamentos e processos comerciais da GTIS Brasil com outras empresas e/ou com fornecedores e contratados;

(ii) Listagem das diferentes atividades da GTIS Brasil e identificação daquelas com alta relevância estratégica e/ou aquelas com alto potencial de risco financeiro, físico ou operacional;

(iii) Lista de instalações, equipamentos, fornecedores, contratados que possam representar dificuldades ou restrições para a aplicação deste plano; e

(iv) Verificação da adequação dos meios de prevenção e proteção às características da operação e do negócio.

10.2 Disseminação do plano

A fim de reduzir e controlar eventuais prejuízos devido à ocorrência de contingências, todos os empregados da GTIS Brasil devem estar cientes dos procedimentos de backup e proteção de informações (confidenciais ou não), planos de evacuação física do local e melhores práticas para a saúde e segurança no local de trabalho.

10.3 Plano de Recuperação de Negócios

A GTIS Brasil mantém a identificação atualizada de seus principais procedimentos comerciais de modo que, em caso de contingências, será possível retomar as operações com os menores custos de operação e a menor perda de tempo, de recursos humanos, físicos e materiais possível.

Durante o desenvolvimento do Plano de Recuperação de Negócios, conforme descrito nesta Política, foram levados em conta os backups de servidores, bancos de dados e arquivos, assim como a estruturação da computação em nuvem. Os backups realizados são:

(i) Backup diário do banco de dados e armazenamento por 5 anos.

(ii) Backup de arquivos em tempo real na nuvem.

Proteger os dados na forma descrita acima constitui o procedimento central da GTIS Brasil para a rápida recuperação do estado operacional em caso de falha do disco rígido do equipamento. A GTIS Brasil possui todos os servidores instalados em seu escritório, porém o servidor de arquivos (file server) foi migrado para a estrutura em cloud da ferramenta Egnyte, que através do aplicativo instalado nos desktops/laptops de todos os funcionários, permitem acessar os arquivos de qualquer local, itens como contas de usuários, são replicados com os servidores que ficam na cloud da Tekscape. Além disso, a GTIS Brasil também conta com dois provedores de internet com firewalls duplos configurados para alta disponibilidade de navegação, monitoramento e permissão de conteúdo. Todos os dados armazenados em nuvens são criptografados.

Devido a esses procedimentos, caso as Pessoas Supervisionadas não tenham acesso às instalações físicas da GTIS Brasil, elas poderão acessar (após a devida autenticação) os sistemas da GTIS Brasil. Os principais serviços da GTIS Brasil estão na nuvem – e-mail (Office365) e servidor de arquivos (Egnyte) –, permitindo que a disponibilidade dos dados seja instantânea em qualquer situação de emergência.

Além disso, para a rápida e efetiva retomada das operações após a ocorrência de uma contingência, a GTIS Brasil mantém procedimentos que lhe permitem:

(iii) Manter os procedimentos de gestão de pessoal e operações administrativas mesmo durante os efeitos da contingência;

(iv) Retornar permanentemente ao uso das instalações de sua sede após a ocorrência da contingência; e

(v) Avaliar os prejuízos ocorridos devido à interrupção dos negócios.

Além disso, como todo o ambiente de dados GTIS Brasil é baseado em nuvem, a empresa entende que, em caso de contingências, as pessoas poderão acessar o ambiente da GTIS Brasil baseado em nuvem a partir de seus computadores pessoais e manter seu trabalho normalmente, não havendo, portanto, necessidade de um escritório alternativo.

10.4 Tratamento de Contingências Operacionais

A fim de lidar com contingências diretamente relacionadas à operação comercial, os procedimentos devem ser mantidos atualizados para permitir que a empresa:

(i) Aumente rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores se a demanda por serviços aumentar rapidamente sem a consequente redução na qualidade da prestação do serviço;

(ii) Substitua qualquer empregado em caso de saída, no menor tempo possível;

(iii) Identifique novos mercados e/ou produtos potenciais se houver períodos curtos ou longos de recessão na demanda de seus clientes atuais;

(iv) Permaneça sempre competitiva e inovadora a fim de evitar perder sua participação no mercado, explorando seus pontos fortes e diminuindo constantemente suas fragilidades;

(v) Mantenha um fluxo de caixa que, a critério do Diretor de *Compliance*, seja capaz de atender a despesas imprevistas;

A equipe Tecnologia junto com *Compliance* são responsáveis pela implementação do plano de contingência da GTIS Brasil.

10.5 Ativação do Mecanismo de Resposta

Os empregados são responsáveis por comunicar ao Diretor de *Compliance* e/ou Diretor de Tecnologia toda e qualquer situação que possa, ainda que potencialmente, originar uma situação que possa levar à ativação dos procedimentos de contingência estabelecidos neste plano. Para tal fim, a GTIS Brasil fornece um aplicativo de comunicação de massa: Alert Media ("**APP"**).

A ativação do plano de contingência ficará a critério e sob a responsabilidade da Equipe de *Compliance*, trabalhando em conjunto com o Diretor de Tecnologia. Em caso de necessidade, poderá ser contratada uma empresa especializada no combate ao evento identificado, bem como na resposta ao eventual dano.

A fim de ser adequadamente evitada, a GTIS Brasil adotará os seguintes mecanismos de resposta para cada contingência específica:

(i) Indisponibilidade da Sede:

Caso o escritório não esteja disponível durante o horário comercial, as Pessoas Supervisionadas permanecerão disponíveis e desempenharão suas funções em sistema de *home office*;

(ii) Indisponibilidade de Servidores (Nuvem):

Uma vez verificada a indisponibilidade dos servidores em nuvem, a GTIS Brasil deverá proceder com as seguintes ações:

(a) acionamento dos prestadores de serviços: imediatamente após a constatação da falha, o Diretor de Tecnologia deverá acionar os prestadores de serviços de nuvem responsáveis para iniciar o processo de recuperação do ambiente;

(b) implementação do plano de recuperação de desastres: paralelamente ao acionamento dos prestadores de serviços, a GTIS Brasil ativará seu plano de recuperação de desastres. Este plano inclui procedimentos detalhados para a restauração dos serviços críticos, priorizando a continuidade de suas operações;

(c) comunicação interna: a GTIS Brasil deverá comunicar imediatamente a equipe sobre a situação de indisponibilidade, fornecendo orientações precisas sobre as ações a serem tomadas. Esta comunicação deve incluir informações sobre a estimativa de tempo para a recuperação e quaisquer alterações temporárias nos procedimentos operacionais;

(d) alternativas de trabalho: enquanto a indisponibilidade persistir, os empregados devem, sempre que possível, continuar desempenhando suas atividades de maneira remota (*home office*) ou conforme as instruções fornecidas pelo Diretor de Tecnologia. A GTIS Brasil deverá assegurar que todos os empregados tenham os recursos necessários para continuar suas atividades durante o período de interrupção;

(e) monitoramento e atualização: a Equipe de *Compliance* deve monitorar continuamente o progresso da recuperação e manter o Diretor de Tecnologia informado sobre o status. Qualquer desenvolvimento relevante deve ser comunicado prontamente a todos os empregados; e

(f) relatório pós-incidente: após a restauração completa dos serviços, a GTIS Brasil realizará uma análise detalhada do incidente para identificar as causas e avaliar a eficácia das ações tomadas. Um relatório será elaborado pela Equipe de *Compliance* e compartilhado com o Diretor de Tecnologia para implementar eventuais melhorias contínuas no plano de recuperação de desastres e respectivos nos procedimentos operacionais.

(iii) <u>Indisponibilidade de Conexão com o Provedor de Internet</u>

A indisponibilidade pode ser dividida em 02 (duas) hipóteses: (i) se a indisponibilidade for inferior a 04 (quatro) horas, será avaliada a necessidade de substituição temporária dos provedores de acesso à internet, assim como haverá um contato com os provedores de internet para que a conexão seja restaurada; e (ii) se a indisponibilidade for superior a 04 (quatro) horas, ou se não houver previsão para restauração da conexão, os provedores de acesso à internet serão substituídos e uma empresa especializada será realocada para restaurar a conexão, ou encontrar uma solução alternativa, ainda que temporária, se o fornecedor terceirizado de tecnologia da informação da GTIS Brasil não puder resolver. Os empregados permanecerão na sede da GTIS Brasil e ali desempenharão suas funções;

(iv) <u>Redução de Empregados</u>

A GTIS Brasil avaliará a possibilidade de transporte até sua sede e determinará as funções a serem desempenhadas pelos empregados disponíveis até que uma solução alternativa seja encontrada, mesmo que temporariamente. Os empregados que não conseguirem chegar à sede da GTIS Brasil permanecerão disponíveis e desempenharão suas funções em sistema de *home office*; e

(v) <u>Tempo de Resposta da Pessoa Supervisionada</u>

É responsabilidade de cada Pessoa Supervisionada manter seus atuais meios de contato e sendo do conhecimento da GTIS Brasil. Da mesma forma, é responsabilidade de cada empregado estar acessível e comunicar seus respectivos locais assim que tomar conhecimento de um evento que possa comprometer a continuidade de suas funções, ainda que momentaneamente, ou dos negócios da GTIS Brasil. Para tal fim, a GTIS Brasil fornece a APP. Eles também devem informar a localização de outros empregados se estiverem familiarizados com sua localização.

11 CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

O objetivo deste dispositivo é estabelecer critérios qualitativos mínimos e orientar o processo de seleção, contratação e monitoramento de indivíduos e entidades que possam ter interesse em iniciar e manter um relacionamento comercial com os fundos de investimentos geridos pela GTIS Brasil.

Para contratações que não relacionadas aos fundos de investimentos geridos pela GTIS Brasil, seguir os procedimentos e regras estabelecidos na política institucional da GTIS.

Este é um procedimento real de *Know Your Partner* – KYP, focado no conhecimento do terceiro a ser contratado, nos procedimentos de integridade instituídos e observados pelas empresas que operam com a GTIS Brasil.

Os critérios e processos aqui estabelecidos visam proporcionar o mínimo indispensável de segurança operacional e jurídica, evitando conflitos de interesse de forma a manter a GTIS Brasil em conformidade com o Código de Administração de Recursos de Terceiros e outras normas e regras aplicáveis à matéria.

11.1 Análise de Mercado

(i) Sempre avaliar se esse prestador de serviços pode gerar qualquer potencial conflito de interesse com o gestor de recursos, administrador fiduciário ou cotista dos Veículos de Investimento administrados pela GTIS Brasil;

(ii) Se o valor cobrado é justo em relação ao serviço oferecido e ao valor de mercado;

(iii) Se há benefícios recebidos pela GTIS Brasil e seus empregados derivados de tal contratação, ou se os benefícios são direcionados ao fundo ou ao investidor.

11.2 Processo de Pré-Seleção

Durante o processo de contratação, os empregados devem obter informações qualitativas sobre o terceiro interessado em iniciar vínculos legítimos com a GTIS Brasil, a fim de permitir um melhor julgamento durante a pré-seleção. As informações a serem obtidas podem incluir:

(i) A data de início das atividades;

(ii) Qualificações dos principais sócios/executivos;

(iii) Lista de clientes (passados e atuais) e objeto da contratação;

(iv) Busca na rede mundial de computadores sobre notícias negativas sobre o terceiro;

(v) Questionário padrão de *due diligence* da Anbima; e

(vi) Outras informações qualitativas que possam ser relevantes para melhor avaliar o terceiro.

Para conduzir o processo a GTIS Brasil criou Due Diligence Check List, ferramenta proprietária que auxilia na classificação de risco a ser associados ao Terceiro, conforme o Anexo II desta Política, e na formalização da diligência realizada. Os seguintes aspectos são considerados durante o processo de pré-seleção:

(i) Estrutura da empresa;

(ii) Boa reputação (no caso de uma pessoa jurídica, a reputação dos sócios e dos principais executivos também deve ser considerada);

(iii) Nível de satisfação de outros clientes, passados e presentes;

(iv) Estrutura para atender o objeto da Contratação;

(v) Capacidade econômica e financeira;

(vi) Código de Conduta e Ética, ou similar;

(vii) Política Anticorrupção, ou similar;

(viii) Política de Combate à Lavagem de Dinheiro, ou similar;

(ix) Qualquer documento, procedimento e/ou formulário relacionado com a integridade e o cumprimento das regras; e

(x) Selo de Associado ou Aderente à ANBIMA, quando aplicável, ou, se não for o caso, as razões para não o obter.

O início das atividades estará vinculado à formalização do contrato, e nenhum pagamento poderá ser feito antes da conclusão do contrato. Os acordos celebrados para formalização do contrato deverão ter os requisitos contidos no Capítulo III, artigo 11 do Regras e Parâmetros de Administração de Recursos de Terceiros.

Os empregados responsáveis pelo processo de seleção de fornecedores manterão registros atualizados dos fornecedores, eliminando aqueles sobre os quais haja qualquer dúvida relativa a má conduta, comportamento antiético, comportamento ilícito ou que possam ter uma má reputação no mercado.

11.3 Procedimento para Locatários

Um Locatário significa nesta política, um indivíduo, empresa, órgão público que utiliza imóvel (escritório, galpão, terreno etc.) detido pelos fundos administrados pela GTIS para fins comerciais e paga aluguel direta ou indiretamente nos termos de um contrato de locação.

O procedimento visa a identificar os principais riscos antes ou na sua manutenção de relacionamento com locatários, com objetivo de identificação de potencial risco reputacional, risco de lavagem de dinheiro, do financiamento do terrorismo e do financiamento da proliferação de armas de destruição em massa e risco de crédito.

Este é um procedimento real de Know Your Client – KYC, focado no conhecimento do cliente que iremos estabelecer ou manter relacionamento através de um contrato de locação.

Semelhante ao processo de terceiro, o responsável pelo relacionamento e/ou Departamento de Compliance classificará o cliente de acordo com seu risco potencial. Realizando conforme o caso, background check do Locatário, beneficiário final e/ou principais executivos, o que inclui a consulta em lista de sanção, mídia negativa, e PPE e quando necessário, emissão de certidões

negativas, para auxílio na classificação, preencher o Due Diligence Check List, seguindo os critérios e frequências estabelecidos no Anexo II.

Adicionalmente para avaliação do risco de crédito, a equipe do Financeiro realizará uma análise de crédito do locatário e/ou garantias fornecidas para avaliar a capacidade financeira, de forma a honrar o compromisso assumido, conforme definido na Política de Gerenciamento de Risco.

11.4 Não Aplicabilidade do Processo de Pré-Seleção

A GTIS Brasil poderá deixar de aplicar os procedimentos ora estabelecidos, a seu critério exclusivo, quando o terceiro não estiver relacionado a atividade principal do fundo de investimento gerido pela GTIS Brasil e tiver uma clara capacidade econômica, financeira e/ou técnica para satisfazer o objeto da contratação e para cumprir suas responsabilidades e arranjos contratuais.

11.5 Outras Disposições

Vale mencionar que, devido às regras estabelecidas na atual regulamentação e autorregulamentação, a GTIS Brasil adotará medidas prévias de *due diligence* para a contratação e monitoramento de terceiros relacionados à tecnologia, sistemas e/ou infraestrutura de informação, visando à proteção de dados.

11.6 Seleção de Corretores

A GTIS Brasil, com a prestação de serviços adequados que garantam a melhor execução das ordens para Veículos de Investimento e/ou carteiras administradas sob gestão, juntamente com a preservação dos interesses e, consequentemente, de seus investidores, adota um cuidadoso processo de seleção e contratação de corretores.

Esse processo é baseado na devida investigação de potenciais corretores-distribuidores de valores mobiliários para permitir que a GTIS Brasil adquira um conhecimento profundo de potenciais prestadores de serviços.

Ao avaliar potenciais prestadores de serviços, a GTIS Brasil adota 3 (três) princípios para selecionar corretores que irão intermediar ativos financeiros para Veículos de Investimento e/ou carteiras administradas:

(i) Estrito cumprimento do dever fiduciário;

(ii) Reconhecida capacidade de execução; e

(iii) Mínimo impacto financeiro.

Com base nestes princípios, os corretores devem ser considerados como terceiros, para fins de aplicação do Processo de Pré-seleção, incluindo solicitando à corretora a qualificação PQO da B3 e o questionário padrão de *due diligence* da Anbima.

11.7 Soft Dollar

O Soft Dollar será permitido, desde que tenha sido recebido de forma aberta e transparente, com a permissão expressa do respectivo gerente de área. O Soft Dollar gerado será utilizado em serviços que auxiliem a administração na tomada de decisões de investimento, sempre no interesse dos investidores.

Além disso, GTIS Brasil deverá transferir para a carteira quaisquer benefícios ou vantagens que possa obter como resultado de sua posição como gestor das carteiras, com a devida consideração à exceção prevista para qualquer regra ou taxas divulgadas nos materiais de oferta.

11.8 Monitoramento

O monitoramento das atividades realizadas por terceiros para a GTIS Brasil, assim como os próprios terceiros, é de responsabilidade da área que solicitou a Contratação. O monitoramento deve ser contínuo durante a vigência da Contratação, e o terceiro avaliado proporcionalmente ao serviço prestado, com ênfase em eventuais disparidades de tempo, qualidade e quantidade esperada.

Além disso, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a GTIS Brasil, e os respectivos relatórios devem ser enviados para a Equipe de *Compliance*.

No caso de qualquer fato novo ou mudança significativa, é possível reavaliar a contratação de terceiros.

É importante notar que este monitoramento se baseia no princípio dos melhores esforços, já que a GTIS Brasil e seus empregados não podem estar presentes no dia a dia de terceiros contratados a todo tempo.

11.9 Manutenção de Documentos

Todos os manuais, relatórios, atas e outros documentos relacionados a essa seleção de terceiros e à Política de Contratação e Monitoramento serão mantidos em arquivos físicos ou armazenados digitalmente no escritório da GTIS Brasil por um mínimo de 5 (cinco) anos.

12 VIOLAÇÃO

A violação desta Política pode resultar em medidas disciplinares até e incluindo a rescisão do contrato de trabalho ou de prestação de serviços. A GTIS Brasil se reserva o direito de notificar as autoridades competentes de aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade.

13 DISPOSIÇÕES GERAIS

Esta Política está disponível no website da GTIS Brasil, de acordo com o Artigo 16, III da Resolução CVM 21.

14 PRAZO E ATUALIZAÇÃO

Esta Política será revisada a cada 2 (dois) anos pela GTIS Brasil e poderá ser alterada a qualquer momento na medida em que houver a necessidade de atualizar seu conteúdo.

* * *

Anexo I

Termo de Compromisso

Declaro que recebi, nesta data, uma cópia de todas as políticas da GTIS Partners Brasil Gestão, Consultoria em Investimentos e Participações Ltda. ("**GTIS Brasil**"), comprometendo-me a observá-las e segui-las integralmente e a comunicar, imediatamente, ao gestor do ativo relevante, a ocorrência de quaisquer violações das respectivas políticas.

Comprometo-me a aceitar, outorgar e cumprir quaisquer novos procedimentos, regras e padrões que possam ser considerados no âmbito de qualquer política da GTIS Brasil, sem a necessidade de assinar um novo Termo de Compromisso para este fim.

Declaro, ainda, ter pleno conhecimento de que a violação deste Termo de Compromisso poderá implicar em responsabilidade civil e criminal, e constituir motivo para a imediato desligamento das atividades das empresas, sem prejuízo da verificação de danos à GTIS Brasil, devido a esta violação.

[Local], [Data].

_____

[Pessoa Supervisionada]

Anexo II

Metodologia de Avaliação do Risco e Monitoramento Individualizado

Com vistas ao cumprimento Código de Administração de Recursos de Terceiros, após a análise do terceiro/cliente, a Equipe de *Compliance* classificará o terceiro/cliente com o potencial de: (i) Baixo Risco; (ii) Médio Risco; ou (iii) Alto Risco, conforme segue:

1. Metodologia e Avaliação

1.1. Baixo Risco

Terceiros/Clientes com Potencial Baixo Risco: não se enquadrou em nenhuma das características principais avaliada na ferramenta de classificação de risco da GTIS Brasil, neste caso a GTIS deixará de aplicar os procedimentos estabelecidos nesta política a seu exclusivo critério.

1.2. Médio Risco

Terceiros/Clientes com Potencial Médio Risco: a GTIS Brasil adotará os procedimentos estabelecidos nesta política sendo sugerido o preenchimento da ficha cadastral, realização de *screenning* pelo Compliance e documentos adicionais poderão ser solicitados conforme o caso. Serão classificados como de Médio Risco, terceiros/clientes que não possam ser classificados como de Baixo Risco por apresentar características de maior exposição a risco avaliada pela ferramenta, mas não atuem em atividades críticas para o fundo de investimento.

1.3. Alto Risco

Terceiros/Clientes com Potencial Alto Risco: a GTIS Brasil sujeitará o terceiro/cliente à mais completa investigação, com o preenchimento da ficha cadastral, realização de *screenning* pelo Compliance, formulário de Cybersecurity (se aplicável) e outros documentos e certificados necessários de terceiros/clientes de acordo com os procedimentos adotados na Política Anticorrupção, Código de Ética, Combate à Lavagem de Dinheiro. Será classificado como de Alto Risco o terceiro/cliente que apresentou uma ou mais das características de maior exposição de risco avaliada pela ferramenta e atue em atividade crítica para o fundo de investimento. Além disso, o terceiro será classificado como alto risco se possuir atividades autorregulada pela ANBIMA e não for Associados ou Aderentes aos Códigos ANBIMA.

Uma vez classificado de Alto Risco, a decisão final sobre a contratação/relacionamento desse terceiro/cliente caberá ao Comitê de Risco, juntamente com um relatório derivado de sua análise da documentação recebida pelo terceiro/cliente durante o Processo de Pré-seleção.

2. Monitoramento

Terceiros/clientes serão supervisionados e reavaliados de acordo com sua classificação por grau de risco, conforme indicado a seguir:

(i) Baixo Risco: Uma vez a cada 60 (sessenta) meses;

(ii) Médio Risco: Uma vez a cada 36 (trinta e seis) meses; e

(iii) Alto Risco: Uma vez a cada 12 (doze meses).

Ou a qualquer momento, na ocorrência de fato novo relevante, ou alteração significativa que seja identificada pela área que solicitou a Contratação ou no processo contínuo de acompanhamento de mídias efetuado pela GTIS Brasil.