POLÍTICA DE SEGUERANÇA E SIGILO DAS INFORMAÇÕES

DA

LEEN CAPITAL LTDA.

30 DE SETEMBRO DE 2025

Versão	Vigência	Alterado/Elaborado	Situação
2.1	Setembro/2025	Risco e Compliance	Versão Revisada

ÍNDICE GERAL

1. INTRODUÇÃO

A Leen Capital Ltda. (“Leen Capital”) é uma sociedade limitada autorizada pela Comissão de Valores Mobiliários (“CVM”) a atuar na prestação de serviços de administração de carteiras de valores mobiliários, oferecendo serviços de gestão de recursos de terceiros.

Com base nisso, a Leen Capital está sujeita aos regramentos que regem o funcionamento do mercado de capitais brasileira, notadamente às normas editadas pela CVM, que atualmente regulam o exercício da atividade de administração de carteiras por meio da Resolução da Comissão de Valores Mobiliários nº 21, de 25 de fevereiro de 2021 (“Resolução CVM 21”).

2. OBJETIVO

A Política de Segurança e Sigilo da Informação (“Política”) tem por objetivo estabelecer regras e procedimentos a serem observados pelos sócios, diretores, administradores, e funcionários (“Colaboradores”) da Sociedade, quanto às regras de acesso às informações confidenciais, reservadas ou privilegiadas da Sociedade e de seus clientes.

O conceito se aplica a todos os aspectos de proteção de informações e dados, no âmbito corporativo ou pessoal, incluindo não apenas a segurança da informação, mas também o acesso e uso aos sistemas.

3. RESPONSABILIDADES

A responsabilidade por verificar e fiscalizar o cumprimento desta Política por parte dos Colaboradores, bem como a de fornecer a estes o treinamento necessário para o seu cumprimento, é do Diretor de *Compliance*, Risco e PLD.

Também será de responsabilidade do Diretor de *Compliance*, Risco e PLD a definição dos métodos para avaliação e monitoramento do conteúdo previsto nesta Política, bem como o atendimento necessário aos órgãos reguladores e autorreguladores.

Todos os Colaboradores e Prestadores de Serviços deverão assinar Termo de Confidencialidade para terem acesso às informações confidenciais a respeito da Sociedade, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante em Contrato de Prestação de Serviços assinado entre as partes.

Ademais, é responsabilidade de todo e cada Colaborador zelar pelo cumprimento desta Política, não obstante as responsabilidades de fiscalização e regulação do Diretor de

Compliance, Risco e PLD.

4. INFORMAÇÕES CONFIDENCIAIS

São consideradas informações confidenciais:

(i) qualquer informação, escrita ou verbal, 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 comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Sociedade, 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 pertinentes às atividades da Sociedade; e

(ii) informações acessadas pelos Colaboradores em função do desempenho de suas atividades na Sociedade, bem como informações estratégicas ou mercadológicas de qualquer natureza, obtidas junto aos sócios, administradores ou funcionários da Sociedade, ou, ainda, junto aos seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Não são consideradas informações confidenciais as informações que:

(i) à época ou após o seu fornecimento ou obtenção pelos Colaboradores, sejam ou se tornem de domínio público por publicação ou qualquer outra forma de divulgação, sem que tal divulgação tenha sido feita em ofensa ao disposto nesta Política ou à legislação e regulamentação aplicável;

(ii) ao tempo da divulgação, sejam conhecidas pelo destinatário, sem violação da legislação e regulamentação aplicável ou da presente Política;

(iii) em virtude de lei, decisão judicial ou administrativa, devam ser divulgadas a qualquer pessoa; ou

(iv) cuja divulgação tenha sido aprovada pelo Diretor de *Compliance*, Risco e PLD.

No intuito de resguardar a privacidade das informações confidenciais dos clientes da Sociedade, prevalecerá, em regra e em qualquer situação de dúvida, o caráter sigiloso dos dados e informações relativas a clientes que não sejam notoriamente de conhecimento público.

A divulgação de informações confidenciais a autoridades governamentais ou em

virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente comunicada ao Diretor de *Compliance*, Risco e PLD, para que este decida sobre a forma mais adequada para proceder tal revelação.

Na hipótese de rescisão do contrato individual de trabalho ou desligamento de Colaboradores, deverão ser restituídos à Sociedade todos documentos físicos e eletrônicos sob seu poder que contenham informações confidenciais e deverá ser imediatamente cancelado o acesso do Colaborador retirante aos diretórios de informações públicas e aos diretórios de acesso restrito da rede da instituição.

5. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

5.1. Conceito Características

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a Sociedade, independentemente de estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

São características básicas da segurança da informação os atributos de:

- **Confidencialidade:** restringe o acesso a informação apenas às competências legítimas;
- **Integridade:** garante que a informação manipulada mantenha as características originais, garantindo o ciclo de vida da informação;
- **Disponibilidade:** garante que a informação esteja sempre disponível para o uso legítimo; e
- **Irretratabilidade:** garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

A utilização mal intencionada das informações disponíveis, com o objetivo de furtar, destruir ou modificar tal informação será considerada descumprimento de norma de conduta da Sociedade e resultarão em ação disciplinar.

5.2. Informações Proprietárias

Os Colaboradores que têm acesso aos sistemas de informação da Sociedade são responsáveis por tomar as medidas necessárias para impedir o acesso não autorizado a estes sistemas.

Informações compreendem todo e qualquer documento originado pela ou para a Sociedade, tais como: planos de negócios, propostas comerciais, contratos, contatos, dados de clientes, rotinas internas, softwares, códigos, bancos de dados, arquivos e relatórios em geral.

A Sociedade detém ainda, os direitos de propriedade das informações acima citadas que forem produzidas por seus Colaboradores ou que estejam relacionadas à realização das atividades dos mesmos para a instituição.

5.3. Utilização dos Meios de Comunicação

As trocas de informações através de sistemas de comunicação estão sujeitas à revisão, monitoramento e gravação a qualquer época sem aviso ou permissão. Uso ou acesso não autorizado pode estar sujeito à ação disciplinar, conforme sua relevância.

Os sistemas de comunicação, como: telefonia, correio eletrônico, ou qualquer outro meio de comunicação via internet, devem ser utilizados de maneira consciente e primordialmente para fins profissionais.

5.4. Controle de Acesso

O acesso à rede e aos softwares possibilita a identificação dos usuários e serão concedidos conforme as atribuições de cada Colaborador. Ademais, cada Colaborador possui acesso exclusivo aos diretórios de suas áreas de competência e somente a Diretoria Executiva da Sociedade possui acesso a todos os diretórios da rede.

Todo software que for caracterizado como de acesso limitado terá senha de acesso e seu uso será exclusivo de seu operador, podendo haver ou não monitoramento, conforme definição do Diretor de *Compliance*, Risco e PLD.

5.5. Segurança dos Arquivos

Para proteção contra softwares maliciosos ou vírus, são instalados softwares de prevenção nos servidores de rede da Sociedade. Além do procedimento preventivo, o Departamento de TI verificará os discos rígidos de todos os computadores periodicamente.

Os arquivos relevantes terão seus backups realizados, através de espelhamento via hardware, efetuado internamente e externamente em dispositivo modular. Somente terão acesso a estes arquivos Colaboradores devidamente autorizados.

5.6. Segregação das Atividades

A Sociedade estabelece barreiras de informação para segregar internamente suas atividades, prevenindo assim o mau uso de informações privilegiadas e para evitar conflitos de interesse.

Apenas os Colaboradores responsáveis pelas decisões de investimento ou que negociam valores mobiliários para a instituição, tem acesso às informações confidenciais referentes ao Mercado de Capitais.

Os Colaboradores envolvidos nas demais áreas como, administrativo-financeira, jurídica, não tendo acesso às informações supracitadas, evitando conflitos de interesse.

A mesma política adotada pressupõe sigilo absoluto das informações ditas confidenciais, proibindo que qualquer Colaborador as revele, independentemente de como essas informações foram obtidas.

5.7. Uso de Informações Privilegiadas

Existem leis no Brasil que proíbem a negociação, recomendação ou outros tipos de transferência de títulos e valores mobiliários em detrimento de conhecimento privilegiado de informações materiais, que não sejam de domínio público, sobre o emissor desses títulos.

Por definição, uma informação é considerada material se a violação de sua confidencialidade tiver potencial para alterar decisões de investimento.

A informação privilegiada é toda a informação relevante sobre emissores de títulos e valores mobiliários que ainda não seja de domínio público ou que ainda não tenha sido veiculada à comunidade de investidores através de fato relevante.

Esta vedação é válida, ainda que a informação tenha sido obtida pelo exercício de sua função ou especialmente se a negociação violar uma obrigação ou tiver sido indevidamente apropriada.

As violações às exigências relacionadas ao uso ou transmissão de informações privilegiadas poderão impor ao violador, penalidades civis e criminais, multas, além de sanções administrativas por parte da Sociedade, na forma descrita no item 7 desta Política.

Dúvidas quanto às normas legais envolvendo podem ser encaminhadas ao Diretor de *Compliance*, Risco e PLD da Sociedade.

A mesma política adotada pressupõe sigilo absoluto das informações ditas confidenciais, proibindo que qualquer Colaborador as revele, independentemente de como essas informações foram obtidas.

5.8. Sigilo de Informações

Todos os Colaboradores, ou mesmo ex-colaboradores, devem proteger a confidencialidade de quaisquer informações que não devam ser de domínio público, informações estas que foram obtidas durante o exercício de suas funções e atividades como membro Colaborador da Sociedade.

Dentre essas, encontram-se informações que não devem ser de domínio público a respeito de operações, estratégias, resultados, ativos, dados e projeções, ou quaisquer outras informações relativas às atividades e negócios da Sociedade, seus Colaboradores, clientes, e fornecedores, conforme descrito no item 4 desta Política.

Da mesma forma, os membros da Sociedade devem evitar manter à vista em suas posições de trabalho, papéis e documentos confidenciais, e manter sigilo sobre senhas de computador, softwares, redes e sistemas.

É de responsabilidade dos Colaboradores garantirem que o acesso à área de trabalho seja feito somente por pessoal autorizado, sob fiscalização periódica do Diretor de *Compliance*, Risco e PLD.

Questões envolvendo assuntos relativos à Sociedade e seus negócios não devem ser tratados em locais públicos.

Caso a Sociedade venha a ser interpelada para a prestação de informações, em razão de procedimento fiscalizatório por parte dos órgãos de regulamentação, a Sociedade ou qualquer dos seus Colaboradores estarão então obrigados prestar os esclarecimentos e fornecer as informações necessárias, seguido de imediata e expressa comunicação aos clientes afetados caso não haja norma dispondo de forma diversa.

5.9. Testes Periódicos

Para garantir a integridade e a segurança dos dados da Sociedade, testes periódicos serão realizados em nossa estrutura, garantindo o correto funcionamento de todos os sistemas da empresa. Todos os testes são efetuados e supervisionado pela equipe de TI, sendo:

- Uma vez a cada trimestre, será efetuado um teste de restauração dos backups realizados do servidor da Sociedade. Esse teste consiste em realizar restaurações aleatórias de 10 arquivos, localizados em pastas diferentes, verificando a consistência e integridade dos backups.
- Bimestralmente, serão avaliados todos os computadores da empresa. Além da varredura contra vírus, serão realizadas a limpeza e desfragmentação dos discos.

6. TREINAMENTOS

6.1. Programa de Treinamento

Todos os Colaboradores da Sociedade, inclusive seus sócios e administradores, deverão obrigatoriamente participar dos programas de treinamento descritos neste

capítulo (“Programas de Treinamento”), como forma de atualização e conscientização das regras de conduta e procedimentos internos da instituição.

Os Programas de Treinamento serão conduzidos pelo Diretor de *Compliance*, Risco e PLD, responsável por supervisionar e fiscalizar os Colaboradores quanto ao cumprimento às normas regulamentares e ao previsto nesta Política.

Os Programas de Treinamento devem necessariamente abordar as regras e os procedimentos previstos nesta Política. Os programas de treinamento devem ser norteados pela clareza, acessibilidade e simplicidade na transmissão de informações. O conteúdo e datas dos programas de treinamento serão definidos pelo Diretor de *Compliance*, Risco e PLD, que também arquivará o Termo de Anuência.

Além dos Programas de Treinamento periódicos, todos os novos Colaboradores da Sociedade participarão de treinamento no momento de seu ingresso. Nessa mesma ocasião, os Colaboradores deverão assinar o Termo de Anuência, em conformidade com as orientações do Diretor de Compliance, Risco e PLD. Essa adesão e formalização serão renovadas anualmente.

7. PENALIDADES

Todos os signatários do Termo de Anuência obrigam-se a seguir rigorosamente as regras estabelecidas nesta Política, pautando suas atividades de acordo com as leis e demais documentos que regulam as práticas aplicáveis aos negócios da Sociedade, além de atender às instruções e diretrizes emitidas pelo Comitê Executivo da instituição.

O descumprimento total ou parcial das regras contidas nesta Política e na legislação vigente constitui violação dos padrões éticos, técnicos e operacionais, conforme o caso, que regem o funcionamento da Sociedade.

Assim, qualquer descumprimento acarretará ação disciplinar de responsabilidade do Diretor de *Compliance*, Risco e PLD da Sociedade, que pode incluir, entre outras, as penalidades de dispensa do vínculo empregatício (demissão) por justa causa, destituição de cargo ou ainda, exclusão do quadro societário da Sociedade, tudo isso sem prejuízo de o infrator sujeitar se às penalidades estabelecidas na legislação brasileira.

Além do disposto neste documento, os signatários do Termo de Anuência, quando for o caso, devem se comprometer na observância das normas de conduta específicas aplicáveis a cada setor e descritas pelas instruções emitidas pela CVM.

Além da obrigatoriedade de cumprimento das instruções da presente Política, dependendo da função ou área de responsabilidade, há ainda a necessidade de cumprimento de políticas adicionais e procedimentos suplementares publicados a critério

da instituição, conforme a conveniência ou necessidade.

Os Colaboradores reconhecem o direito de a Sociedade exercer direito de regresso caso venha a ser responsabilizada, sofra prejuízo ou venha arcar com ônus de qualquer espécie em decorrência de atos ilícitos ou infrações cometidas por seus Colaboradores no exercício de suas funções.