



**CLOUD9 CAPITAL LTDA.**  
**MANUAL DE COMPLIANCE**  
**Dezembro, 2023**

<b>1 POLÍTICA DE CONTROLES INTERNOS</b>	<b>3</b>
<b>2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>8</b>
<b>3 POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA</b>	<b>16</b>
<b>4 POLÍTICA DE COMBATE À CORRUPÇÃO</b>	<b>23</b>
<b>5 POLÍTICA DE CONTRATAÇÃO DE FUNCIONÁRIOS E TERCEIROS</b>	<b>26</b>
<b>6 POLÍTICA DE TREINAMENTO</b>	<b>28</b>
<b>7 POLÍTICA DE CONFIDENCIALIDADE</b>	<b>30</b>
<b>8 POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E CONFLITO DE INTERESSE</b>	<b>32</b>
<b>9 POLÍTICA DE CERTIFICAÇÃO CONTINUADA</b>	<b>34</b>

## 1 POLÍTICA DE CONTROLES INTERNOS

### 1.1 OBJETIVO

Este Manual de Compliance (“**Manual**”) tem por objetivo estabelecer regras e procedimentos, bem como descrever os controles internos a serem implementados e observados no desempenho das atividades da **CLOUD9 CAPITAL LTDA** (“**Cloud9**” e/ou “**Gestora**”).

As regras e procedimentos aqui previstos visam garantir o atendimento às normas, políticas e regulamentações vigentes, referentes à atividade de gestão de carteiras de valores mobiliários e aos padrões ético e profissional exigidos pela Cloud9 no bom exercício de suas atividades.

Desta forma o presente Manual foi devidamente elaborado em conformidade com a regulamentação e autorregulamentação, em especial com o disposto na Resolução da Comissão de Valores Mobiliários (“**CVM**”) nº 21, de 25 de fevereiro de 2021, conforme alterada (“**Resolução CVM 21**”), nos Códigos de Regulação e Melhores Práticas para Administração de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“**ANBIMA**”).

A Cloud9 deverá manter versões atualizadas deste Manual em seu website: <https://www.cloud9capital.com.br/>

### 1.2 APLICABILIDADE

Este Manual aplica-se a todos os Colaboradores da Cloud9.

Para os fins deste Manual, são considerados colaboradores da Cloud9 todos aqueles que possuam cargo, função, posição e/ou relação, societária, empregatícia, de estágio, profissional ou de confiança (independentemente da natureza destas atividades, sejam elas direta, indireta e/ou secundariamente relacionadas com quaisquer atividades fim ou meio) com a Cloud9 (“**Colaboradores**”) e ainda todos aqueles que possuam relação comercial e/ou contratual com a Cloud9 (“**Terceiros**”).

### 1.3 DIRETRIZES

Este Manual tem como diretrizes:

- (i) disseminar a cultura sobre a importância dos controles internos a todos os Colaboradores;
- (ii) assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;
- (iii) alinhar a estrutura dos controles internos aos objetivos do negócio e aos riscos deles decorrentes;
- (iv) criar o arcabouço necessário para a existência de atribuição de responsabilidades e delegação de autoridade, observada a estrutura hierárquica da Cloud9;
- (v) possibilitar a elaboração de relatórios sobre a situação dos controles internos;
- (vi) estabelecer os fluxos de aprovação; e
- (vii) assegurar a revisão periódica dos processos de controles internos.

#### 1.4 DIRETOR DE COMPLIANCE E RISCO - RESPONSABILIDADES PELOS CONTROLES INTERNOS

O Diretor de *Compliance* e Risco terá plena autonomia para o exercício de suas funções, sendo certo que são obrigações do Diretor de *Compliance* e Risco além das demais obrigações previstas na legislação e regulamentação aplicáveis:

- (i) Vigiar, fiscalizar e verificar a eficácia dos controles internos;
- (ii) Avaliar o nível de segurança dos controles internos existentes;
- (iii) Avaliar se os controles internos existentes são adequados para cumprir com as normas e regulações aplicáveis;
- (iv) Levar quaisquer dúvidas para apreciação dos administradores da Cloud9;
- (v) Atender prontamente todos os Colaboradores; e
- (vi) Identificar possíveis condutas contrárias a este Manual e demais políticas internas da Cloud9

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Cloud9, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual e demais políticas internas da Cloud9, deverá informar ao Diretor de *Compliance* e Risco, para que sejam tomadas as providências cabíveis.

São atribuições do Diretor de *Compliance* e Risco:

- (i) Definir os princípios éticos a serem observados por todos os Colaboradores conforme o Manual, o “Código de Ética” e a “Política de Investimentos Pessoais” (conjuntamente, os “**Códigos Cloud9**”) o ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- (ii) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores;
- (iii) Apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos éticos e de *Compliance* e apreciar e analisar situações não previstas nos Códigos Cloud9;
- (iv) Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial ou em manifestação em processo administrativo;
- (v) Tratar todos os assuntos que chegue ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da Cloud9, como também dos Colaboradores envolvidos; e
- (vi) Definir e aplicar eventuais sanções aos Colaboradores.

Ainda é de competência do Diretor de *Compliance* e Risco analisar situações que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- (i) Investimentos pessoais (observadas as disposições da “**Política de Investimentos Pessoais**”);
- (ii) Participações na administração de outras empresas;

- (iii) Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, terceiros ou clientes (observadas as disposições do “Código de Ética”);
- (iv) Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
- (v) Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; e/ou
- (vi) Participações em alguma atividade política.

Ainda no que tange aos controles internos a responsabilidade deve observar o disposto a seguir:

#### **1.4.2 Implementação e Manutenção de Processos de Controles Internos:**

Os gestores de cada uma das áreas da Cloud9 são responsáveis por estabelecer, manter, promover e avaliar as atividades desempenhadas e estabelecer controles internos adequados e eficazes, bem como documentá-los de maneira clara e objetiva sempre observado as políticas internas da Cloud9

A área de *Compliance* deverá receber de cada um dos gestores de área um relatório compreendendo o status dos controles internos por eles implantados, incluindo os eventos negativos e impactos. De posse dos relatórios, o Diretor de *Compliance* e Risco emitirá tempestivamente o relatório com eventuais propostas à administração da Cloud9 (“**Administração**”), que por sua vez irá deliberar pelo método de adequação mais apropriado para situação em específico.

#### **1.4.3 Análise, avaliação e acompanhamento dos Processos de Controles Internos:**

Conforme disposto anteriormente o Diretor de *Compliance* e Risco é encarregado de definir os métodos de avaliação e monitoramento dos processos de controles internos da Cloud9, sendo também responsável pelo atendimento aos órgãos reguladores e autorreguladores.

Ainda, será responsável por promover a avaliação independente das atividades desenvolvidas pelas diversas áreas da Cloud9, de modo a aferir a adequação dos controles estabelecidos ao cumprimento das normas e regulamentos aplicáveis, bem como aos Códigos Cloud9. O processo de aferição é realizado através de exames de aderência nos processos existentes e documentados. A periodicidade e os exames de aderência a serem realizados são definidos pelo Diretor de *Compliance* e Risco, sempre respeitando os prazos estabelecidos pelas normas e regulamentos aplicáveis, tendo periodicidade mínima anualmente.

O Diretor de *Compliance* e Risco é responsável também por acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos da Cloud9, bem como por monitorar a qualidade e integridade dos mecanismos de controles internos, apresentando as recomendações de aprimoramento de políticas, manuais, práticas e procedimentos que entender necessários.

Nos termos da regulamentação aplicável, a Cloud9 elabora anualmente relatórios de conclusão dos testes e exames efetuados, que é devidamente encaminhado ao órgão da administração da Cloud9 e ficando disponível em sua sede para acesso pelos órgãos reguladores, caso solicitados.

## 1.5 DÚVIDAS OU AÇÕES CONTRÁRIAS AOS PRINCÍPIOS E NORMAS

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Cloud9, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual e demais Códigos Cloud9, deverá informar ao Diretor de Controles Internos, para que sejam tomadas as providências cabíveis.

Para os fins do presente Manual, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance e Risco, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da Cloud9, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance e Risco, exclusivamente através do e-mail: [compliance@c9.com.br](mailto:compliance@c9.com.br)

## 1.6 TERMO DE COMPROMISSO

Este Manual é parte integrante das regras e procedimentos internos que regem as atividades da Cloud9 e, conseqüentemente, de seus Colaboradores. Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Cloud9, bem como o completo entendimento acerca do conteúdo deste Manual. Em caso de dúvidas ou necessidade de aconselhamento, é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance e Risco.

Todo Colaborador, ao receber este Manual, firma o Termo de Compromisso conforme **Anexo I**, por meio do qual reconhece e confirma seu conhecimento e concordância com os termos deste Manual e das normas de Compliance e princípios aqui contidos. Ao firmar o Termo de Compromisso, cada Colaborador compromete-se a zelar pela aplicação das normas de Compliance e princípios contidos neste Manual, bem como nos demais Códigos Cloud9. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

## 1.7 CANAL DE DENÚNCIA

A Cloud9 sempre deverá manter a disposição de seus Colaboradores e Relacionados, bem como terceiros, um canal de denúncia (“**Canal de Denúncia**”) apto para recebimento de denúncias e/ou quaisquer informações pertinentes a respeito do cumprimento e conformidade das normas previstas neste Manual.

O Canal de Denúncia está disponível para seus Colaboradores, terceiros e demais interessados, como uma ferramenta de interlocução proativa, transparente, independente e imparcial para o reporte de violações ou suspeitas de descumprimento de qualquer dos temas descritos nos Códigos Cloud9, bem como na legislação anticorrupção.

Toda denúncia deverá ser baseada no desempenho das funções éticas, sociais e profissionais do denunciante e na boa-fé.

## 1.8 CONDUTAS A SEREM DENUNCIADAS

São exemplos de condutas que devem ser denunciadas, sem prejuízo daquelas especificamente indicadas nos demais Códigos Cloud9:

- (i) Ações que possam resultar em riscos para segurança de Colaboradores;

- (ii) Ofensas criminais tais como: fraude, propina, suborno e lavagem de dinheiro e outras atividades ilegais ou criminosas;
- (iii) *Insider trading*;
- (iv) Conflito de Interesses que tenha sido devidamente analisado pela Cloud9 e cuja resolução não tenha sido respeitada;
- (v) Comportamento anticompetitivo;
- (vi) Falhas no cumprimento de obrigações legais;
- (vii) Mau uso de ativos da Cloud9;
- (viii) Práticas contábeis antiéticas;
- (ix) Preocupações legais ou éticas;
- (x) Violência, bullying, ameaças e/ou toda e qualquer conduta abusiva (gesto, palavra, escritos, comportamento, atitude, etc.) que fira a dignidade e a integridade física ou psíquica de uma pessoa, ameaçando seu emprego ou degradando o clima de trabalho;
- (xi) Qualquer manifestação de preconceitos relacionados a origem, raça, cor, religião, condição social, gênero, ideologia política, deficiência, profissão ou qualquer outra forma de manifestação de preconceito ou discriminação;
- (xii) Violação ou descumprimento dos Códigos Cloud9, tanto por seus Colaboradores; e
- (xiii) Condutas suspeitas do Diretor de Compliance e Risco.

Após a submissão da denúncia, uma resposta automática de e-mail será encaminhada para confirmação do recebimento da denúncia. E, para conhecimento sobre o andamento do processo de análise e investigação, para a adição de informações e para acesso ao resultado de toda investigação, novos e-mails serão enviados. Dentro dos limites da confidencialidade e anonimato previstos neste Canal de Denúncia, toda denúncia será analisada e devidamente acompanhada pelo Diretor de Compliance e Risco, exceto nos casos de denúncia contra o próprio Diretor de Compliance e Risco, que será analisada e acompanhada pela Administração, excluindo o Diretor de Compliance e Risco.

A Cloud9 assegura, em todos os casos, a confidencialidade, anonimato, independência, imparcialidade e isenção no tratamento, apuração e arquivamento das informações recebidas no âmbito de uma denúncia. No mesmo sentido, estão assegurados os direitos do denunciante e das pessoas citadas, sendo vedado qualquer tipo de retaliação àqueles que de boa-fé fizerem uso do Canal de Denúncia, independentemente do resultado da apuração, garantindo a credibilidade do processo.

Todas as denúncias recebidas serão encaminhadas para o Diretor de Compliance e Risco e passarão por processo de organização e classificação de acordo com: (a) a relação do denunciante com a Cloud9; (b) o grau de embasamento dos fatos; (c) a gravidade dos fatos; (d) o tipo de conduta; (e) o tipo de violação; (f) o processo de remediação; e (g) a extensão do impacto dentro da empresa e fora, entre outros.

Todas as informações encaminhadas na denúncia serão avaliadas quanto à sua relevância e fundamento, em conexão com a violação ou irregularidade relatada.

Todos os fatos relatados serão pesquisados e analisados determinando o prosseguimento ou não do processo.

O Diretor de Compliance e Risco tomará todas as ações necessárias para inibir efetivamente qualquer irregularidade e desvios de comportamento no dia a dia da empresa e, conforme necessário, poderá iniciar processos de investigação e auditorias.

Após a conclusão do processo de apuração, um relatório será gerado e armazenado conjuntamente com toda documentação levantada, justificando a medida recomendada pelo Diretor de Compliance e Risco (“**Relatório de Conformidade**”). Tal relatório deverá ser encaminhado ao Comitê de Risco e Conformidade com recomendação ou não da sanção a ser tomada, que deverá ser composto pelo Diretor de Compliance e Risco, pelo Diretor de Investimentos e pela Diretora Sem-Designação Específica. O Comitê de Risco e Conformidade deverá se reunir em caráter extraordinário (presencialmente ou por conferência telefônica) para decidir quanto à aplicação ou não de sanção, tendo em vista a recomendação do Diretor de Compliance e Risco.

### **1.9 VIGÊNCIA E ATUALIZAÇÃO**

Este Manual ficará vigente a partir da presente data e poderá ser revisado e/ou alterado a qualquer tempo sempre que necessário ou, ainda, em razão de circunstâncias que demandem tal providência. A Cloud9 deverá manter versões atualizadas deste Manual em seu website: <https://www.cloud9capital.com.br/>

## **2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

### **2.1 OBJETVO**

Esta Política de Segurança da Informação (“**PSI**”) visa proteger as informações de propriedade e/ou sob guarda da Cloud9, visando garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade de tais informações.

A PSI leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Cloud9

### **2.2 APLICABILIDADE**

A PSI aplica-se a todos os Colaboradores, prestadores de serviços e sistemas da Cloud9, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Cloud9 ou que acessem informações a ela pertencentes.

Todo e qualquer usuário de recursos computadorizados e/ou da infraestrutura lógica da Cloud9 tem a responsabilidade de proteger a segurança e a integridade de suas informações e dos equipamentos de informática disponibilizado pela Cloud9

A coordenação direta das atividades relacionadas à presente PSI ficará a cargo do Diretor de *Compliance* e Risco, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

### **2.3 CLASSIFICAÇÃO E CONFIDENCIALIDADE DA INFORMAÇÃO**

Todas as informações da Cloud9 ou que circulem em sua infraestrutura terão sua confidencialidade assegurada com base em sua criticidade, de acordo com os seguintes níveis de sensibilidade:

- (i) **Informação confidencial (ou sensível):** Informação cuja divulgação possa causar danos financeiros ou à imagem da Cloud9 ou cujo sigilo ou limitações de uso sejam estabelecidos por lei, bem como informação que a Cloud9 não tenha interesse de divulgar publicamente e cujo acesso por parte de indivíduos externos deva ser evitado.
- (ii) **Informação pública:** Informação disponibilizada publicamente e que pode ser utilizada por todos, incluindo público externo, sem causar danos à Cloud9 (por exemplo, informações disponíveis em seu website).

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Cloud9, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Cloud9, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, deverá ser tratada como informação confidencial, e só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado previamente pelo Diretor de *Compliance* e Risco.

Os Colaboradores devem sempre se abster de tratar e/ou mencionar informações internas ou confidenciais da Cloud9 em locais públicos.

Em caso de dúvida pelos Colaboradores acerca da classificação acima mencionada, o Colaborador deverá, antes de qualquer divulgação interna e/ou externa, verificar com a área de *Compliance*.

Todos os dados de clientes da Cloud9 devem ser tratados como informações confidenciais. Em conformidade com a legislação atual, a Cloud9 garante aos titulares de dados diversos direitos, previstos nos termos da Lei Geral de Proteção de Dados (“**LGPD**”) tais como (i) direito de acesso; (ii) direito de revogação de consentimento; (iii) solicitação de anonimato; dentro outros conforme Política de LGDP da Cloud9.

São consideradas informações confidenciais (“**Informações Confidenciais**”), para os fins deste Manual:

- (i) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, operações estruturadas, demais operações e seus respectivos valores, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Cloud9 e a seus sócios ou clientes, independente destas informações estarem contidas em pen-drives, HDs, outros tipos de mídia ou em documentos físicos; e
- (ii) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Cloud9, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários,

*trainees* ou estagiários da Cloud9 e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela Cloud9 ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Não são consideradas Informações Confidenciais quaisquer informações que:

- (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador;
- (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Manual;
- (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade;
- (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; e
- (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Diretor de Compliance e Risco para que as medidas legais cabíveis sejam tomadas.

É dever da Cloud9: (i) garantir a segurança e confidencialidade das Informações Confidenciais não públicas de seus clientes e fundos sob sua gestão; (ii) proteger a segurança de tais Informações Confidenciais contra qualquer ameaça ou perigo antecipados; (iii) proteger tais Informações Confidenciais contra o acesso ou uso não autorizado; e (iv) garantir a correta eliminação dos dados pessoais em caso de solicitação do titular dos dados.

A Cloud9 realiza o tratamento de dados pessoais com finalidades específicas e de acordo com as bases legais previstas na LGPD.

## **2.4 SEGURANÇA DA INFORMAÇÃO**

A Cloud9 está comprometida e empenhada em buscar o mais alto grau de proteção de suas informações e sistemas. A Cloud9 investe em ferramentas e tecnologias para garantir que sua infraestrutura de tecnologia esteja em linha com as melhores práticas em termos de segurança e confiabilidade. Os procedimentos de segurança dos sistemas aplicados pela empresa são revistos continuamente e atualizados sempre que necessário. Periodicamente, são realizados também testes de segurança e treinamentos com seus Colaboradores sobre o uso apropriado da infraestrutura de tecnologia.

As práticas de segurança da informação adotadas pela Cloud9 têm como objetivo impedir a ocorrência de (i) transmissão não autorizada de informações confidenciais sobre clientes, Colaboradores ou sobre a Cloud9 em geral; (ii) cópia ou transmissão não autorizada de softwares ou dados proprietários; (iii) acesso não autorizado a arquivos, comunicações e outros dados confidenciais relacionados aos clientes, Colaboradores da Cloud9 ou à Cloud9 em geral; (iv) tentativas de interceptação de e-mail ou mensagem instantânea; (v) quaisquer ataques cibernéticos; e (vi) liberação não autorizada de senhas e códigos de ID de usuários.

As medidas de segurança da informação utilizadas pela Cloud9 têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da Cloud9.

### **2.4.1 Cópias e Impressões**

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos e documentos utilizados, gerados ou disponíveis da Cloud9 ou circulem com eles em ambientes externos à empresa sem prévia autorização do Diretor de *Compliance* e Risco. Isso porque tais arquivos podem conter informações internas ou confidenciais da empresa e/ou de seus clientes, que não devem ser disponibilizadas externamente.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Cloud9, de acordo com as devidas atribuições profissionais do Colaborador.

Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade, devendo adotar as precauções necessárias para evitar o acesso não autorizado de terceiros às informações, por exemplo, garantindo que os documentos não se encontrem visíveis para terceiros não autorizados a acessar as informações (por exemplo, pelo uso de pasta transparente).

Ainda, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter Informações Confidenciais de não acesso a todos os Colaboradores.

#### **2.4.2 Guarda de arquivos, mesa e tela limpa**

Cada Colaborador é responsável pelos documentos deixados sobre suas mesas, armários e gaveteiros, sendo certo que arquivos ou documentos contendo informações confidenciais armazenados em meio físico não devem ficar expostos em mesas, devendo, sempre que possível, ser armazenados em armários e gaveteiros trancados quando não utilizados.

Ao se ausentarem de suas estações ou se afastarem de seus equipamentos de trabalho, os Colaboradores deverão bloquear tais equipamentos, de modo a evitar o acesso não autorizado.

Arquivos digitais devem ser armazenados na rede disponibilizada pela Cloud9, não devendo haver o armazenamento local de arquivos em dispositivos eletrônicos de Colaboradores.

#### **2.4.3 Descarte de Informações**

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações internas ou confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação, sendo recomendável a sua destruição total, como, por exemplo, por meio de picotadora.

#### **2.4.4 Uso de equipamentos**

Adicionalmente, os Colaboradores devem se abster de utilizar na estrutura tecnológica da Cloud9 pen-drives, HD externos, disquetes, fitas, discos ou quaisquer outros dispositivos que não tenham sido fornecidos pela empresa, com a finalidade de utilização exclusiva para o desempenho das atividades profissionais na Cloud9. O uso de dispositivos desta natureza pode ser integralmente bloqueado

pela Cloud9, hipótese em que eventual necessidade de uso de tais dispositivos deverá ser solicitada ao setor de Tecnologia da Informação da Cloud9 (“TI”) sendo, portanto, proibido a conexão de equipamentos na rede da Cloud9 que não estejam previamente autorizados.

Todos os equipamentos de tecnologia da informação considerados críticos para as atividades da Cloud9 (e.g., os servidores) devem ser mantidos em um local seguro, cujo acesso seja restrito, controlado e devidamente protegido contra potenciais ameaças (e.g. inundações, incêndios, invasão, roubo, vandalismo, agentes químicos e outras ameaças físicas).

Equipamentos eletrônicos corporativos ou nos quais circulem informações internas ou confidenciais da Cloud9 devem ter seu acesso protegido por, no mínimo, login e senha, atualizados periodicamente.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar seu superior hierárquico ou o Diretor de *Compliance* e Risco.

#### **2.4.5 Acesso a websites e instalação de programas**

O acesso a *websites* e *blogs*, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Cloud9 e de seus Colaboradores.

Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve comunicar imediatamente o setor de TI e o Diretor de *Compliance* e Risco, para que sejam adotadas as providências pertinentes.

Somente devem ser instalados programas de computador necessários para o desenvolvimento de atividades profissionais dos Colaboradores, mediante prévia análise e aprovação do Diretor de *Compliance* e Risco.

#### **2.4.6 Senha e Login**

A senha e login para acesso aos dados contidos em todos os computadores e equipamentos da Cloud9, bem como nos e-mails que também 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 Cloud9.

Todas as senhas utilizadas no ambiente tecnológico da Cloud9 devem respeitar os padrões de segurança indicados pelo setor de TI.

As senhas utilizadas devem seguir as seguintes orientações:

- (i) Não devem ser mantidas por escrito em lugar algum;

- (ii) Não devem ser transmitidas através de e-mail;
- (iii) Não devem ser compartilhadas em nenhuma circunstância;
- (iv) Possuir tamanho e complexidade adequados;
- (v) Devem ser trocadas periodicamente.

#### **2.4.7 Acesso Remoto**

Os acessos remotos darão permissões de acesso aos mesmos sistemas, pastas e arquivos disponíveis no escritório da Cloud9. O Diretor de *Compliance* e Risco será responsável por autorizar e validar tais acessos aos Colaboradores que deles necessitem para o desenvolvimento de suas atividades profissionais.

Ademais, a Cloud9 deverá (i) manter atualizados softwares de proteção contra vírus nos dispositivos remotos, e os Colaboradores autorizados deverão (ii) relatar ao Diretor de *Compliance* e Risco qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Cloud9 e que ocorram durante o trabalho remoto, e (iii) não armazenar informações internas ou confidenciais localmente nos dispositivos autorizados para acesso remoto.

#### **2.4.8 Controle de Acesso**

O acesso de pessoas que não os Colaboradores da Cloud9 a áreas restritas somente será permitido com a autorização expressa de Colaborador autorizado pelo Diretor de *Compliance* e Risco. O acesso à rede de informações e equipamentos da Cloud9 é exclusivo dos Colaboradores da gestora conforme disposto nesta PSI e não poderão ser compartilhados com terceiros.

#### **2.4.9 Arquivamento de Informações**

Os Colaboradores deverão manter arquivada na rede da Cloud9 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 Cloud9 em relação à esta PSI e as atividades desenvolvidas pela Cloud9

#### **2.4.10 Manutenção e Revisão**

São guardadas cópias de todos os e-mails contidos nas caixas postais da Cloud9 pelo período de 5 (cinco) anos. Todas as mensagens, originadas ou recebidas por e-mails ou sistemas de mensagem instantânea da Cloud9, são consideradas de propriedade da Cloud9 e estão sujeitas à revisão do Diretor de *Compliance* e Risco a qualquer momento e sem aviso prévio.

Além disso, o departamento de tecnologia (ou empresa terceirizada) da Cloud9 poderá vir a acessar as comunicações de e-mail ou mensagem instantânea durante a execução de atividades como manutenção de rotina, upgrade e resolução de problemas. As informações do usuário não serão divulgadas para o Diretor de *Compliance* e Risco, exceto em casos de suspeitas ou violações das normas dos Códigos Cloud9 ou leis e regulamentações aplicáveis.

## **2.5 UTILIZAÇÃO DO AMBIENTE TECNOLÓGICO E MONITORAMENTO**

Todos os computadores, telefones, equipamentos, internet, e-mails, redes e demais sistemas disponibilizados pela Cloud9 aos seus Colaboradores, que compõem sua

estrutura tecnológica, se destinam exclusivamente à utilização para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores.

Deste modo, o uso da infraestrutura tecnológica da Cloud9 poderá ser monitorado, com o objetivo de apurar o cumprimento das disposições da presente PSI e demais normas internas da Cloud9, bem como da legislação e regulamentação brasileiras, pelos Colaboradores.

Os Colaboradores encontram-se cientes de tal monitoramento e reconhecem que este não corresponde à violação de sua privacidade, na medida em que (i) tem como objetivo apurar o desenvolvimento de suas atividades profissionais e a segurança dos ativos da empresa e de seus clientes; e (ii) a expectativa de privacidade no ambiente de trabalho se encontra mitigada.

## 2.6 PROPRIEDADE INTELECTUAL

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais exercidas na Cloud9 (contrato, memorandos, cartas, fac-símiles, apresentações a clientes, bases de dados e de cadastros, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão), em qualquer formato, são e permanecerão sendo propriedade exclusiva da Cloud9, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na gestora, devendo todos os documentos permanecer em poder e sob a custódia da Cloud9

É vedado ao Colaborador, inclusive, apropriar-se ou realizar cópias de quaisquer desses documentos e arquivos após seu desligamento.

Caso um Colaborador, ao ser admitido, disponibilize à Cloud9 quaisquer documentos, planilhas, arquivos ou outras ferramentas para fins de desempenho de sua atividade profissional junto à Cloud9, o Colaborador deverá assinar declaração confirmando que (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Cloud9, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento.

## 2.7 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A Cloud9 irá atuar periodicamente na identificação dos riscos internos e externos bem como na revisão de processos e melhorias em suas proteções de segurança. Esse processo será conduzido pela equipe de TI e pelo Diretor de *Compliance e Risco* em conjunto com uma empresa especializada para tratamento de dados e na prevenção de ataques cibernéticos (“**Empresa Especializada**”), o qual deverá ser documentado com o fim de dar visibilidade à metodologia utilizada (que será proposta pela Empresa Especializada) para avaliar e gerir as vulnerabilidades da Cloud9. Conforme o caso a Cloud9 poderá contratar uma empresa terceirizada para tanto.

Abaixo encontra-se uma listagem de alguns riscos de segurança cibernética identificados em avaliação inicial:

- (i) Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- (ii) Comunicações falsas causando o comprometimento de estações de trabalho decorrente de cliques em link malicioso (“*Phishing*”); ou
- (iii) Vazamento de informações confidenciais.

A Cloud9 poderá adotar as seguintes medidas, com o objetivo de mitigar os riscos de segurança cibernética acima elencados, conforme processos descritos ao longo da presente PSI:

- (i) Utilização de softwares antivírus e firewall atualizados, visando evitar ataques cibernéticos em seus sistemas, incluindo e-mails;
- (ii) Testes de penetração, de modo a identificar possíveis falhas sistêmicas;
- (iii) Armazenamento de informações confidenciais protegidas por criptografia;
- (iv) Treinamentos periódicos de segurança da informação a seus Colaboradores.

## **2.8 REPORTE DE SITUAÇÕES SUSPEITAS E RESPOSTA A VIOLAÇÕES**

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Cloud9, efetiva ou potencial, ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser imediatamente informada o Diretor de *Compliance* e Risco. Caberá ao Diretor de *Compliance* e Risco comunicar a Administração e decidir, conforme aplicável, a comunicação a agências reguladoras e de segurança pública, bem como determinar quais terceiros (clientes, administrador fiduciário etc.), deverão ser contatados com relação à violação.

O Diretor de *Compliance* e Risco nas situações acima descritas deverá observar os seguintes critérios:

- (i) Avaliação do tipo de incidente ocorrido, a criticidade das informações acessadas e a medida da respectiva perda;
- (ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- (iii) Definição das atribuições de cada Colaborador visando investigar, sanar ou mitigar os impactos da violação nas atividades da Cloud9 e a seus clientes;
- (iv) Determinação das responsabilidades;
- (v) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- (vi) Avaliação da necessidade de notificação de partes internas e externas à Cloud9, incluindo seus clientes e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD);
- (vii) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação, se privilegiada; e

- (viii) Determinação do responsável que arcará com as perdas decorrentes do incidente após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

## **2.9 TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES**

A Cloud9 entende essencial que o treinamento anual em segurança da informação, nos termos de política específica prevista neste Manual, supervisionado pelo Diretor de *Compliance* e Risco, abranja todos os preceitos contidos na presente PSI.

## **2.10 RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES**

A Cloud9 realizará anualmente testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente PSI, incluindo, mas não se limitando, aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros. Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas serão descritos no relatório de controles internos da Cloud9, nos termos da regulamentação aplicável.

## **3 POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA**

### **3.1 OBJETO**

A Cloud9, nos termos da Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada (“**Resolução CVM 50**”), bem como demais regulamentações aplicáveis, estabelece neste Manual sua Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa (“**PLDFTP**” e “**Política de PLDFTP**”, respectivamente), de modo a adequar suas atividades às normas pertinentes ao crime de lavagem de dinheiro e financiamento ao terrorismo e ao financiamento da proliferação de armas de destruição em massa.

É de responsabilidade de todos os Colaboradores o conhecimento, a compreensão e a busca de meios para proteger a Cloud9 contra práticas de lavagem de dinheiro e financiamento ao terrorismo e ao financiamento da proliferação de armas de destruição em massa. As leis e regulamentações atreladas a estes delitos, bem como as regras aqui previstas devem ser obrigatoriamente cumpridas.

### **3.2 REGULAMENTAÇÃO**

A Política de PLDFTP visa promover a adequação da Cloud9 às normas, leis e instruções que dispõem e regulam os procedimentos sobre estes assuntos, tais como, mas não limitadas a:

- (i) Lei n.º 9.613, de 3 de março de 1998, conforme alterada (“**Lei 9.613**”), que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos na referida lei, cria o Conselho de Controle de Atividades Financeiras (“**COAF**”) e dá outras providências;
- (ii) Circular n.º 3.978, de 23 de janeiro de 2020, conforme alterada, do Banco Central do Brasil (“**BACEN**”), que dispõe sobre a política, os procedimentos e os controles

internos a serem adotados pelas instituições autorizadas a funcionar pelo BACEN visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei 9.613, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016, conforme alterada (“**Lei 13.260**”);

- (iii) Carta Circular n.º 4.001, de 29 de janeiro de 2020, conforme alterada, do BACEN, que divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei 9.613, e de financiamento ao terrorismo, previstos na Lei 13.260, passíveis de comunicação;
- (iv) Resolução CVM 50, que dispõe sobre a prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa no âmbito do mercado de valores mobiliários; e
- (v) Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

As normas indicadas acima deverão ser de pleno conhecimento de todos os Colaboradores da Cloud9.

### **3.3 REPORTE E APLICABILIDADE**

Seguindo o determinado pelos normativos acima descritos, qualquer indício e/ou suspeita de operações financeiras e não financeiras que possam envolver atividades relacionadas aos crimes de lavagem de dinheiro, ocultação de bens e valores, bem como incorporar ganhos de maneira ilícita, para a Cloud9, clientes ou para o Colaborador, devem ser comunicadas imediatamente ao Diretor de *Compliance* e Risco.

É, ainda, de responsabilidade dos Colaboradores:

- (i) Compreender e cumprir as disposições desta Política de PLDFTP;
- (ii) Relatar qualquer proposta, transação ou situação considerada incomum ou suspeita ao Diretor de *Compliance* e Risco;
- (iii) Fornecer qualquer documentação solicitada pelas agências reguladoras, autorreguladoras e pelos auditores independentes;
- (iv) Participar dos treinamentos requeridos sobre prevenção à lavagem de dinheiro, corrupção e combate ao financiamento do terrorismo; e
- (v) Monitorar clientes classificados como PEPs (conforme definido posteriormente neste Manual).

### **3.4 RESPONSABILIDADE | EQUIPE DE COMPLIANCE**

A área de *Compliance* é responsável pela análise e monitoramento desta Política de PLDFTP, sendo certo que o Diretor de *Compliance* e Risco possui pleno e irrestrito acesso a quaisquer dados e informações a respeito das operações realizadas pela Cloud9 e seus Colaboradores bem como possui soberania e autonomia para a comunicação de indícios da ocorrência dos crimes previstos na regulamentação aplicável ou a eles relacionados.

Ainda, o Diretor de *Compliance* e Risco é responsável por:

- (i) Desenvolver e implementar ferramentas e procedimentos que apoiem as estratégias da Cloud9 relativos à prevenção a lavagem de dinheiro, corrupção e financiamento ao terrorismo;
- (ii) Apresentar à administração qualquer risco relevante de *compliance* e lavagem de dinheiro que tenha identificado;
- (iii) Decidir se eventuais riscos relevantes em termos de *compliance* e lavagem de dinheiro necessitam monitoramento adicional ou a instauração de investigação;
- (iv) Interagir com agências reguladoras e reportar qualquer atividade suspeita nos termos da legislação aplicável;
- (v) Treinar Colaboradores da Cloud9 e manter registros dos referidos materiais de treinamento e desenvolver e promover campanhas e atividades para apoiar os Colaboradores da Cloud9 na detecção de transações suspeitas; e
- (vi) Verificar se os administradores fiduciários e terceiros contratos cumpram as disposições desta Política de PLDFTP e tenham normas e procedimentos internos adequados e suficientes para identificar e combater práticas de lavagem de dinheiro e financiamento ao terrorismo e ao financiamento da proliferação de armas de destruição em massa.

### 3.5 LAVAGEM DE DINHEIRO

A expressão lavagem de dinheiro consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e serviços obtidos ilícitamente. O processo de lavagem de dinheiro envolve três etapas, são elas: colocação, ocultação e integração.

- (i) A **colocação** é a etapa em que o agente introduz os valores obtidos ilícitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens (remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, ao mercado financeiro).
- (ii) A **ocultação** é o momento que o agente realiza transações suspeitas e caracterizadoras do crime de lavagem. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro.
- (iii) Na **integração** o recurso ilegal integra definitivamente o sistema econômico e financeiro. A partir deste momento, os valores recebem aparência lícita.

### 3.6 INDÍCIOS DE LAVAGEM DE DINHEIRO

Em conformidade com o estipulado na regulamentação anteriormente citada, é de suma importância que os Colaboradores tenham conhecimento das referidas normas, de modo a ter conhecimento das operações que configuram indícios de lavagem de dinheiro.

São considerados indícios de lavagem de dinheiro, as operações:

- (i) Cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional e a situação financeira patrimonial declarada;
- (ii) Realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;

- (iii) Evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;
- (iv) Cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários, respectivamente;
- (v) Cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- (vi) Que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);
- (vii) Realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;
- (viii) Com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;
- (ix) Transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;
- (x) Em que não seja possível identificar o beneficiário final; e
- (xi) Cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do cliente ou de seu representante.

Podem ser também configuradas como indícios de lavagem de dinheiro, as seguintes práticas:

- (i) Resistência em facilitar as informações necessárias para a abertura de conta;
- (ii) Declarar diversas contas bancárias e/ou modificá-las com habitualidade; e
- (iii) Autorizar procurador que não apresente vínculo aparente.

### **3.7 ABORDAGEM BASEADA NO RISCO**

A Cloud9 adota uma abordagem baseada no risco de lavagem de dinheiro, corrupção e financiamento ao terrorismo e financiamento da proliferação de armas de destruição em massa, de modo a que as medidas preventivas aplicadas sejam diretamente proporcionais aos riscos identificados. Neste sentido, a Cloud9 realizará avaliações de risco periódicas para monitorar seus prestadores de serviços, envidando seus melhores esforços para assegurar que estes sigam as diretrizes nacionais e internacionais aplicáveis.

Ainda, todas as operações que envolvam quaisquer dos indícios acima elencados, independentemente de ter sido classificada como de Baixo Risco, Médio Risco ou Alto Risco conforme **Anexo II**, deverão ser reportados ao Diretor de *Compliance* e Risco, que será responsável por respeitar o sigilo do reporte e proporcionar a devida averiguação dos fatos.

A classificação de risco será abordada nos vários tipos de Cadastro.

A classificação de risco pode ser refeita a qualquer momento por conta de fatos novos que sejam identificados ou por alteração relevante do relacionamento da contraparte com a Cloud9, além de ser atualizada periodicamente de acordo com a classificação obtida.

### 3.8 CADASTRO

A Cloud9 utiliza as seguintes ferramentas para implementação ao combate dos crimes de lavagem de dinheiro:

#### 3.8.1 Cadastro de Colaboradores (*Know your Employee*)

A Cloud9 adota uma postura rígida e transparente na contratação de seus funcionários e sócios. Antes do ingresso na Cloud9, todos os candidatos devem ser entrevistados pelos sócios designados para essa função. Requisitos ligados à reputação no mercado e perfil são avaliados, bem como antecedentes profissionais do candidato. O departamento de *Compliance* é responsável por realizar anualmente, a análise reputacional de todos os Colaboradores, bem como conduzir treinamentos de integridade nos termos dos Códigos Cloud9.

Com o objetivo de evitar risco reputacional para a Cloud9 e fraudes realizadas por Colaboradores e demais crimes financeiros, e combater a corrupção e a conivência com a prática de crimes, todo novo Colaborador deve ser submetido às seguintes análises:

- (i) Histórico de crédito disponível no Serasa;
- (ii) Lista de Pessoas Politicamente Expostas (PEPs) disponível no Serasa PEP e World-Check;
- (iii) Qualquer informação material adversa disponível no sistema World-Check e no Google;
- (iv) Situação fiscal disponível no site da Receita Federal brasileira; e
- (v) Litígios através do Tribunal Federal do Estado em que a parte reside.

A conduta dos Colaboradores deve estar permanentemente em conformidade com esse Manual. Desta forma, a Cloud9 estabeleceu procedimentos para conhecer adequadamente seus Colaboradores, realizados através de treinamentos, declarações periódicas (anualmente) e revisão anual das pesquisas realizadas antes da contratação.

#### 3.8.2 Cadastro de Parceiros (*Know your Partners*)

O cadastro de parceiros deverá observar a Política de Contratação de Terceiros conforme capítulo 6 deste Manual que visa estabelecer os princípios que regem o processo de contratação de prestadores de serviços e fornecedores da Cloud9, de forma a assegurar a extinção de potenciais conflitos de interesses e garantir que o processo de contratação de terceiros seja conduzido de forma diligente.

### 3.9 CONTROLE E MONITORAMENTO DE OPERAÇÕES

#### 3.9.1 Verificação de Contrapartes e Ativos

A Cloud9 também adota uma postura rígida e transparente no monitoramento dos investimentos realizados pelos fundos sob sua gestão, sendo responsável pelo processo de identificação e verificação da contraparte nas operações de investimento (via processos de *due diligence*), visando identificar a proveniência dos recursos utilizados e prevenir que referidas contrapartes utilizem a Cloud9 ou seus fundos geridos para atividades ilegais ou impróprias.

Neste sentido, a Cloud9, na qualidade de gestora de recursos, adota medidas visando monitorar e prevenir ocorrência de práticas atreladas à lavagem de dinheiro/terrorismo por intermédio dos seus fundos geridos, tais como inclusão de artigos sobre tal tema dentro do regulamento de cada um dos fundos, limitação de distribuição de cotas de seus fundos geridos por distribuidores pré-aprovados pelo Diretor de *Compliance e Risco*, entre outros.

### **3.9.2 Monitoramento**

A Cloud9 monitora todas as atividades e informações que passam pelo seu conhecimento e que são possíveis de serem descobertas, privilegiando o cumprimento desta Política de PLDFTP inclusive conforme disposto no **Anexo I** ao presente Manual.

Em caso de identificação de situação suspeita, o Diretor de Compliance e Risco tomará todas as medidas cabíveis e necessárias, consultando ou não os sócios da Cloud9, podendo optar desde proibição de aplicações e resgates ou eventuais esclarecimentos, até o efetivo processo de comunicação aos órgãos reguladores, ou entre outros, na forma prevista nesta Política de PLDFTP.

### **3.9.3 Risk Assessment**

A Cloud9 conduzirá avaliação de riscos periódica a fim de identificar operações e produtos que estejam particularmente expostos a riscos de lavagem de dinheiro.

### **3.9.4 Pessoas Politicamente Expostas (“PEPs”) e Pessoas de “Atenção Especial”**

Nos termos da regulamentação vigente, a Cloud9 e seus Colaboradores prestarão muita atenção a PEPs e Pessoas de “Atenção Especial”. Os PEPs são indivíduos que são, ou foram encarregados de funções públicas, bem como seus familiares e pessoas próximas.

A Cloud9 adota processos de prevenção à PLDFTP que confronta as informações de terceiros com a lista oficial de PEPs, elaborada e divulgada no sistema do Conselho de Controle de Atividades Financeiras. Referido sistema de identificação é levado em consideração na análise de riscos e evidência de lavagem de dinheiro.

Todos os terceiros expostos politicamente são definidos pelo sistema como de alto risco. Todos os Colaboradores devem levar ao Diretor de *Compliance e Risco*, quaisquer operações que tenham como terceiro/contraparte PEP, que será responsável por registrar e monitorar a operação e quaisquer produtos, atividades subsequentes relacionadas à operação em análise pela Cloud9

Pessoas de “Atenção Especial” são aquelas que, no sistema de PLDFTP, devido a suas ocupações profissionais e os ramos de atividades, são considerados de “alto risco” e serão consideradas pela Cloud9 como incompatíveis com certas transações no mercado financeiro ou com maior probabilidade de envolvimento intencional (ou não) em lavagem de dinheiro, corrupção e financiamento do terrorismo.

Por fim, terceiros que venham a ter relação com a Cloud9 – sejam pessoas físicas ou jurídicas – que já se envolveram com lavagem de dinheiro, corrupção e financiamento ao terrorismo, ou que receberam publicidade negativa, podem ser caracterizados como “suspeitos”.

Para fins de controle, a equipe a Cloud9 adota medidas para garantir que nenhuma subscrição seja autorizada e nenhum contrato de gerenciamento de investimentos seja assinado com uma entidade sancionada, uma entidade comercial situada em um país sancionado ou um indivíduo sancionado, conforme determinado pelos Estados Unidos, pela Agência de Controle de Ativos Estrangeiros dos EUA – OFAC, e que nenhuma distribuição seja feita a uma entidade ou indivíduo sancionado, seja como beneficiário, proprietário da garantia, garantidor/consignatário ou parte receptora ou remetente.

Quando identificada alguma informação adversa ou atípica, o Comitê de Risco e *Compliance* pode rejeitar o novo investidor ou o novo investimento de um cliente existente. Se houver preocupações relacionadas a crimes financeiros o Comitê de Risco e *Compliance* deve ser informado para determinar a necessidade de reporte às autoridades. Um cliente só pode ser rejeitado com o aval do Comitê de Risco e *Compliance*.

Em instâncias em que a Cloud9 decidir não aceitar um novo investidor ou um novo investimento de um cliente existente, considera-se que o Diretor de *Compliance* e Risco pode denunciar o fato para as autoridades relevantes embora nenhuma transação tenha de fato ocorrido. A Cloud9 vai manter toda a documentação relacionada à transação por cinco anos a partir da data em que o negócio foi rejeitado ou encerrado.

Qualquer suspeita não pode ser comunicada ao cliente ou a terceiros de modo a evitar qualquer potencial responsabilidade da Cloud9 e de seus representantes.

### **3.10 IDENTIFICAÇÃO E TRATAMENTO DAS OCORRÊNCIAS E COMUNICAÇÃO AOS ÓRGÃOS REGULADORES**

A Cloud9 procura estar sempre em conformidade com as normas reguladoras do mercado financeiro. Portanto, prioriza o tratamento dos alertas gerados pelas regras de prevenção à lavagem de dinheiro, de modo que qualquer evento que chegue ao conhecimento da Cloud9 e que apresente suspeita ou evidência de lavagem de dinheiro, corrupção e financiamento ao terrorismo será imediatamente reportado ao Diretor de *Compliance* e Risco, que será responsável por manter a confidencialidade do reporte.

As ocorrências geradas demandam total atenção por parte do Diretor de *Compliance* e Risco, ficando responsável por realizar todas as tratativas necessárias e comunicar quaisquer atividades atípicas ou suspeitas à autoridade competente sempre que necessário.

Toda comunicação será formulada respeitando os prazos estabelecidos e atentando para a forma e meio exigidos, a Cloud9 ainda realiza a comunicação negativa anual à CVM, nos termos do artigo 23 da Resolução CVM 50, sempre que não houver no ano ocorrência de transações ou propostas de transações passíveis de serem comunicadas por motivos de lavagem de dinheiro.

### **3.11 TREINAMENTO**

A Cloud9 promove treinamentos anuais sobre os conceitos previstos nesta Política de PLDFTP, possibilitando o conhecimento de seus Colaboradores acerca dos preceitos e diretrizes aqui estabelecidos em relação as suas atividades nos termos do Capítulo 6 deste Manual.

### 3.12 DISPOSIÇÕES GERAIS

Esta Política de PLDFTP foi devidamente aprovada pelos sócios da Cloud9 e encontra-se disponível para consulta pública no endereço eletrônico da Cloud9

A Cloud9 mantém todos os documentos referentes aos cadastros e registros, à disposição dos órgãos reguladores, durante o período de 5 (cinco) anos, contados a partir do encerramento da conta ou da conclusão da última transação realizada em nome do respectivo cliente, podendo este prazo ser estendido indefinidamente na hipótese de existência de investigação comunicada formalmente pelos órgãos reguladores à Cloud9 e, ainda, conforme disposto na regulamentação vigente.

## 4 POLÍTICA DE COMBATE À CORRUPÇÃO

### 4.1 INTRODUÇÃO

Seguindo os preceitos da Lei n.º 12.846, de 1º de agosto de 2013, conforme alterada (“**Lei Anticorrupção**”), bem como os de sua regulação, através do Decreto n.º 8.420, de 18 de março de 2015, o combate à corrupção também é um dever da Cloud9 e de todos seus Colaboradores, razão pela qual foi elaborada a presente Política de Combate à Corrupção.

A Lei Anticorrupção responsabiliza as pessoas jurídicas, nos âmbitos administrativo e civil, pelos atos lesivos previstos praticados em seu interesse ou benefício e não exclui a responsabilidade individual de seus dirigentes ou administradores ou de qualquer pessoa natural, autora, coautora ou partícipe do ato ilícito.

Conforme previsto na regulamentação vigente a Cloud9 está sujeita as regras aplicáveis à Lei Anticorrupção e qualquer violação a esta norma e demais podem gerar impactos reputacionais negativos a instituição, impactos que podem vir a ser irreparáveis.

### 4.2 POLÍTICA ANTICORRUPÇÃO

Com o objetivo de facilitar o entendimento da Lei Anticorrupção e do presente Manual, é imprescindível que os Colaboradores estejam familiarizados com as seguintes definições:

- (i) **Corrupção.** A corrupção pode ser definida como a utilização de poder ou autoridade com o fim de se obter benefício em interesse próprio, ou de um terceiro relacionado. Neste sentido, pratica ato lesivo contra o patrimônio público quem (a) promete, oferece ou fornece, direta ou indiretamente, vantagem indevida a Agente Público, ou a terceira pessoa a ele relacionada; (b) financia, custeia, patrocina ou de qualquer modo subvenciona a prática de corrupção; (c) utiliza-se de um intermediário, pessoa física ou jurídica, para ocultar ou dissimular seus reais interesses ou ocultar a identidade dos beneficiários pelo ato corrupto; ou, ainda, quem (d) dificulta a investigação ou fiscalização de agentes públicos, inclusive no âmbito de agências reguladoras e órgãos de fiscalização do sistema financeiro.
- (ii) **Agente Público.** Considera-se agente público quem, ainda que transitoriamente ou sem remuneração, exerça cargo, emprego ou função pública. Equipara-se a agente público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da administração pública.

- (iii) **Vantagem Indevida.** Qualquer pagamento em dinheiro ou qualquer transferência de valor, tangível ou intangível, com o objetivo de influenciar ou recompensar qualquer ato oficial ou decisão de um Agente Público. Os pagamentos de facilitação - “subornos” pagos a Agentes Públicos, com o fim de acelerar a conclusão de processos oficiais nos quais o cidadão tem direito concedido por lei, também são uma Vantagem Indevida proibida pela legislação e podem ser objeto de acusação criminal. O conceito de Vantagem Indevida ainda inclui, por exemplo, presentes, brindes, viagens, refeições, patrocínios, doações e quaisquer outras contribuições ou benefícios prometidos ou oferecidos ao Agente Público ou entidades a ele relacionadas com o intuito de influência ou recompensa para benefício próprio.

### 4.3 ATOS LESIVOS E SANÇÕES

Na forma da referida Lei Anticorrupção, entende-se por atos lesivos à administração pública, nacional ou estrangeira, os seguintes:

- (i) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
- (ii) Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nesta Lei;
- (iii) Comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
- (iv) No tocante a licitações e contratos:
  - (a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
  - (b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
  - (c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; fraudar licitação pública ou contrato dela decorrente;
  - (d) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
  - (e) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
  - (f) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; e
- (v) Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

Ainda, pela Lei Anticorrupção, as sanções previstas para a pessoa jurídica responsabilizada pelos atos ilícitos apresentados anteriormente são:

- (i) A perda dos bens, direitos ou valores que representem vantagem ou proveito direta ou indiretamente obtidos da infração, ressalvado o direito do lesado ou de terceiro de boa-fé;
- (ii) Suspensão ou interdição parcial de suas atividades;
- (iii) Dissolução compulsória da pessoa jurídica;
- (iv) Proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo mínimo de 1 (um) e máximo de 5 (cinco) anos.

#### 4.4 NORMAS DE CONDUTA

Diante do exposto, é proibido dar ou oferecer qualquer valor, presente ou benefício a qualquer agente público sem prévia e expressa autorização do Diretor de *Compliance* e Risco da Cloud9, observado, ainda, os Códigos Cloud9.

Os Colaboradores deverão (i) se atentar que qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação à Lei Anticorrupção e ensejar a aplicação das penalidades previstas; (ii) se atentar que a violação à Lei Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público; e (iii) questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Ainda, é de responsabilidade de todos os Colaboradores proteger a Cloud9 de atividades de corrupção e suborno, de forma que não serão tolerados comportamentos omissos sobre a questão ou envolvimento nesses tipos de atividade.

A Cloud9 utiliza seus melhores esforços para monitorar todos os Colaboradores da instituição, de forma a garantir que eles atuem em observância à Lei Anticorrupção e sua regulamentação. Diante disso, constituem parâmetros mínimos as seguintes medidas:

- (i) Políticas de conduta e ética que são aplicadas para todos os Colaboradores da Cloud9, inclusive a Relacionados e Terceiros, quando necessário, conforme os Códigos Cloud9;
- (ii) Treinamento periódico dos Colaboradores, conforme Política de Treinamento e Reciclagem dos Colaboradores nos termos do Capítulo 6 deste Manual;
- (iii) Registros contábeis que reflitam as transações da Cloud9 de forma precisa e completa, feitos por empresa especializada externa;
- (iv) Independência dos procedimentos da Cloud9;
- (v) Medidas disciplinares executadas contra aqueles que violarem as normas da Cloud9, ou cometerem qualquer tipo de infração corruptiva listada acima; e
- (vi) *Due diligence* prévia à contratação de Terceiros conforme Política de Contratação de Terceiros nos termos do Capítulo 5 deste Manual.

Ademais, conforme mencionado acima, a Cloud9 não aceita e/ou aceitará a prática de qualquer das infrações apontadas nesta política, devendo os seus Colaboradores informar imediatamente ao Diretor de *Compliance* e Risco, o conhecimento de qualquer atividade mesmo que suspeita que essa e/ou se enquadre na caracterização das infrações previstas na Lei Anticorrupção conforme disposto nesta Política de Combate à Corrupção.

## **5 POLÍTICA DE CONTRATAÇÃO DE FUNCIONÁRIOS E TERCEIROS**

### **5.1 OBJETIVO**

A presente Política de Contratação de Terceiros tem como objetivo estabelecer os processos e procedimentos que devem ser observados quando da seleção, contratação e supervisão de colaboradores e terceiros – prestadores de serviços/fornecedores – visando garantir (i) a verificação de eventual conflito de interesse; (ii) que a condução da contratação seja feita de forma diligente; e (iii) definir as competências e responsabilidades pela contratação de um terceiro.

### **5.2 CADASTRO DE SEU COLABORADOR OU PARCEIRO – KNOW YOUR EMPLOYEE / PARTNER**

#### **5.2.1 COLABORADOR**

**Todos os colaboradores da Cloud9, independente do modelo da relação de trabalho adotado, devem passar por um processo de diligência antes da celebração do vínculo, com o objetivo de analisar se o mesmo cumpre com os requisitos solicitados e não possui questões reputacionais ou de qualquer natureza que possa acarretar risco a imagem ou a condução de qualquer atividade da gestora.**

**Neste sentido, serão solicitadas informações e documentos, realizadas pesquisas por processos administrativos e judiciais, da idoneidade do Terceiro e pesquisa de potenciais mídias negativas anteriores.**

**O início das atividades do Terceiro deve ser vinculado à formalização da contratação por meios da celebração do respectivo contrato.**

**Deverá ser mantida arquivada toda a documentação do processo de seleção e contratação dos colaborador, incluindo a pesquisa reputacional realizada.**

**Caso o terceiro não seja aprovado, a área de Compliance informará ao gestor da vaga e a justificativa da negativa.**

#### **5.2.2 PARCEIRO**

Quaisquer terceiros com os quais a Cloud9 tenha interesse em realizar negócios devem passar por um processo de diligência inicial com o objetivo de analisar a sua capacidade de prestar os serviços a serem contratados (“**Terceiros**”). Neste sentido, serão solicitadas informações e documentos, realizadas pesquisas por processos administrativos e judiciais e outros relacionados à prevenção e combate à lavagem de dinheiro e financiamento ao terrorismo, da idoneidade do Terceiro, questionamentos acerca de eventual mudança societária, a expertise, efetividade e qualidade dos serviços prestados.

Nesse sentido, Terceiros que venham a firmar relação contratual e/ou comercial com a Cloud9 passarão a ser considerados como “**Relacionados**”, para os fins deste Manual. Ademais e conforme aplicável, determinados Terceiros que venham a ser contratados pela Cloud9 podem vir a assinar acordos de confidencialidade, caso tenham acesso a Informações Confidenciais.

O início das atividades do Terceiro deve ser vinculado à formalização da contratação por meios da celebração do respectivo contrato.

Nos termos da regulamentação vigente, a contratação de Terceiros em nome dos veículos de investimentos geridos pela Cloud9 deve ser formalizada em contrato escrito e deve prever, no mínimo (i) as obrigações e deveres das partes envolvidas; (ii) a relação e as características dos serviços que serão contratados e exercidos por cada uma das partes; (iii) a obrigação de cumprir suas atividades em conformidade com as disposições previstas na regulamentação em vigor; e (iv) a obrigação de no limite de suas atividades deixar à disposição do administrador fiduciário e/ou da Cloud9 todos os documentos e informações exigidos pela regulamentação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais nos termos da regulamentação em vigor.

Todo processo de contratação de serviços deverá ser previamente apresentado pelo responsável da área que solicitou a contratação e, em seguida encaminhado para a área de *Compliance* coordenar o processo de *due diligence* e verificação de antecedentes. As regras para formalização do contrato e cadastro do Terceiro a ser contratado são estabelecidas pela área de *Compliance*, de acordo com o nível de sensibilidade de informações a serem transmitidas durante o relacionamento contratual, avaliando: (i) se o serviço poderá impactar os fundos de investimento; (ii) se as condições de ruptura contratual estão bem dimensionadas e eventual rescisão não impactará a Cloud9; (iii) existência de cláusula de confidencialidade e PLDFTP, dentre outros aspectos que se fizerem necessários para o caso concreto.

Deverá ser mantida arquivada toda a documentação do processo de seleção de prestadores de serviço, incluindo os orçamentos recebidos, as características técnicas do serviço, garantias, a aprovação da área da Cloud9 que solicitou a contratação, e-mail, recibos e notas de compra e quaisquer outros documentos e/ou informações relevantes. As obrigações e condições tratadas por telefone deverão ser formalizadas por e-mail, de forma a manter histórico das decisões tomadas e eventuais conflitos existentes.

Caso o terceiro não seja aprovado, a área de *Compliance* informará ao solicitante a justificativa da negativa, com cópia ao responsável da área.

### 5.3 SUPERVISÃO BASEADA EM RISCO PARA TERCEIROS CONTRATADOS

A área de *Compliance* da Cloud9 é responsável por realizar avaliações periódicas dos Terceiros contratados, de acordo com a classificação de risco atribuída ao final do processo de avaliação com o objetivo de destinar maior atenção aqueles contratados que venham a demonstrar maior probabilidade de apresentar falhas em sua atuação ou representem potencialmente um dano maior para os veículos de investimentos e para a integridade do mercado financeiro e de capitais.

A Cloud9 fará a análise de Relacionados e Terceiros a partir da classificação interna de risco descrita abaixo:

- (i) **Risco Baixo:** Terceiros e Relacionados cuja atividade não gera riscos estratégicos, legais/*compliance*, operacionais, financeiros/de crédito ou reputacionais para a Cloud9.
- (ii) **Risco Médio:** Terceiros e Relacionados cuja atividade gera ao menos um dos riscos acima apontados, ou tenham acesso a informações confidenciais dos fundos de investimento ou investidores, mas que demonstram procedimentos e controles

aparentemente satisfatórios. A avaliação será feita apenas por meio da declaração dos Terceiros e Relacionados em questionários e/ou conversas, reuniões e entrevistas.

- (iii) **Risco Alto:** Terceiros e Relacionados cuja atividade gera ao menos um dos riscos acima apontados, e que não são capazes de demonstrar a existência de controles satisfatórios e/ou que apresentam problemas cuja natureza pode trazer responsabilidade/implicações à Cloud9, como no caso de Terceiros e Relacionados que já foram envolvidos em escândalos de corrupção, lavagem de dinheiro, ou que estão sendo processados ou investigados pela prática de algum ato relacionado a sua atividade ou a atividade a ser prestada à Cloud9. Terceiros e Relacionados que não sejam associados ou aderentes aos códigos ANBIMA, mas que prestem serviços que são objeto destes códigos, serão automaticamente classificados como Alto Risco.

Cabe destacar que a Cloud9 não realizará testes para confirmar a efetividade dos controles internos dos Terceiros e Relacionados e tampouco é responsável pela gestão desses controles.

A partir do nivelamento dos Terceiros e Relacionados nos termos descritos acima ficará a área de Compliance responsável pela manutenção e atualização deste controle devendo manter uma atualização nos termos a seguir descritos:

- (i) **Risco Baixo:** atualização no mínimo a cada 36 meses;
- (ii) **Risco Médio:** atualização no mínimo a cada 24 meses; e
- (iii) **Risco Alto:** atualização no mínimo a cada 12 meses.

Não obstante a periodicidade definida acima, caso observado fatos novos relativos ao negócio ou a pessoa do Terceiro e/ou Relacionado, como por exemplo alterações no escopo da contratação inicial, a critério da área de Compliance, deverá ser conduzida reavaliação do Terceiro e/ou Relacionado, em razão de tais fatos, mesmo antes da periodicidade aqui mencionada.

#### **5.4 RESPONSABILIDADE E GESTÃO DE CRISE**

Esta política deve ser observada por todos os Colaboradores da Cloud9 e será monitorada e analisada pela área de *Compliance* da Cloud9.

Em caso de identificação de não conformidades no relacionamento contratual ou, se a qualquer momento do relacionamento, o terceiro seja envolvido em operações relacionadas à corrupção, fraude a licitação, suborno, ou qualquer outro crime ou ilícitos administrativos, a área de *Compliance* deliberará sobre a necessidade de encerramento imediato do relacionamento, mediante envio de notificação de rescisão contratual.

## **6 POLÍTICA DE TREINAMENTO**

### **6.1 OBJETIVO**

A Cloud9 incorpora ao processo de integração e treinamento inicial dos seus Colaboradores, a disponibilização dos códigos e políticas da companhia, e adota procedimentos visando a reciclagem contínua dos conhecimentos de tais Colaboradores

com relação aos princípios gerais e normas em especial as de *compliance* da Cloud9 descritas nesta Política de Treinamento, bem como às principais leis e normas aplicáveis às suas atividades.

## **6.2 TREINAMENTO INICIAL**

Assim que cada Colaborador passa fazer parte do time da Cloud9 e antes do início efetivo de suas atividades, este participará de um processo de integração e treinamento em que irá adquirir conhecimento sobre as atividades da Cloud9, suas atribuições e normas internas, políticas e códigos, além de informações sobre as principais leis e regulamentações relacionadas às atividades da Cloud9 e aos fundos de investimento sob sua gestão.

## **6.3 TREINAMENTO CONTÍNUO**

A Cloud9 entende que é fundamental que todos os Colaboradores se mantenham sempre atualizados, dos seus princípios éticos e das normas regulamentares, aplicáveis às atividades de gestão de recursos, em especial aqueles Colaboradores que possuam acesso a informações confidenciais.

Neste sentido, a Cloud9 adota um programa de reciclagem dos seus Colaboradores, com o objetivo de fazer com que eles estejam sempre atualizados sobre os termos e responsabilidades aqui descritos. O programa de reciclagem será executado no mínimo anualmente ou à medida que as regras e conceitos contidos nesta Política de Treinamento sejam atualizados e/ou a regulamentação aplicável a atividade da Cloud9 seja alterada.

Não obstante o referido programa de reciclagem, a Cloud9 ressalta que a área de *Compliance*, em especial o Diretor de *Compliance* e Risco, estarão sempre disponíveis para tirar quaisquer dúvidas dos Colaboradores a qualquer momento, com o intuito de manter os Colaboradores sempre em consonância com as regras dos órgãos reguladores e autorreguladores e da própria Cloud9.

Ademais, em caso de alguma alteração nas políticas da Cloud9, devido à exigência de órgãos reguladores ou por outros motivos, a Cloud9 poderá realizar um programa de reciclagem eventual para os Colaboradores, com o intuito de fornecer a nova política e também de apresentar as mudanças implementadas.

Por fim, cumpre salientar que o processo de treinamento inicial e o programa de reciclagem continuada são controlados pela área de *Compliance* sob a gestão do Diretor de *Compliance* e Risco e exigem o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação, sendo obrigatório a participação de todos os Colaboradores.

## **6.4 PROGRAMAS DE TREINAMENTO**

A Cloud9 entende que um programa eficaz de treinamento deve observar e assegurar que:

- (i) O treinamento seja contínuo, incorporando eventos atuais e mudanças nos códigos, políticas e produtos da Cloud9, bem como leis e regulamentos que digam respeito a sua atividade; e
- (ii) O treinamento se concentra em instruir os Colaboradores da Cloud9 quanto às políticas e valores da empresa, dispondo ainda sobre as consequências do descumprimento delas.

A área de *Compliance* terá a responsabilidade de controlar a frequência de todos os Colaboradores de modo a garantir que todos estejam presentes nos treinamentos

periódicos. Ademais, o Diretor de *Compliance* e Risco poderá também contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem nas dependências da Cloud9

## **7 POLÍTICA DE CONFIDENCIALIDADE**

### **7.1 TERMO DE CONFIDENCIALIDADE**

Conforme estabelecido no Termo de Responsabilidade e Confidencialidade constante no **Anexo II**, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a terceiros não Colaboradores da Cloud9. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais.

Qualquer informação sobre a Cloud9, seu *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo mas não limitando se a saldos, extratos e posições de clientes e/ou dos fundos geridos pela Cloud9, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Cloud9, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Cloud9 e/ou de seus sócios e clientes, obtida em decorrência do desempenho das atividades do Colaborador na, ou para a, Cloud9, só poderá ser fornecida à terceiros, ao público em geral, aos meios de comunicação de massa ou demais órgãos públicos ou privados se assim for previamente autorizado pelo Diretor de Compliance e Risco.

A informação obtida em decorrência da atividade profissional exercida na Cloud9 não pode ser divulgada, em hipótese alguma, a terceiros não Colaboradores ou a Colaboradores não autorizados. Enquadram-se neste item, por exemplo, posições compradas ou vendidas, estratégias de investimento ou desinvestimento, relatórios, estudos realizados (*Research*) – independentemente destas análises terem sido realizadas pela Cloud9 ou por terceiros contratados – opiniões internas sobre ativos financeiros, informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos pela Cloud9, transações realizadas e que ainda não tenham sido divulgadas publicamente, além daquelas estabelecidas no **Anexo II**.

Na questão de confidencialidade e tratamento da informação, o Colaborador deve observar e cumprir o estabelecido nos itens a seguir:

### **7.2 INFORMAÇÃO PRIVILEGIADA**

Considera-se informação privilegiada qualquer informação relevante a respeito de qualquer companhia ou outro ativo, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros) (“**Informação Privilegiada**”).

Qualquer informação deve ser considerada Informação Privilegiada se for capaz de influir na decisão de um investidor de comprar, manter ou vender um ativo financeiro. Além disso, devem ser consideradas materiais também informações que, caso sejam divulgadas,

tenham capacidade de impactar o preço de mercado de um ativo, seja positiva ou negativamente.

São exemplos de Informação Privilegiada: (i) transferência de controle; (ii) alterações em acordo de acionistas; (iii) entrada ou saída de acionistas relevantes; (iv) mudanças no conselho de administração ou na diretoria; (v) fusão, cisão ou qualquer outro tipo de reorganização societária que envolva a companhia; (vi) informação documentada ou verbal sobre os resultados operacionais da companhia; (vii) dissolução da companhia; (viii) mudanças na estrutura dos ativos da companhia; (ix) mudanças nos critérios contábeis adotados ou renegociações de dívidas; (x) anúncios de lucros ou prejuízos; ou (xi) qualquer fato que esteja sujeito a um acordo de confidencialidade assinado pela companhia com terceiros. Essa lista não é exaustiva e outros tipos de informações, eventos e circunstâncias podem vir a constituir Informação Privilegiada.

As Informações Privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal. O Colaborador que tiver acesso a uma Informação Privilegiada deverá divulgá-la imediatamente ao Diretor de *Compliance* e Risco, não devendo divulgá-la a ninguém mais, nem mesmo a outros integrantes da Cloud9, profissionais de mercado, amigos e parentes, e nem a utilizar, seja em benefício próprio ou de terceiros. Caso haja dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deve se abster de utilizar tal informação, seja em benefício próprio, de terceiros ou mesmo da Cloud9 e de seus clientes, bem como deve imediatamente relatar tal fato ao Diretor de *Compliance* e Risco. Todos aqueles que tenham acesso a uma Informação Privilegiada deverão, ainda, restringir totalmente a circulação de documentos e arquivos que contenham essa informação.

### 7.3 INSIDER TRADING, DIVULGAÇÃO PRIVILEGIADA E FRONT RUNNING

**7.3.1** *Insider Trading*: consiste na compra e venda de títulos ou valores mobiliários com base na utilização de Informação Privilegiada, visando à obtenção de benefício próprio ou de terceiros ("*Insider Trading*").

**7.3.2** *Divulgação Privilegiada*: é a divulgação, a qualquer terceiro, de Informação Privilegiada que possa ser utilizada com vantagem na compra e venda de títulos ou valores mobiliários ("**Divulgação Privilegiada**").

**7.3.3** *Front Running*: é a prática de aproveitar alguma Informação Privilegiada para concluir uma negociação antes de outros ("*Front Running*").

É vedada a prática de quaisquer das ações acima referidas por qualquer integrante da Cloud9, seja atuando em benefício próprio, da Cloud9, de seus clientes, ou de terceiros. Deve ser observado o disposto nos itens de "Informação Privilegiada", "*Insider Trading*", "Divulgação Privilegiada" e "*Front Running*" não só durante a vigência de seu relacionamento profissional com a Cloud9, mas mesmo depois do seu término.

A utilização ou divulgação de Informação Privilegiada, *Insider Trading*, *Divulgação Privilegiada* e *Front Running* sujeitará os responsáveis às sanções previstas neste Manual, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Cloud9, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Cloud9, e ainda às consequências legais cabíveis. Diante do exposto, é expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de

títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas nestes Códigos Cloud9 e na legislação aplicável.

## **8 POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E CONFLITO DE INTERESSE**

### **8.1 INTRODUÇÃO**

O Colaborador tem o dever de agir com boa-fé e de acordo com os interesses dos investidores e da Cloud9 com o intuito de não ferir a relação fiduciária da mesma junto ao cliente, para tal, o Colaborador deverá estar atento para uma possível situação de conflito de interesses, e sempre que tal situação ocorrer deverá informar, imediatamente, ao seu superior hierárquico e ao Diretor de *Compliance* e Risco sobre sua existência e abster-se de consumir o ato ou omissão originador do conflito de interesses até decisão em contrário.

### **8.2 SEGREGAÇÃO DE ATIVIDADES E CONFLITO**

As atividades desenvolvidas pela Cloud9 são reguladas pela CVM e, portanto, exigem credenciamento específico e estão condicionadas a uma série de providências, dentre elas a segregação da gestão de carteiras de valores mobiliários de outras atividades potencialmente conflitantes que sejam ou possam vir a ser desenvolvidas pela Cloud9 ou empresas controladoras, controladas, ligadas ou coligadas no âmbito do mercado de capitais, bem como prestadores de serviços.

Atualmente, a Cloud9 desenvolve a atividade regulada de gestão de carteiras de valores mobiliários. Ainda, a Cloud9 não tem a intenção de realizar outras atividades reguladas que possam gerar conflitos adicionais, observado que se e quando necessário, a Cloud9 assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a segregação de suas atividades, adotando procedimentos operacionais objetivando, sempre que possível, a mitigação de conflitos de interesses.

Não obstante o disposto acima, importante destacar que a Cloud9 prestará também os serviços de consultoria e suporte a investimentos em *Private Equity*, atividade que não é regulada pela CVM. Ocorre que, considerando a natureza das atividades de consultoria que venham a ser prestadas, existe potencial para conflitos de interesses reais ou aparentes com a Cloud9. Tais potenciais conflitos de interesse deverão ser previamente identificados, monitorados e divulgados pela Cloud9 aos seus investidores e aos clientes objeto dos serviços de consultoria. A Cloud9 possui como preceitos básicos a transparência e divulgação às partes envolvidas em situações de potencial conflito de interesses entre seus fundos e clientes, preceitos estes corroborados, por exemplo, na regulamentação aplicável aos fundos de investimento em participações, que exige necessariamente a divulgação e aprovação de atos que configurem potencial conflito de interesses nos termos dos artigos 9º e 24, inciso XII da Instrução da CVM n.º 578, de 30 de agosto de 2016, conforme alterada.

Assim, mesmo na realização da prestação dos serviços de consultoria para eventuais clientes, a Cloud9 sempre manterá a preferência de investimentos em novos ativos voltada aos fundos de investimento que estiverem sob sua gestão e/ou aos potenciais clientes que tenham a intenção de realizar investimentos nos fundos da Cloud9 .

### **8.3 CONFLITO DE INTERESSES**

Conflitos de interesses são situações decorrentes do desempenho das funções de determinado Colaborador, nas quais os interesses pessoais de tal Colaborador possam ser divergentes ou conflitantes com os interesses da Cloud9 e/ou entre os interesses diferentes de seus clientes (“**Conflito de Interesses**”).

Em situações de Conflito de Interesses o Colaborador tem o dever de agir com boa-fé e de acordo com os interesses dos investidores com o intuito de não ferir a relação fiduciária existente entre a Cloud9 e seus Colaboradores junto ao cliente. Neste sentido, o Colaborador deverá estar atento para uma possível situação de conflito de interesses e, sempre que tal situação ocorrer, deverá informar, imediatamente, ao Diretor de *Compliance* e Risco sobre sua existência e abster-se de consumir o ato ou omissão originador do Conflito de Interesse até decisão em contrário.

Tendo sido devidamente notificado do potencial Conflito de Interesses, o Diretor de Compliance e Risco deverá avaliar e preparar um relatório, com base nos preceitos dos Códigos Cloud9, contemplando sua recomendação a respeito do potencial Conflito de Interesses e enviá-lo ao Comitê de Risco e Conformidade para decisão final sobre qual ação a Cloud9 e, conseqüentemente, o Colaborador deverá tomar quanto ao potencial Conflito de Interesse.

Ademais, a ampla divulgação de potenciais conflitos de interesses aos seus clientes é o meio mais eficaz de segregação de atividades e mitigação de conflitos de interesses. Portanto, além do *disclosure* dos Códigos Cloud9 disponíveis ao público, quando do exercício de suas atividades, os Colaboradores devem atuar com a máxima lealdade e transparência com os clientes.

Por fim, é proibido que Colaboradores desenvolvam qualquer atividade paralela concorrente e/ou incompatível com o negócio conduzido pela empresa, ou, ainda, que possam gerar conflitos de interesse, ainda que potenciais, com as atividades desempenhadas pela instituição, neste sentido, qualquer atividade paralela que interfira ou que possa interferir no trabalho ou no desempenho do Colaborador estará condicionada à autorização prévia e expressa do Diretor de Compliance e Risco.

Não é permitido que Colaboradores:

- (i) exerçam atividades político-partidárias nas dependências da empresa;
- (ii) utilizem bens ou recursos da Cloud9 para causas ou campanhas políticas;
- (iii) deixar que suas atividades externas, ou o tempo gasto com elas, interfiram em seu desempenho no trabalho;
- (iv) tomar para si mesmos uma oportunidade de negócios da Cloud9; e
- (v) envolver-se em negócios que compitam com os negócios da Cloud9.

Os Colaboradores devem solicitar aprovação prévia do Diretor de Compliance e Risco antes de exercerem as seguintes atividades:

- (i) Qualquer atividade externa remunerada, incluindo projetos esporádicos, um segundo emprego ou serviço remunerado prestado para organizações sem fins lucrativos;
- (ii) Qualquer afiliação com outras empresas ou negócios, remunerada ou não, na condição de diretor, conselheiro, administrador, consultor, detentor de qualquer cargo oficial ou sócio com 5% ou mais de participação no negócio;

- (iii) Qualquer posição governamental, remunerada ou não, eleita ou indicada, incluindo membro, diretor, gerente ou funcionário de agência, autoridade, conselho consultivo ou outro órgão governamental;
- (iv) Qualquer candidatura a cargo eletivo;
- (v) Qualquer posição em conselho, comitê de investimento ou outro cargo oficial em entidades sem fins lucrativos;
- (vi) Qualquer atividade em entidades sem fins lucrativos a pedido de clientes ou fornecedores, ou quando a própria entidade for cliente da Cloud9; e
- (vii) Qualquer atividade que represente um Conflito de Interesse ou um risco substancial à reputação da Cloud9.

## **9 POLÍTICA DE CERTIFICAÇÃO CONTINUADA**

### **9.1 OBJETIVO**

A presente Política de Certificação Continuada (“**Política de Certificação**”) é parte integrante da governança corporativa da Cloud9 e visa definir as diretrizes e regras para que todos os Colaboradores possuam certificação adequada e necessária para exercer suas respectivas funções junto à Cloud9 em conformidade com a regulamentação vigente em especial as disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada (“**Código ANBIMA**”) e demais normativos aplicáveis.

### **9.2 ÁREA RESPONSÁVEL**

A área de *Compliance* será responsável por adotar controles que garantam o cumprimento desta Política de Certificação, bem como será responsável pelo monitoramento contínuo dos Colaboradores de modo a supervisionar que eles mantenham devidamente atualizadas e válidas quaisquer das certificações exigidas pelo Código ANBIMA e demais regulamentações aplicáveis.

Ainda, a área de *Compliance* será responsável por, no momento de contratação de um novo profissional, solicitar esclarecimentos ou confirmar junto ao gestor da área responsável se o profissional a ser contratado necessita de certificação em decorrência das funções a serem desempenhadas na Cloud9. Caso positivo caberá a área de *Compliance*, em conjunto com o gestor da área responsável pela contratação, a verificação se o referido profissional possui a certificação necessária nos termos desta política.

Em caso de dúvidas acerca do conteúdo desta Política de Certificação, os Colaboradores poderão entrar em contato a área de *Compliance* e/ou o Diretor de *Compliance* e Risco.

### **9.3 MONITORAMENTO E CONTROLE DE PRAZOS**

A área de *Compliance* será responsável por monitorar o prazo de vencimento da certificação ou isenção daqueles Colaboradores que necessitam dela para exercer sua atividade, exigindo sua atualização, quando de seu vencimento. Caberá também a área de *Compliance* a atualização dos Colaboradores no Banco de Dados da ANBIMA inclusive em relação à novas contratações e/ou demissões, de acordo com as diretrizes expedidas pelo Código ANBIMA e demais regulamentações aplicáveis.

## 9.4 ATIVIDADES ELEGÍVEIS

Atualmente, a Cloud9 realiza exclusivamente a atividade de gestão de recursos, em especial a gestão de carteira de valores mobiliários de fundos de investimento de participações (os FIPs). Neste sentido, a área de gestão é a única elegível à certificação segundo o Código ANBIMA por desempenhar atividade de gestão profissional de recursos de terceiros.

Será obrigatória a obtenção do credenciamento aplicável (conforme descrito abaixo) para todos os Colaboradores responsáveis pela atividade de gestão de recursos de terceiros e que tenham alçada e/ou poder discricionário para decidir sobre a compra e venda de ativos financeiros integrantes das carteiras dos fundos de investimento geridos pela Cloud9, salvo exceções previstas na regulamentação.

Nesse contexto, é obrigatória a obtenção da:

- (i) Certificação de ANBIMA de Fundamentos em Gestão (CFG); e
- (ii) Certificação de Gestores ANBIMA para Fundos Estruturados (CGE)

Os demais Colaboradores que exercem atividades de apoio à área de gestão não são elegíveis a certificação por não desempenharem as atividades acima mencionadas. Caso a Cloud9 venha a desempenhar outras atividades que demandem certificação, essa Política de Certificação deverá ser alterada, de forma a incluir referida atividade como uma atividade elegível.

### 9.4.2 Afastamento de Colaboradores

O profissional elegível que não regularizar a renovação de sua certificação ou isenção até a data de vencimento será informado pelo diretor responsável que ficará afastado da respectiva atividade elegível, e passará a atuar apenas em atividades de apoio. Nesse caso, o Colaborador receberá um e-mail da área de *Compliance* sobre seu afastamento e terá suas senhas de acesso aos sistemas de negociação e às corretoras bloqueados, até a obtenção da sua devida verificação.

Na hipótese mencionada acima, tal Colaborador somente retomará suas atividades após a devida regularização da certificação e envio de comprovação à área de *Compliance*. Após a verificação da documentação pela área de *Compliance* e a devida atualização junto ao Banco de Dados da ANBIMA, a área de *Compliance* comunicará, ao diretor responsável pela área elegível, que o profissional afastado está devidamente regularizado e poderá voltar as suas atividades.

## 9.5 INGRESSOS, TRANSFERÊNCIA E SAÍDA DE COLABORADORES

### 9.5.1 Ingresso de Colaboradores

Conforme mencionado acima, antes da admissão de qualquer profissional, a área de *Compliance* deverá solicitar esclarecimentos ou confirmar junto ao gestor da área responsável se o profissional a ser contratado necessita de certificação para atividade de suas funções. Caso seja necessária a certificação e o profissional a ser contratado não possua tal certificação, este receberá no momento de sua contratação, instruções adequadas sobre a necessidade de certificação dependendo da atividade que irá exercer.

O profissional que não apresentar a certificação necessária deverá ficar impedido de dar início às atividades pelas quais foi contratado a exercer. Se completado o

prazo estabelecido para retirada da certificação e o profissional não tiver apresentado, caberá à área de *Compliance* a comunicação ao responsável pela área em que o profissional foi contratado informando que o profissional ainda não está habilitado a exercer as atividades pelas quais foi contratado. A decisão sobre remanejá-lo em outra área ou mantê-lo em atividades não elegíveis tendo suas atividades supervisionadas por funcionários que possuem a certificação, até a retirada da certificação, será do responsável pela área contratante juntamente com a área de *Compliance*.

Caso o profissional já possua certificação caberá a área de *Compliance* verificar se seu certificado é compatível com a atividade que o profissional irá desempenhar bem como se está em perfeita ordem. Caso esteja de acordo com os requisitos regulamentares a área de *Compliance* deverá efetuar os devidos registros do novo Colaborador junto às instituições pertinentes.

#### **9.5.2 Mudança de área ou função**

A área de *Compliance* será previamente comunicada de qualquer transferência interna de Colaboradores. Na hipótese do Colaborador ser transferido para função que exija certificação, a transferência ficará sujeita ao cumprimento de todas as etapas de verificação e controle estabelecidos acima, em especial ao disposto no item “Ingresso de Colaboradores”. Ademais, o gestor responsável pela área elegível deverá manter um substituto devidamente certificado para a respectiva atividade.

Na hipótese de um Colaborador sair de uma área que exija certificação para uma outra, que não exija certificação, a transferência ocorrerá de imediato, devendo a área de *Compliance* atualizar as informações do profissional e desvinculá-lo do Banco de Dados da ANBIMA.

#### **9.5.3 Licenciamento de Profissional Certificado**

As áreas consideradas atividades elegíveis nos termos da regulamentação vigente deverão manter, ao menos, um substituto devidamente certificado apto para assumir as funções do cargo em vacância. Os Colaboradores em período de licença deverão ser atualizados no Banco de Dados da ANBIMA, para que não continuem vinculados como se ativos fossem. Quando retornarem de licença, a área de *Compliance* providenciará novamente a vinculação ao Banco de Dados do referido Colaborador. Colaboradores em licença serão comunicados caso o certificado esteja perto de seu vencimento e/ou vencido e este somente poderão retornar as suas atividades mediante regularização de sua certificação devidamente atestada e verificada pela área de *Compliance*.

#### **9.5.4 Certificação**

O Colaborador deverá se inscrever no site de certificação da instituição competente e escolher a melhor data disponível para a prova. O Colaborador ficará responsável desde o seu cadastro nos respectivos sites ao pagamento da inscrição até a realização do exame e todos os procedimentos necessários para a emissão de eventual certificação. Devendo comunicar a área de *Compliance* qualquer situação que enseje atraso na obtenção da certificação pretendida.

#### **9.5.5 Processo de Desligamento**

Todos os Colaboradores que desempenham atividades elegíveis sem a devida certificação ou com a certificação vencida serão afastados imediatamente de suas atividades. No caso de desligamento, a área de *Compliance* deverá desvincular o profissional do Banco de Dados da ANBIMA em até 15 (quinze) dias da data do desligamento.

#### **9.6 ATUALIZAÇÃO DO BANCO DE DADOS**

Cabe a área de *Compliance* a manutenção atualizada do Banco de Dados da ANBIMA. Diante do exposto, os Colaboradores desligados, admitidos e transferidos deverão ser atualizados no Banco de Dados até o último dia do mês subsequente, considerando a data do evento, nos termos da autorregulamentação vigente.

## ANEXO I

### *Termo de Compromisso*

Por meio deste instrumento eu, \_\_\_\_\_, inscrito no CPF sob o nº \_\_\_\_\_, declaro para os devidos fins que:

- 1 Recebi, li e compreendi os seguintes manuais e políticas internas da **CLOUD9 CAPITAL LTDA. ("Cloud9")**, me comprometendo a observar integralmente todas as disposições constantes nos manuais e políticas internas durante o desempenho de minhas funções:
  - (i) Manual de Compliance;
  - (ii) Código de Ética;
  - (iii) Política de Investimentos Pessoais;
  - (iv) Política de Rateio e Divisão de Ordens;
  - (v) Política de Gerenciamento de Risco; e
  - (vi) Manual de Cadastro e Prevenção e Combate à Lavagem de Dinheiro.
- 2 Estou ciente de que as políticas e manuais acima passam a fazer parte dos meus deveres como Colaborador da Cloud9, incorporando-se às demais regras de conduta adotadas.
- 3 Comprometo-me, ainda, a informar imediatamente a Cloud9 qualquer fato que eu venha a ter conhecimento que possa gerar algum risco para a Cloud9.
- 4 A partir desta data, a não observância de qualquer política interna poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades regulamentares cabíveis, inclusive eventual obrigação de indenizar a Cloud9 e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.
- 5 Entendo que as regras estabelecidas nas políticas internas da Cloud9 apenas servem de complemento e esclarecem como lidar com determinadas situações relacionadas à minha atividade profissional e, portanto, não invalidam nenhuma disposição contratual de trabalho e/ou societária.
- 6 Esclareci todas as minhas dúvidas relacionadas aos princípios e normas estabelecidos pela Cloud9 em seus manuais e políticas internas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento e de reciclagem a ser conduzido pela Cloud9.
- 7 Tenho ciência de que é terminantemente proibido fazer cópias (físicas ou eletrônicas) ou imprimir os arquivos utilizados, gerados ou disponíveis na rede da Cloud9 e circular em ambientes externos à Cloud9 com estes arquivos sem a devida autorização, uma vez que tais arquivos podem conter informações confidenciais.
- 8 Tenho ciência de que a Cloud9 poderá gravar qualquer ligação telefônica realizada ou recebida por meio das linhas telefônicas disponibilizadas pela Cloud9 para minha atividade profissional.
- 9 Tenho ciência de que a Cloud9 monitora toda e qualquer troca, interna ou externa, de meus e-mails, bem como meus acessos a sites e arquivos eletrônicos.

- 10** Tenho ciência de que a senha e *login* para acesso aos dados contidos em todos os computadores, inclusive nos e-mails, são pessoais e intransferíveis, de modo que me comprometo a não os divulgar para outros Colaboradores da Cloud9 e/ou quaisquer terceiros.
- 11** As regras estabelecidas nas políticas e manuais internos da Cloud9 não invalidam nenhuma disposição do contrato de trabalho, nem de qualquer outra regra estabelecida pela Cloud9, mas apenas servem de complemento e esclarecem como lidar com determinadas situações relacionadas à minha atividade profissional.
- 12** Declaro que participei do processo de integração e treinamento inicial da Cloud9, onde tive conhecimento das normas internas, especialmente sobre as descritas neste termo, além das principais leis e normas que regem as atividades da Cloud9 e me comprometo a participar assiduamente do programa de treinamento continuado.
- 13** Por fim, cabe ressaltar que as informações e regras descritas nos Códigos Cloud9 se complementam com o disposto do contrato de vínculo empregatício que tenho firmado com a Cloud9 e com outras regras estabelecidas pela Cloud9, que deixam claro o comportamento esperado dos Colaboradores e terceiros em relação às atividades vinculadas à minha função profissional.

São Paulo, \_\_\_ de \_\_\_\_\_ de 20\_\_

---

**Nome Colaborador**

## ANEXO II

### *Termo de Responsabilidade e Confidencialidade*

Através deste instrumento, \_\_\_\_\_, inscrito no CPF sob o nº \_\_\_\_\_, doravante denominado “Colaborador” e Cloud9 Capital Ltda., inscrita no CNPJ sob o n.º 42.517.868/0001-03 (“**Cloud9**”), resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da Cloud9, celebrar o presente termo de responsabilidade e confidencialidade (“**Termo**”), que deve ser regido de acordo com as cláusulas que seguem:

- 1 São consideradas informações confidenciais (“**Informações Confidenciais**”), para os fins deste Termo:
  - (i) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Cloud9, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para um fundo de investimento gerido pela Cloud9, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Cloud9 e a seus sócios ou clientes, independente destas informações estarem contidas em *pen-drives*, HDs, outros tipos de mídia ou em documentos físicos;
  - (ii) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Cloud9, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Cloud9 e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela Cloud9 ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.
- 1.1 Não são consideradas Informações Confidenciais quaisquer informações que:
  - (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador;
  - (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo;
  - (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade;
  - (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade;
  - (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Diretor de *Compliance* e Risco da Cloud9 para que as medidas legais cabíveis sejam tomadas, observado o disposto no item 5 deste Termo.

- 2** O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Cloud9, comprometendo-se, portanto, observadas as disposições dos Códigos Cloud9, a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas à Cloud9, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.
- 2.1** O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Cloud9.
- 2.2** As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela Cloud9.
- 2.3** A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.
- 3** O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Cloud9 e terceiros, ficando desde já o Colaborador obrigado a indenizar a Cloud9, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.
- 3.1** O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis do Trabalho e desligamento ou exclusão por justa causa do Colaborador se este for sócio da Cloud9, sem prejuízo do direito da Cloud9 de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.
- 3.2** O Colaborador expressamente autoriza Cloud9 a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízo do direito da Cloud9 de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.
- 3.3** A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, conforme mencionado nos itens 2 e 2.1 acima.
- 3.4** O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.
- 4** O Colaborador reconhece e toma ciência que:
  - (i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas/físicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Cloud9 são e permanecerão sendo propriedade exclusiva da Cloud9 e de seus sócios, razão pela

qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Cloud9, devendo todos os documentos permanecer em poder e sob a custódia da Cloud9, salvo se em virtude de interesses da Cloud9 for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Cloud9;

- (ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Cloud9 todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;
- (iii) Nos termos da Lei n.º 9.609, de 19 de fevereiro de 1998, conforme alterada, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Cloud9, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei;
- (iv) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela Cloud9 em seu equipamento; e
- (v) A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

**5** Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Cloud9, permitindo que a Cloud9 procure a medida judicial cabível para atender ou evitar a revelação.

**5.1** Caso a Cloud9 não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

**5.2** A obrigação de notificar a Cloud9 subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

**6** Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Cloud9, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

**6.1** A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelo Diretor de *Compliance* e Risco, conforme descrito no Código.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

São Paulo, \_\_\_ de \_\_\_\_\_ de 202\_\_

---

**Nome Colaborador**

---

**CLOUD9 CAPITAL LTDA.**

Testemunhas:

1. \_\_\_\_\_

Nome:

RG:

CPF:

2. \_\_\_\_\_

Nome:

RG:

CPF:

\* \* \*