# POLÍTICA DE SEGURANÇA CIBERNÉTICA

**DA**

**LEEN CAPITAL LTDA.**

**20 DE JUNHO DE 2023**

| Versão | Vigência | Alterado/Elaborado | Situação |
|---|---|---|---|
| 1.0 | Junho/2023 | Risco e Compliance | Versão Revisada |

## ÍNDICE GERAL

## 1. INTRODUÇÃO

A Leen Capital Ltda. ("Leen Capital" ou "Gestora") 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

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Leen Capital Ltda. ("Leen Capital" ou "Gestora"), estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM 21 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, assim como à Lei 13.709, de agosto de 2018 ("Lei Geral de Proteção de Dados)", a Leen Capital procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

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

Qualquer informação sobre a Leen Capital, 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, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e *Compliance*, nos termos estabelecidos no Código de Ética da Gestora.

## 3. ABRANGÊNCIA

Os procedimentos aqui estabelecidos se aplicam à Leen Capital e aos seus Colaboradores, em atendimento aos requisitos do sistema de gestão de *compliance*.

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações

Confidenciais, Dados Pessoais e dos ativos disponibilizados pela Leen Capital ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Gestora, sendo de responsabilidade individual e coletiva o seu cumprimento.

## 4. PREMISSAS

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, que são de extremo valor para a Leen Capital, à luz do princípio fundamental de confiança que a instituição trabalha para manter junto aos seus cotistas, a Leen Capital utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA. Referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a Leen Capital abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de *Compliance* da Leen Capital, sob a direção do Diretor de Risco e *Compliance* da Gestora.

## 5. PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

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

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

i. *Malware – softwares* desenvolvidas para corromper computadores e redes:
    a. Vírus: *software* que causa danos a máquina, rede, *softwares* e banco de dados;

b. Cavalo de Troia: aparecer dentro de outro *software* e cria uma porta para a invasão do computador;
c. *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
d. *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii. Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
a. *Pharming*: direcionar o usuário para um site fraudulento, sem o seu conhecimento;
b. *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações condifenciais;
c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
e. Acesso Pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii. Ataques de DDoS (*Distributed Denial of Services*) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

iv. Invasões (*Advanced Persistent Threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Leen Capital pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar a perda e/ou adulteração de dados e Informações Confidenciais.

### 5.1. Ação de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Leen Capital, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Leen Capital, em caso de incidente de segurança. Deste modo, a Leen Capital segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte

destas informações. Assim, classificam-se as informações digitais da instituição em 4 (quatro) classes diferentes, quais sejam:

- **Públicas**

Devem ser classificadas como PÚBLICAS, as informações que podem ser divulgadas publicamente e não necessitam de atenção especial quanto à preservação de sigilo. São passíveis de classificação como PÚBLICAS, dados ou informações que podem ser divulgadas para o mercado ou para a comunidade em geral.

Exemplos: Informações divulgadas a investidores e ao mercado, telefones de atendimento ao público, sites institucionais da empresa na Internet e em mídias sociais etc.

- **Internas**

Devem ser classificadas como INTERNAS as informações que devem ser divulgadas a todos os colaboradores da Leen Capital e/ou para terceiros formalmente comprometidos com a segurança das informações. A informação somente deve ser classificada como INTERNA se for necessário que todos os colaboradores da Leen Capital tenham conhecimento de tal informação.

Exemplos: Listas de ramais internos, campanhas e comunicações internas, divulgações de metas da Gestora, normas e procedimentos de aplicação geral na Leen Capital, etc.

- **Restritas**

Devem ser classificadas como RESTRITAS as informações que devem ser divulgadas apenas para algumas pessoas, grupos de trabalho ou áreas da Leen Capital e que não devem ser divulgadas abertamente a todos os colaboradores da Leen Capital. A perda destas informações pode gerar impactos em processos, produtos ou serviços específicos da Gestora.

Exemplos: Informações de projetos internos, dados ou informações referentes a produtos, processos e serviços, procedimentos operacionais, indicadores de desempenho das áreas, relatórios de auditoria, relatórios específicos das áreas etc.

- **Confidenciais**

Informações que requerem forma de proteção mais robusta contra acesso e compartilhamento não autorizado. Devem ser classificadas com Confidencial todas as informações relativas a:

- Informações privadas das pessoas;
- Informações estratégicas de clientes e fornecedores;
- Informações estratégicas da Leen Capital;
- *Know How* da Leen Capita; e
- Informações que prejudicam a reputação e imagem da Leen Capital.

São informações cujo perda, roubo, acesso indevido ou não autorizado podem trazer sérios problemas para a reputação, imagem, ações judiciais, gerar passivo trabalhista e prejuízos financeiros diretos com eventual perda de competividade para a Leen Capital.

Exemplos: Atas de reuniões estratégicas da Gestora, contratos com cotistas e fornecedores, informações sobre os projetos com os cotistas, demonstrações financeiras da empresa, informações pessoais e privadas dos colaboradores, informações sobre o método da Leen Capital, *know how* relativo a produtos e serviços, *feedback* dos colaboradores, etc.

A partir da definição acima, a Leen Capital se empenhará para manter controles, conforme o nível de criatividade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Públicas, Internas, Restritas e Confidenciais.

## 6. PROPRIEDADE DOS RECUROS DE TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Leen Capital. Não é permitida a utilização de notebooks, tablets ou outros hardwares próprios para operações no âmbito da Leen Capital, salvo expressa permissão do Diretor de Risco e *Compliance.*

### 6.1. Disponibilização e Uso

Todos os computadores disponibilizados para os Colaboradores da Leen Capital têm por objetivo o desempenho das atividades na Leen Capital. Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela equipe de TI, mediante solicitação de Colaboradores da Gestora, que pressupõe a aprovação do Diretor de Risco e *Compliance.*

A disponibilização e uso dos computadores da Leen Capital respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de Risco e *Compliance* autorizará a criação de novo usuário e a disponibilização técnica de recursos;

- Todos os equipamentos, *softwares* e permissões acessos devem ser testados, homologados e autorizados pela equipe de TI, mediante supervisão e aprovação do Diretor de Risco e *Compliance*, quando julgar necessário; e
- O Diretor de Risco e *Compliance* autorizará, a retirada ou substituição do computador disponibilizado para o usuário, quando aplicável.

### *6.2. Softwares*

A implementação e configuração de *softwares* da Leen Capital respeitam as seguintes regras:

- Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Leen Capital; e
- A utilização de equipamentos pessoais por terceiros nas instalações da Leen Capital e a conexão destes na rede interna à Internet requer autorização e autenticação de acesso a rede apartada da rede da Gestora. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

### 6.3. Responsabilidade do Usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento. O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Leen Capital.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da Leen Capital em qualquer meio (CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecidas;

- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Leen Capital.

## 7. REGRAS E RESPONSABILIDADES DO USO DA INTERNET

O Colaborador é responsável por todo acesso realizado com a sua autenticação. Quando o usuário se comunicar através de recursos de tecnologia da Leen Capital, este deve sempre resguardar a imagem da Leen Capital, evitando entrar em sites de fontes não seguras, ou de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de Risco e *Compliance*.

O usuário não deve acessar endereços de internet (*sites*) que:

- Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física; e
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

É proibido o uso de serviços de mensagem instantânea, através dos computadores da Leen Capital, exceto em eventuais situações de uso profissional, salvo autorização do Diretor de Risco e *Compliance*.

## 8. USO DE CORREIO ELETRÔNICO PROFISSIONAL

A Leen Capital disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuário@leencapital.com.br).

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Leen Capital. O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Leen Capital.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Risco e *Compliance*, se necessário.

### 8.1. Endereço Eletrônico de Programas ou Comunicação Corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da Área de *Compliance* responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Leen Capital, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da Leen Capital.

### 8.2. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Leen Capital mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet. O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Leen Capital.

### 8.3. Responsabilidade e Forma de Uso do Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na Leen Capital.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Leen Capital, a sugestão deve ser encaminhada para o responsável pela área, que definirá a sua publicação ou não em conjunto com a Área de Risco e *Compliance*;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de

nascimento ou deficiência física;

- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Leen Capital; e
- Sejam incoerentes com o Código de Ética da Leen Capital.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Leen Capital é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Leen Capital.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado. O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculdo/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos; e
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

### 8.4. Cópias de Segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria, a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos da Leen Capital, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Risco e *Compliance*.

### 8.5. Armazenamento em Nuvem (*Cloud*)

A Leen Capital poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud). De forma a possuir um ambiente seguro de

nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

## 9. MONITORAMENTO E TESTES PERIÓDICOS

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área responsável, sob supervisão do Diretor de Risco e *Compliance*. O referido monitoramento acontecerá de forma no mínimo anual.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Leen Capital esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da Leen Capital.

## 10. PLANO DE RESPOSTA

Caso seja identificado um potencial incidente relacionado à segurança cibernética, o Diretor de Risco e *Compliance* deverá ser imediatamente comunicado.

Num primeiro momento, o Diretor de Risco e *Compliance* se reunirá com os demais diretores da Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, serão observados os procedimentos previstos no plano de continuidade do negócio da Leen Capital.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

## 11. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem

tal providência.

O objetivo principal do processo de revisão dessa Política é manter sempre atualiza a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.