POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E CONFIDENCIALIDADE

2023/4

Curitiba/PR

VERSÕES

Versão	Data	Responsável	Aprovação
2020/1	20/07/2020	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2020/2	08/10/2020	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2022/3	15/02/2022	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance
2023/4	10/03/2023	Diretor de Risco, Compliance e PLDFT	Comitê de Compliance

Sumário

1. INTRODUÇÃO 4
2. ABRANGÊNCIA 4
3. IMPLEMENTAÇÃO E REVISÃO 4
4. RESPONSABILIDADE 5
5. ENDEREÇO ELETRÔNICO 5
6. SEGREGAÇÃO DO COMPLIANCE 5
6.1 Segregação Estrutural, Física e de Funções 5
7. *CHINESE WALL* E SEGREGAÇÃO DE FUNÇÕES 6
8. CONFLITOS DE INTERESSES 7
8.1. Atividades de Colaboradores Alheias à SIGA 7
8.2. Identificação de Conflito de Interesses 8
8.3. Declaração de Conflito de Interesses 9
9. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO 9
9.1. Objetivo e a Quem se Aplica 9
9.2. Definições 10
9.3. Diretrizes 11
9.4. Controles e Barreiras 11
9.5. Segurança Cibernética 13
9.6. Testes de Segurança 16
10. DISPOSIÇÕES GERAIS E FINAIS 17
ANEXO I 18

1. INTRODUÇÃO

A Política de Segregação de Atividades e Confidencialidade visa estabeleceras orientações aptas a garantir as devidas segregações de atividades e a confidencialidade necessária ao atendimento das funções da SIGA, em conformidade com o artigo 28, incs. I e II, da Resolução da Comissão de Valores Mobiliários (RCVM) nº 21/2021.

Por intermédio deste instrumento, visa-se o atendimento integral e ininterrupto às normas, políticas e regulamentações vigentes, mas não se limitando a isto. Visa, também, a transparência na condução dos negócios, a salvaguarda da confidencialidade das informações outorgadas pelos clientes, obliterar o conflito de agência entre os diversos atores da entidade, evitar ganhospessoais indevidos por meio da criação de condições artificiais de mercado ou da manipulação e uso de informação privilegiada.

A Política, ademais, teve seu desenvolvimento voltado ao cumprimento das obrigações objetivadas pelas Instruções da Comissão de Valores Mobiliários, entre as quais destacamos ICVMs n. 356/2001, 472/2008, RCVMs n. 21/2021, 35/2021, 50/2021, pela legislação aplicável e demais práticasnacionais e internacionais aplicadas à política de *Compliance*.

2. ABRANGÊNCIA

Este Manual é aplicável aos administradores, colaboradores, estagiários, terceirizados e operadores envolvidos com negócios e atividades da SIGA, bemcomo aos sócios da gestora.

3. IMPLEMENTAÇÃO E REVISÃO

A implementação desta Política se dará de forma imediata, após a aprovaçãoda Diretoria e será revisada, no mínimo, anualmente, ou em qualquer tempo quelhe possa agregar valor, de acordo com a relevância, para que seja garantida asua adequação.

O planejamento de *Compliance* e Controles Internos é efetuado anualmente,com o objetivo de revisar e atualizar todos os procedimentos, códigos, manuaise políticas da SIGA. Essa atividade coincidirá com a entrega do Relatório Anualde Controles Internos e Cumprimento da RCVM nº 21/2021, no prazo legal.

Em caso de mudanças significativas nos negócios ou na regulação, planos devem ser alterados. Deficiências de Controles Internos detectadas devem ser relatadas para as áreas responsáveis por tais controles e reportadas ao Comitêde *Compliance*.

Revisões extraordinárias destes procedimentos, códigos, manuais e políticaspoderão ocorrer em

caso de situações imprevistas e/ou mudanças significativase repentinas, também com vistas a apurar a permanência da conformidade.

4. RESPONSABILIDADE

Compete ao Diretor de Risco, *Compliance* e Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLDFT) a gestão e a aplicação desta Política. Ressalta-se, ainda, que este documento não detalha, necessariamente,todas as situações passíveis de ocorrência no dia a dia dos negócios. Quaisquerdúvidas deverão ser remetidas ao Diretor de Risco, *Compliance* e PLDFT.

5. ENDEREÇO ELETRÔNICO

Em respeito ao artigo 16, inciso II, da RCVM nº 21/2021, este documentoestará disponível no site da SIGA (www.sigafinance.com.br).

6. SEGREGAÇÃO DO SETOR DE *COMPLIANCE*

O Diretor de Risco, *Compliance* e PLDFT atua em funções de supervisão, controle e jurídico, em área segregada daquelas utilizadas para a operacionalização dos negócios da SIGA. É considerado profissional *behind all barriers*, na forma das melhores práticas vigentes, sob quem recai o dever legal de zelar pela perfeita segregação de atividades da entidade.

A SIGA atua com a premissa de que a Diretoria de Risco, *Compliance* e PLDFT deve ser completamente independente, de modo que não haja interferência no trabalho por esta desenvolvido.

A segregação funcional da Diretoria de Risco, *Compliance* e PLDFT e demais órgãos da entidade é garantida pela SIGA, de forma a fornecer ao Diretorde Risco, *Compliance* e PLDFT meios para que possa agir de modo independente, fiscalizar qualquer tipo de conduta imprópria e com poderes para vedar a realização de determinados negócios.

6.1 Segregação Estrutural, Física e de Funções

A SIGA preza pela prevenção e remediação de qualquer caso de conflito deinteresses. Desta forma, os órgãos da entidade são independentes entre si, de modo que previna o conflito de agência. Para tanto, conta com diversas políticasneste sentido.

Todos os colaboradores da SIGA que tiverem suas atividades profissionais relacionadas com a administração de ativos e carteiras de valores mobiliários, nos termos dos artigos 27 e 28 da RCVM nº 21/2021, serão alocados para desempenhar suas funções em local diverso e fisicamente segregado

dos demais colaboradores. Caracteriza-se como administração de ativos e carteiras de valores mobiliários os profissionaisque atuam com:

(i) Gestão de Fundos de Investimentos;
(ii) Originação de novos negócios;
(iii) Gestão de risco dos Fundos de Investimentos;
(iv) *Compliance* e Prevenção à Lavagem de Dinheiro;
(v) Distribuição de ativos;
(vi) Qualquer outra função que detenha informações privilegiadas.

Ainda, cada colaborador deverá firmar um Termo de Adesão, anexo ao presente instrumento (Anexo I), atestando expressamente o seu conhecimentoacerca das regras estabelecidas nesta Política, comprometendo-se a cumpri-las.

A Diretoria e o Comitê de *Compliance* da SIGA visarão promover a aplicação das regras aqui contidas, de forma a assegurar a segregação física dasinstalações entre áreas responsáveis pelas atividades prestadas pela empresa.

7. *CHINESE WALL* E SEGREGAÇÃO DE FUNÇÕES

A RCVM nº 21/2021, impõe a segregação da atividade de administração de carteiras de valores mobiliários das demais atividades exercidas pela pessoa jurídica.

Entende-se tal segregação pelo conjunto de procedimentos internos adotados com o objetivo de impedir o acesso e o fluxo de informações confidenciais, sigilosas e privilegiadas entre setores alheios à atividade deadministração de carteiras de valores mobiliários, de forma a evitar vazamento de informações, conflito de interesses ou quaisquer das práticas vedadas pela RCVM nº 62/2022 ou pela Lei nº 6.385/1976.

Para tanto, a área de administração de carteiras de valores mobiliários da SIGA deverá estar em um ambiente físico isolado, com acesso exclusivo para os colaboradores que a integram, respeitando todos os níveis de segregação a seguir:

a. Segregação de Atividades e Funções: O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para cada um dos colaboradores.
b. Segregação Física: A área de c*ompliance* é segregada das áreas de análise e gestão. Além disso, a área financeira, administrativa e pagamentos é separada das áreas de *compliance* e análise.
c. Segregação de Acessos a Documentos: Controle de acessos a documentos e segregação física com acesso restrito aos documentos de cadastro de clientes e de colaboradores, prevenção de informações confidenciais por todos os colaboradores.

Na sede da SIGA, além dos espaços destinados a Recepção, Copa, Banheiros, Sala de Reuniões, existem salas segregadas para as áreas de Gestão e Distribuição e para a área de Risco, *Compliance* e PLDFT.

8. CONFLITOS DE INTERESSES

Extensivamente às regras de segregação, tendo em vista a grande preocupação da SIGA em adotar a mais rígida política de identificação, eliminação e mitigação de quaisquer conflitos de interesses, inclusive no que se refere a partes relacionadas.

Para tanto, a SIGA conta com as obrigatoriedades previstas neste capítulo.

8.1. Atividades de Colaboradores Alheias à SIGA

Todos os colaboradores com participações em outras entidades, que deterem mais de 10%, direta ou indiretamente, de participação, bem como se ocuparem cargos de diretoria ou conselhos, tendo influência significativa na tomada de decisões, deverão declarar à SIGA tais fatos.

São consideradas transações com partes relacionadas a transferência de recursos, bens, serviços ou obrigações entre pessoas físicas ou jurídicas definidas no parágrafo acima, independentemente de haver ou não um valor pecuniário atribuído à transação.

O conflito de interesses, neste caso, irrompe quando uma parte relacionadase encontra envolvida em processo decisório, ou de assessoramento, que tenhao condão de resultar em um ganho para si, para algum familiar, ou para terceiro com o qual esteja envolvido, ou ainda que possa interferir na sua capacidade de julgamento isento, em qualquer caso, desde que em detrimento dos interesses da SIGA e dos clientes.

Os colaboradores da SIGA, em regra, não poderão ter atuação funcional relevante em outras atividades, exceto como conselheiros ou consultores em entidade cujos objetivos sociais não sejam conflitantes com a entidade.

Ademais, estas atividades somente poderão ser realizadas se aprovadas, por ata, pelo Comitê de *Compliance*, se limitadas a 20 (vinte) horas mensais e que não conflitem com as atividades da SIGA.

Estes colaboradores, ainda, deverão assinar um termo de responsabilidade,assumindo o dever de observação das regras de conflitos de interesses, informações confidenciais e privilegiadas, e todas as demais regras dispostas nos manuais da SIGA, sob pena de desligamento e multas relevantes, sem prejuízo de indenização por perdas e danos e processos judiciais criminais e administrativos.

Estas atividades restritas não poderão ser exercidas dentro do estabelecimento da SIGA e nem com os equipamentos (notebooks) de propriedade da entidade. É vedado o salvamento de quaisquer

arquivos estranhos à SIGA nas pastas físicas e virtuais do servidor da entidade.

Neste sentido, a SIGA demonstrará publicamente, na forma da regulamentação aplicável, qualquer tipo de conflito, potencial ou material, que seja decorrente desta situação, por intermédio de regulamentos ou documentação acessória dos veículos de investimento, questionários de *due diligence* de prestadores de serviços, formulários de referência etc.

8.2. Identificação de Conflito de Interesses

No caso da SIGA, também podem ser consideradas como situações envolvendo conflitos de interesses aquelas nas quais os objetivos pessoais dos tomadores de decisão, por qualquer razão, não estejam alinhados aos objetivosda entidade e de seus clientes.

Na hipótese de mera suspeita de conflitos de interesses nas atividades extra laborais dos colaboradores, inclusive sócios, diretores e administradores, os envolvidos serão chamados a comparecer em reunião extraordinária do comitê de *compliance*, que ouvirá este sujeito e deliberará se:

(i) Não há conflito de interesses;

(ii) Há conflito de interesses e, portanto, deverá deixar de praticar determinada atividade;

(iii) Há conflito de interesses e será desligado da SIGA;

(iv) Sem prejuízo, o colaborador poderá ser afastado das operações em andamento, ou do próprio trabalho, por prazo definido pelo comitê.

Qualquer suspeita deverá ser objeto de denúncia à diretoria de compliance ou ao administrador da entidade, quando aquele for impedido para deliberar.

O Diretor de Risco, *Compliance* e PLDFT é o responsável por identificar qualquer outra situação que possa gerar conflito de interesses. Nesta hipótese, a depender do tipo, risco e materialidade do conflito, o Diretor de Risco, *Compliance* e PLDFT deverá proceder à instauração de alguma(s) das seguintes medidas:

I. Vedar a operação.
II. Estabelecer barreiras de informação, com o objetivo de isolamento dacirculação de dados.
III. Retirar da operação e afastar o(s) colaborador(es) que tenha(m) relaçãocom o conflito.
IV. Informar a investidores e ao mercado.
V. Aprovar previamente a deliberação em assembleias dos demais titularesde ativos investidos.

Caso qualquer colaborador note que pode haver ou suspeite haver potenciais conflitos de interesses, deverá comunicar o fato imediatamente ao Diretor de *Compliance*, seu superior ou ao administrador.

Na hipótese descrita acima, adicionalmente, o colaborador deverá:

(i) Interromper qualquer ação sob sua responsabilidade que possa resultar ou agravar eventual Conflito de Interesses, seja ele aparente ou concreto; e

(ii) Não utilizar sua influência pessoal para incentivar a Companhia a darandamento em processos internos que possam estar influenciados porConflito de Interesses, seja ele aparente ou concreto.

8.3. Declaração de Conflito de Interesses

A SIGA reconhece que se encontra em situação de potencial conflito de interesse ao atuar junto a player ou grupo econômico, que mesmo não sendo parte relacionada, em que seus colaboradores tenham, de alguma forma, atuado nos últimos 5 (cinco) anos.

Qualquer colaborador ou prestador de serviços deverá declarar, por escrito,eventuais situações passíveis de gerar conflito de interesses.

A declaração será devida, cumulativamente:

I. Na data da admissão;

II. Na ocorrência de fato superveniente que altere o anteriormente declarado

III. A cada período de 12 meses.

Eventualmente, se uma transação onde exista conflito de interesse oupotencial para conflito de interesse for autorizada pelo Comitê de *Compliance*, a SIGA deverá divulgá-la como informação relevante nos documentos aplicáveise em seu website, detalhando o tipo de relação e de transação realizada, fornecendo detalhes suficientes para identificação das Partes Relacionadas e de quaisquer condições essenciais, ou não estritamente comutativas, inerentes às transações em questão.

9. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

9.1. Objetivo e a Quem se Aplica

A Política de Confidencialidade e Segurança da Informação objetiva concretizar princípios e diretrizes de proteção das informações.

Aplica-se a todos os colaboradores, prestadores de serviços, à Diretoria e sócios.

9.2. Definições

A SIGA segrega e classifica as informações, tratadas, armazenadas ou transferidas, de acordo com sua natureza. Elas podem ser:

(i) Públicas: Informação de acesso livre, disponibilizada em sites ou meios de comunicação.

(ii) Internas: À Procedimentos operacionais, que podem ser acessados de forma irrestrita pelos colaboradores. Quaisquer solicitações de transmissão destas informações a terceiros dependerão de anuência prévia do titular e de aval fundamentado da Diretoria de Risco, *Compliance* e PLDFT.

(iii) Confidenciais: São todas aquelas informações sobre clientes, ativos, composição de carteira, estudos e análises, aquelas que identifiquem dados pessoais ou patrimoniais de clientes, sejam objetos de acordo deconfidencialidade celebrado com terceiros, identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva. Estes dados somente serão compartilhados com os colaboradores que necessitem, de maneira irremediável, das informações para exercerem as suas funções (princípiodo *need to know*). Quaisquer solicitações de transmissão destas informações a terceiros dependerão de anuência prévia do titular e de aval fundamentado da Diretoria de Risco, *Compliance* e PLDFT.

(iv) Sigilosas: Informações de conhecimento único da Diretoria, relativas a, geralmente, planos de negócio ou posicionamento.

Todos os tratamentos, armazenamentos ou transferência de dados irão obedecer estritamente às determinações da Lei nº 13.709/2018, Lei Geral da Proteção de Dados (LGPD). Além disso, cada classificação de informações terá diretórios segregados, cujo acesso será concedido apenas a profissionais autorizados, por escrito, além de toda uma estrutura cibernética de proteção dedados, inclusive em respeito à LGPD.

Serão oferecidos, periodicamente, treinamentos e cursos aos colaboradoressobre as questões de proteção de dados, conforme descrito no capítulo 15 do Manual de *Compliance*, Regras, Procedimentos e Controles Internos.

9.3. Diretrizes

As diretrizes a seguir dispostas são vinculantes e obrigatórias a todos os colaboradores.

(i) As informações confidenciais devem ser tratadas de forma ética e sigilosae de acordo com os procedimentos, códigos, manuais e políticas vigentes, evitando-se mau uso e exposição indevida.

(ii) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

(iii) A concessão de acessos às informações confidenciais deve obedecer aocritério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

(iv) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

(v) Segregação de instalações, equipamentos e informações comuns, quando aplicável.

(vi) A senha é utilizada como assinatura eletrônica e deve ser mantidasecreta, sendo proibido seu compartilhamento.

(vii) Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao Diretor de Risco, *Compliance* e PLDFT. No caso de impedimento deste, deverá ser reportada ao Diretor de Gestão e Distribuição ou a outra pessoa a ser designada em assembleia de sócios devidamente convocada.

9.4. Controles e Barreiras

Com o objetivo de se assegurar o cumprimento das políticas de confidencialidade e segurança da informação, serão adotados, entre outros, os seguintes pontos preventivos:

(i) Identificação e Classificação da Informação: O colaborador que receber ou tratar uma informação deverá classificá-la em uma dentre as quatro definições expostas neste documento, de acordo com as necessidades do negócios e os possíveis impactos no caso de utilização indevida.

(ii) Gestão de Informações Confidenciais: As informações confidenciais deverão ser identificadas desta maneira em qualquer meio de comunicação (e-mails, memorandos, documentos, arquivos físicos ou eletrônicos). As informações confidenciais serão salvas em HD externo segregado ou dispositivo de armazenamento em nuvem, com limitação esenhas de acesso. Os e-mails serão protegidos. Eventual documento disponibilizado a terceiros deve

indicar a sua qualificação e editada com marca d´água ou carimbo especial.

(iii) Salvaguarda da Informação: Toda informação terá o ciclo de vida definidopelas seguintes etapas: geração, manuseio, armazenamento e descarte.O tempo de cada uma das etapas deverá ser de conhecimento docolaborador, que terá a liberdade de consultar a Diretoria de Risco, C*ompliance* e PLDFT em caso de eventuais dúvidas. Por fim, o descartedeverá ser feito por técnico de Tecnologia da Informação (TI), que não poderá ter acesso às informações e, portanto, será acompanhado duranteo processo. Em caso de documentos em papel, estes deverão ser incinerados ou fragmentados.

(iv) Controle de Acessos: Os acessos físicos e digitais dos documentos serãorastreados, a fim de garantir a possibilidade de auditoria, que poderá identificar individualmente cada colaborador que acessou as informações.

(v) Quaisquer riscos e incidentes deverão ser, imediatamente, reportados aoDiretor de Risco, *Compliance* e PLDFT. O plano de contingência e de continuidade dos sistemas e serviços implantados deverá ser testado semestralmente, com o objetivo de se minorar quaisquer riscos de perda de informações, confidencialidade, integridade e disponibilidade da documentação, assim como o *backup*.

(vi) Teste de Controle: O responsável pela TI deverá, periodicamente, efetuar testes que assegurarão que os recursos estarão: a.) adequados ao porte e às áreas de atuação; b.) adequados ao nível de confidencialidade; c.) segregados físicos e logicamente; d.) os recursos computacionais estarão protegidos e assegurados de que a sua manutenção permita a realizaçãode auditorias e inspeções.

Todos os quais estas normas são aplicáveis, deverão assinar formalmente,termo obrigando-se a atuar de acordo com estas políticas, sob pena de sanções.

A SIGA, ainda, disponibilizará treinamentos obrigatórios a todos que participem ou tenham acesso às informações confidenciais.

Por fim, em respeito aos artigos 22 e 23 da RCVM nº 19/2021, os documentos e informações exigidos pela CVM serão mantidos pelo prazo mínimo de cinco anos, salvo por determinação expressa em sentido contrário pelo órgão, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, cálculos que fundamentaram a cobrança de taxa de performance de seus clientes classificados como investidores profissionais, quando for o caso, relatórios e pareceres relacionados com o exercício de suas atividades e os estudos e análises que fundamentaram as orientações, recomendações ou aconselhamentos.

Todos os e-mails e arquivos serão armazenados em um *file server* com altos padrões de segurança e ética, possibilitando controle de acesso e rastreamento de uso dos arquivos por usuário, o que garante a preservação de informações confidenciais e a restrição de acesso aos arquivos sensíveis.

O file server, que fica hospedado internamente, também possui, como medida de segurança adicional, um sistema de cópia incremental para um repositório na nuvem com periodicidade semanal.

Toda a base de dados conta com a realização de *backups* simultâneos queficam armazenados na nuvem e que permitem, em caso de falhas operacionais,recuperação de dados e arquivos.

O *file server* é acessado pelos colaboradores mediante *login* com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional.

Os diferentes níveis de permissão viabilizam melhor controle de acesso e dereprodução dos dados e arquivos pelos profissionais. De forma não taxativa, asseguintes condutas devem ser observadas:

(i) Os colaboradores devem evitar circular em ambientes externos à SIGA com cópias (físicas ou digitais) de arquivos contendo informações confidenciais, devendo essas cópias ser mantidas com senha de acesso.

(ii) O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico.

(iii) As informações que possibilitem a identificação de um cliente da SIGA devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da entidade ou do próprio cliente.

(iv) Os colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da SIGA, como, por exemplo, vírusde computador, fraudes, entre outros.

(v) Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

9.5. Segurança Cibernética

A SIGA identificará e avaliará os principais riscos cibernéticos aos quais estáexposta. Levará, como parâmetro inicial, como ataques mais prováveis:

(i) *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);

(ii) Engenharia Social;

(iii) *Pharming*;

(iv) *Phishing scam*;

(v) *Vishing*;

(vi) *Smishing*;

(vii) Acesso pessoal;

(viii) Ataques de DDoS e botnets;

(ix) Invasões (*advanced persistent threats*).

Para avaliar as ameaças e vulnerabilidades, serão realizadas varreduras internas/externas de cada ativo de rede, em busca de possíveis problemas de segurança, e eventual correção.

A principal regra de proteção consiste na segregação de acessos a sistemase dados, conforme já detalhado nesta Política.

A SIGA adotará, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância doativo acesso.

A entidade trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

A senha e *login* para acesso aos dados contidos em todos os computadores,bem como a conta de e-mail acessada via *webmail* devem ser conhecidas pelo respectivo usuário destes dispositivos. Estas senhas são pessoais e intransferíveis, não podendo ser divulgadas para quaisquer terceiros.

O acesso à informações confidenciais é limitado a determinados colaboradores cuja necessidade é justificada.

Arquivos eletrônicos são protegidos com senhas de acesso ou outros controles estabelecidos dentro dos sistemas computacionais, o que garante o acesso somente à pessoas autorizadas.

Todo conteúdo que está na rede pode ser acessado pela área Diretoria de Risco, *Compliance* e PLDFT e pelo Comitê de *Compliance* caso haja necessidade.

Arquivos pessoais salvos em cada computador poderão ser acessados caso o Comitê de *Compliance* julgue necessário.

A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial. Para segurança dosperfis de acesso dos colaboradores, as senhas de acesso são parametrizadas conforme regras estabelecidas globalmente, bem como criptografadas. Desta forma, o colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

A SIGA exige que os colaboradores efetuem a validação bimestral de suas senhas por meio da adoção da seguinte política de senhas:

(i) A senha expirará a cada 60 dias, podendo ser revalidada sem alteração somente pelo próprio usuário.
(ii) Após, no máximo, oito meses ou quatro revalidações (o que acontecer primeiro) o colaborador deverá alterar sua senha de acesso.
(iii) O tamanho mínimo da senha é de oito caracteres.
(iv) Após quatro tentativas de acesso com senhas erradas, a conta docolaborador será bloqueada.

A política de senha disposta neste documento poderá ser modificada a qualquer momento, em

decorrência de avanços tecnológicos ou decisão interna da Diretoria, visando sempre o aprimoramento dos procedimentos, sistemas e da segurança das informações.

O acesso remoto a arquivos e sistemas internos ou na nuvem terão controles adequados, de acordo com o técnico de TI.

Ainda, a SIGA conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* e *firewalls* locais em cada um desses equipamentos, bem como, *firewall* interno a rede e *firewall* UTM de borda, o qual contempla todos os serviços de ips/ids, *antispyware*, antivírus de *gateway*, filtro de aplicações e filtro de conteúdo.

A SIGA deverá, adicionalmente, proibir o acesso a determinados *websites* ea execução de *softwares* e/ou aplicações não autorizadas. A utilização dos ativos da entidade, incluindo computadores, telefones, internet, programas de mensagem instantânea, e-mail e demais aparelhos se destina a fins profissionais.

O uso indiscriminado dos mesmos para fins pessoais deve ser evitado, enunca deve ser prioridade em relação a qualquer utilização profissional. A SIGApoderá gravar ligações telefônicas e históricos de navegação dos colaboradores. A visualização de sites ou páginas que contenham conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibida,estando o colaborador que o fizer sujeito aos processos e sanções determinados no Código de Ética e Conduta da SIGA.

Programas instalados nos computadores, principalmente via Internet (*downloads*), sejam de utilização profissional ou para fins pessoais devem obter autorização prévia do Diretor de Risco, *Compliance* e PLDFT.

Não é permitida a instalação de nenhum *software* ilegal ou que possuam direitos autorais protegidos. Somente arquivos sob licenciamento "GPL" (http://www.gnu.org/licenses/gpl.html) ou como consentimento expresso do respectivo autor poderão ser gravados, mediante autorização prévia do responsável pela TI.

O responsável pela TI, em conjunto com o Diretor de Risco, *Compliance* e PLDFT, são os principais responsáveis para tratar e responder questões de segurança cibernética, bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Os deveres e responsabilidades dos responsáveis podem ser exemplificados pelo seguinte rol não taxativo:

(i) Testar a eficácia dos controles utilizados e informar à Diretoria os riscos residuais.

(ii) Acordar com a Diretoria o nível de serviço que será prestado por terceiroscontratados e os procedimentos de resposta aos incidentes.

(iii) Configurar os equipamentos e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem

como definir e assegurar asegregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os *logs*e trilhas de auditoria das suas próprias ações.

(iv) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem,processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

(v) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da SIGA em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.

(vi) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueiode acesso de usuários por motivo de desligamento da SIGA, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da entidade.

(vii) Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da SIGA, mediante treinamentos.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar o Diretor de Risco, *Compliance* e PLDFT, que poderá convocar reunião do Comitê de *Compliance*. No caso de impedimento deste, o Comitê será instaurado pelo Diretor de Gestão e Distribuição ou outra pessoa aser designada em assembleia de sócios devidamente convocada.

Ainda, uma vez que cada colaborador possui um login e senha personalíssimos, o acesso a qualquer documento e pasta ficará registrado no sistema, com o ID do usuário e data e horário de acesso, para eventualresponsabilização em caso de vazamento.

9.6. Testes de Segurança

A SIGA realizará testes de segurança para os sistemas de informações anualmente, visando reduzir riscos de perda de confidencialidade, integridade edisponibilidade dos ativos de informação.

Os testes de segurança englobarão, mas não se limitarão, a análises de vulnerabilidade física e eletrônica, revisão e teste de códigos, transações sintéticas, testes de intrusão e análises dos registros eletrônicos.

Ainda, o treinamento sobre segurança de informação fará parte do treinamento inicial e contínuo da entidade, conforme previsto na Política de Treinamento descrita neste documento, que deverá assegurar que todos os colaboradores tenham conhecimento dos procedimentos e das obrigações aquiprevistos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretaçãodas normas e procedimentos.

10. DISPOSIÇÕES GERAIS E FINAIS

O desrespeito a quaisquer das regras da SIGA resultarão em Processo Administrativo Interno, podendo imputar sanções internas, de acordo com deliberações da Diretoria, incluindo desligamento.

Eventuais medidas legais poderão ser tomadas pela entidade em face do infrator.

Em caso de dúvidas de interpretação ou eventuais antinomias entre as regras aqui dispostas e outras vigentes na entidade, deverá haver consulta imediata ao Diretor de Risco, Compliance e PLDFT.

Quaisquer alterações legais ou normativas expedidas pelos órgãos regulamentadores e competentes serão aplicadas imediatamente a esta política, e todos os colaboradores serão imediatamente alertados de eventuais mudanças.

Eventuais dúvidas deverão ser encaminhadas à Diretoria de Risco, Compliance e PLDFT, por intermédio do e-mail matheus.cardoso@sigafinance.com.br ou pelo telefone (41) 3044-7464.

ANEXO I

TERMO DE ADESÃO AO CÓDIGO DE SEGREGAÇÃO DE ATIVIDADES E CONFIDENCIALIDADE

Eu, [NOME], [NACIONALIDADE], [ESTADO CIVIL], portador da cédula deidentidade RG nº [NÚMERO], inscrito no CPF/MF sob nº [NÚMERO], residentee domiciliado na [RUA, NÚMERO, CEP, CIDADE, ESTADO], exercendo a função de [FUNÇÃO], junto à SIGA GESTORA DE RECURSOS LTDA., declaro para osdevidos fins que:

(i) Tenho total conhecimento da existência da Política de Segregação de Atividades e Confidencialidade da SIGA, o qual recebi, li e entendi, sendoque me comprometo a observar integralmente seus termos e condições.

(ii) Sei, a partir desta data, que a não observância dos termos da Política deSegregação de Atividades e Confidencialidade da SIGA poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa.

(iii) As regras estabelecidas na presente Política de Segregação de Atividades e Confidencialidade não invalidam nenhuma disposição relativa a qualquer norma interna estabelecida, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução de minhas atividades profissionais.

(iv) Tenho ciência de que o descumprimento de qualquer regra estabelecida na Política de Segregação de Atividades e Confidencialidade da SIGA, poderá me sujeitar a penalidades e responsabilização na esfera civil e criminal. Adicionalmente, sei que, caso haja o vazamento de informação confidencial advindo da utilização de minha senha pessoal, poderei ser responsabilizado tanto civil, quanto penalmente.

(v) Estou ciente que o disposto nesta Política de Segregação de Atividades e Confidencialidade é aderido, por meio deste Termo de Adesão, em caráter irrevogável e irretratável, por prazo indeterminado, válido indefinidamente mesmo após o término de meu vínculo com a SIGA, não podendo ser rescindido sem expressa e inequívoca concordância, por escrito, das partes relacionadas.

(vi) Li e entendi a legislação e regulamentação aplicável a negociação de valores mobiliários, em particular, conforme disposto na Resolução CVM 44/2021 de 23 de agosto de 2021, conforme alterada, acerca de divulgação e o uso de informações sobre ato ou fato relevante na negociação de valores mobiliários.

Curitiba/PR,___de_____de_____.

_____

ADERENTE [NOME]
CPF/MF