Política de Segurança da Informação e Segurança Cibernética

KAETÉ INVESTIMENTOS LTDA.

Responsável:	Diretor de Compliance e Controles Internos
Data da atualização:	03 de julho de 2025
Versão	05

Sumário

Introdução

De forma geral, a informação pode ser considerada o ativo de maior valor gerado diariamente pela Kaeté Investimentos Ltda. (“Kaeté Investimentos” e/ou “Gestora”). Neste sentido, este documento tem como objetivo central apresentar e disseminar entre todos os sócios, dirigentes, empregados, funcionários, trainees e estagiários da Kaeté Investimentos (em conjunto, ‘’Colaboradores’’) as políticas e os procedimentos definidos pela Diretoria de Compliance e Controles Internos para garantir a integridade das informações produzidas e gerenciadas dentro do ambiente de trabalho.

Este roteiro da Kaeté Investimentos formaliza e esclarece as regras, os procedimentos e controles internos para fins de política de Segurança da Informação e Segurança Cibernética (“Política”).

1. Segurança da Informação e Segurança Cibernética

Esta Política leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora. A coordenação direta das atividades relacionadas a esta Política ficará a cargo do Diretor de Compliance, que será responsável, inclusive, por sua revisão, realização de testes e treinamento dos Colaboradores da Gestora, conforme aqui descrito.

Os seguintes princípios básicos norteiam esta Política:

- Confidencialidade e controle de acesso;
- Treinamento e conscientização sobre segurança da informação para todos os Colaboradores; e
- Testes periódicos dos sistemas de informação.

1.1 Confidencialidade e Controle de Acesso

A responsabilidade por garantir a total confidencialidade e integridade das informações diariamente produzidas pela Kaeté Investimentos cabe a cada um de seus Colaboradores, sendo essencial que todo funcionário tenha plena consciência acerca de sua importância no processo de garantia do cumprimento dos procedimentos definidos por meio desta política.

O acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do Colaborador. O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gestora dispõe de controles internos para que o acesso seja liberado mediante aprovação.

1.2 Treinamento e conscientização sobre segurança da informação para todos os Colaboradores

A Gestora oferece treinamentos periódicos aos quais os Colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, cyber segurança, engenharia social, phishing, entre outras potenciais ameaças à integridade dos sistemas de informação.

1.3 Testes periódicos dos sistemas de informação

A Gestora dispõe de tecnologias de defesa contra possíveis ataques aos seus sistemas de informação, tais como o uso de antivírus e firewall, e realiza testes periódicos no sistema disponível na rede mundial de computadores.

2. Identificação de Riscos (Risk Assessment)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio e Compliance da Gestora; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

- Malware: softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware, e Ransomware);

- Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas e dados pessoais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
- Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

3. Ações de Prevenção e Proteção

No tocante à segurança da informação, seguindo o princípio da confidencialidade e do controle de acesso mencionados acima, o acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do Colaborador, aplicando-se referido princípio, inclusive no que se refere às informações confidenciais, reservadas ou privilegiadas. O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gestora dispõe de controles internos para que o acesso seja liberado mediante aprovação.

Toda informação gerada internamente pela Kaeté Investimentos e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência.

Todos os Colaboradores, incluindo prestadores de serviços, quando necessário, terão acesso aos meios eletrônicos de comunicação fornecidos pela Kaeté Investimentos, incluindo, mas não se limitando, hardwares, softwares e aparelhos móveis, os quais deverão ser utilizados única e exclusivamente para o desempenho de atividades profissionais. Da mesma forma, cabe ressaltar que todo e qualquer meio eletrônico (chats, Skype, e-mails, páginas da rede mundial de computadores – internet – entre outros) deve ser encarado como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os acessos a e-mails e à internet, assim entendidos como ferramentas

de trabalho de propriedade da Kaeté Investimentos, poderão ser revisados pelo Diretor de Compliance e Controles Internos a qualquer momento, e passam por backups diários.

A responsabilidade do Colaborador e/ou prestador de serviços em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os itens desta política.

O não cumprimento das disposições acima previstas será considerado infração grave, passível de advertência formal e sujeito à imposição de sanções administrativas, as quais, em casos extremos, incluem o desligamento do profissional, embasado na legislação vigente. Eventuais violações às disposições previstas nesta Política serão tratadas de maneira individual e levadas imediatamente à avaliação do Diretor de Compliance e Controles Internos da Kaeté Investimentos.

Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a Kaeté Investimentos cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para fins pessoais. Adicionalmente, a Kaeté Investimentos recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da rede mundial de computadores, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis, conforme parágrafo anterior.

Com o objetivo de garantir maior alinhamento da conduta de todos os seus Colaboradores, este documento abordará alguns itens de maneira direta e específica. Vale salientar, entretanto, que esta política não deve se restringir aos aspectos tratados a seguir e que eventuais dúvidas e/ou questionamentos devem ser imediatamente levados ao conhecimento do Diretor de Compliance e Controles Internos da Kaeté Investimentos.

3.1 Utilização de senhas

A utilização de senhas para acesso às estações de trabalho, correios eletrônicos (e-mails), softwares e demais dispositivos que se façam necessários é obrigatória, cabendo a cada Colaborador a responsabilidade pelo respectivo resguardo e confidencialidade, não as repassando a terceiros. As senhas deverão possuir validade máxima de 90 dias e podem ser substituídas a qualquer momento por decisão do Diretor de Compliance e Controles Internos s ou por solicitação formal do Colaborador. Uma vez que a substituição de senhas seja necessária, o novo código deverá atender, no mínimo, às seguintes regras de complexidade:

- A senha não deve conter o nome ou parte do nome que ultrapasse 2 (dois) caracteres consecutivos;
- A senha deve possuir, no mínimo, 6 (seis) caracteres;
- A senha deve conter duas das seguintes categorias: (a) Caractere maiúsculo (de A a Z); (b) Caractere minúsculo (de a a z); (c) Dígitos (de 0 a 9); e (d) Símbolos (Ex.: !, $, #, %).

3.2 Utilização da internet

Como já explorado anteriormente, a utilização da internet no ambiente da Kaeté Investimentos deve restringir-se a assuntos profissionais. Ainda assim, a Gestora solicita a cada um de seus Colaboradores que empregue os mais elevados padrões éticos para a utilização deste meio e define as seguintes diretrizes para sua utilização:

- A internet não pode ser utilizada como ferramenta para download ou distribuição de software ou dados não legalizados;

- A internet não deve ser utilizada como ferramenta para a divulgação de informações confidenciais em grupos de discussão, Instant Messenger ou “salas de bate-papo”, não importando se a divulgação foi deliberada ou inadvertida;

- Caso a Kaeté Investimentos julgue necessário, haverá bloqueios de acesso a arquivos e/ou domínios que possam comprometer o uso de banda ou que impactem o bom andamento dos trabalhos;

- O acesso à internet poderá ser fornecido por meio de uma configuração no serviço de Proxy, o qual faz o controle e a gerência da navegação. Todo e qualquer conteúdo acessado pelos Colaboradores da Kaeté Investimentos fica devidamente registrado em arquivos mantidos no formato de “log”, os quais podem, a qualquer momento, ser acessados para a realização de trabalhos de auditoria ou revisão; e

- O acesso à internet deve, obrigatoriamente, ser realizado por meio do programa “Internet Explorer”, “Google Chrome”, “Microsoft Edge” ou outro software, desde que devidamente homologado pelo Diretor de Compliance e Controles Internos da Kaeté Investimentos.

3.3 Utilização do correio eletrônico (e-mail)

É proibida a utilização do correio eletrônico para:

- Envio ou recebimento de mensagens externas (internet) com tamanho superior a 20Mb, salvo com autorização do Diretor de Compliance e Controles Internos;
- Envio de mensagens ofensivas, difamatórias, preconceituosas, ou que possam causar hostilidade de qualquer espécie (de conteúdo religioso, sexual, político ou racial), ou que comprometam a imagem da Kaeté Investimentos;
- Envio de mensagens por outros usuários que não os responsáveis pelo login e pela senha de acesso ao sistema;
- Envio de mensagens que solicitem inscrição em listas de distribuições de mensagens na internet de assuntos não relacionados aos negócios da Kaeté Investimentos;
- Envio de mensagens com o objetivo de prejudicar o serviço de indivíduos e/ou empresas (quantidade ou tamanho excessivo de mensagens, código malicioso etc.);
- Envio de mensagens que levem o destinatário a incorrer em erro de identificação do emitente (se passar por outra pessoa);
- Envio de mensagens cujo objetivo seja a venda de serviços e/ou produtos não relacionados aos negócios da Kaeté Investimentos;
- Envio de mensagens à internet, cujo conteúdo seja confidencial ou restrito à Kaeté Investimentos e não possa tornar-se público;
- Execução de arquivos anexados a mensagens recebidas de emitentes desconhecidos ou suspeitos;
- Prática de ato que, de qualquer forma, possa ferir a legislação em vigor, as regras de sigilo bancário e direitos autorais;
- Prática de ato em contraste com os deveres profissionais e com os interesses da Kaeté Investimentos, ou a fim de violar a política da instituição sobre segurança da informação; e

O recebimento de arquivos do tipo "executáveis" (programas) será controlado por programa antivírus contido nos equipamentos de controle de mensagens.

A assinatura de e-mail será atribuída de forma automática (não é necessário assinar durante a composição da mensagem) e seguirá o seguinte padrão:

Nome do Funcionário

Kaeté Investimentos

Rua Bandeira Paulista, 702, conjunto 22, parte B, Itaim Bibi

CEP 04532-002 - São Paulo, SP

www.kaeteinvestimentos.com.br

3.4 Utilização de softwares

Tendo em vista que os equipamentos de informática disponibilizados pela Gestoras e destinam exclusivamente ao desempenho de atividades profissionais, a utilização de softwares limita-se aos programas aprovados e devidamente homologados pelo Diretor de Compliance e Controles Internos da Kaeté Investimentos. A instalação de arquivos executáveis nas estações de trabalho ou na rede é terminantemente proibida, a não ser em casos em que haja expressa autorização do Diretor de Compliance e Controles Internos.

3.5 Acesso a sistemas, bases de dados e redes

O acesso a sistemas, bases de dados e redes é restrito e definido em função do perfil de cada Colaborador da Kaeté Investimentos. O detalhamento do perfil de acesso de cada funcionário (incluindo operadores e eventuais prestadores de serviços) é realizado no momento da contratação e criteriosamente analisado pelo Diretor de Compliance e Controles Internos para cada caso. A liberação do acesso a qualquer sistema,

base de dados ou endereço de rede depende de prévia aprovação do Diretor de Compliance e Controles Internos.

Diante do exposto acima, ficam aqui estabelecidas as seguintes diretrizes:

- Tentativas para obtenção de acesso não autorizado (fraude de autenticação de usuário ou segurança de qualquer servidor, rede ou conta) não são permitidas. Inclui-se neste ponto o acesso a dados não disponíveis para o usuário, bem como a tentativa de conexão a servidores ou contas cujo acesso não tenha sido expressamente autorizado e situações que coloquem à prova a segurança de outras redes;

- Tentativas de interferência nos serviços de qualquer outro usuário, servidor ou rede não são permitidas. Inclui-se neste ponto ataques do tipo "negativa de acesso", congestionamento em redes, bem como tentativas deliberadas de sobrecarga e/ou invasão de um servidor;

- Materiais de conteúdo inapropriado (ex.: pornografia) não podem ser expostos, armazenados, distribuídos, editados ou gravados por meio do uso dos recursos computacionais da rede;

- A pasta TRANSFERÊNCIA (ou similar) não deverá ser utilizada para armazenamento de arquivos que contenham materiais de natureza sigilosa ou sensível;

- A armazenagem de arquivos inerentes às atividades profissionais desempenhadas por cada um dos Colaboradores da Kaeté Investimentos nos servidores de arquivos é obrigatória. Tal medida visa assegurar a realização de backups de segurança; e

- A varredura simples ou em massa, visando a descoberta de endereços ou portas e/ou qualquer ataque ou tentativa de invasão é terminantemente proibida.

3.6 Utilização das estações de trabalho

As estações de trabalho destinam-se exclusivamente ao exercício e ao desempenho de atividades profissionais por cada um dos Colaboradores da Kaeté Investimentos. A responsabilidade pela manutenção da integridade física das estações de trabalho cabe a cada um dos Colaboradores da empresa, sendo vedada a realização de qualquer alteração em termos de configuração, sem prévio consentimento por escrito do

Diretor de Compliance e Controles Internos. Da mesma forma, cabe a cada um dos Colaboradores bloquear a respectiva estação de trabalho durante período de ausência, de forma a garantir a total confidencialidade e integridade das informações utilizadas.

Cada Colaborador deve manter sua mesa de trabalho limpa e organizada, não deixando papéis de trabalho, relatórios ou qualquer documento confidencial em cima da mesa. Isso também é valido para scanner e impressora, ao utilizar os equipamentos, os documentos escaneados e impressos devem ser retirados imediatamente.

3.7 Utilização de mensageiros eletrônicos

Conforme informações apresentadas anteriormente, todo e qualquer dispositivo de mensagens eletrônicas deve ser encarado como ferramenta de trabalho e, como tanto, é de propriedade da empresa e destina-se a assuntos profissionais e de interesse da organização. Por se tratar de ferramenta de trabalho, todos os dispositivos estão sujeitos aos mecanismos de controle impostos pela Kaeté Investimentos.

Seguindo a mesma linha de atuação imposta aos demais requerimentos definidos por meio desta Política, a utilização de dispositivos de mensagens eletrônicas sem a devida aprovação e liberação por parte do Diretorde Compliance e Controles Internos e/ou a utilização das ferramentas disponibilizadas pela Kaeté Investimentos para a tratativa de assuntos pessoais serão alvo de constante fiscalização e poderão implicar em penalidades aos envolvidos, conforme definição estabelecida pelo Diretor de Compliance e Controles Internos.

3.8 Procedimentos de Segurança da Informação

Como forma de preservar informações confidenciais detidas pela Kaeté Investimentos, seguimos ainda as medidas de segurança abaixo:

- Sistema de Armazenamento de Dados: A Kaeté Investimentos adota o sistema de servidores remotos da Dropbox Business para gerenciar suas informações. Nesse sistema, os arquivos eletrônicos ficam armazenados remotamente em servidores seguros e com redundância. As vantagens dessa tecnologia são as seguintes: **(a)** somente usuários com senha conseguem acessar as informações confidenciais. Assim sendo, eventuais intrusos dentro da área de trabalho da Kaeté Investimentos não são capazes de acessar informações confidenciais. O

acesso é feito com uso de senhas pessoais e intransferíveis, com procedimento de verificação em 2 (duas) etapas: o acesso ao sistema só é permitido caso o usuário (i) faça uso de login e senha validados pelo sistema e (ii) acesse o sistema por meio de equipamento (computador, celular, tablet) previamente cadastrado e aprovado. Qualquer atividade na rede é monitorada, identificada (usuário, computador e IP que acessou o sistema), e pode ser revertida ou bloqueada; **(b)** existem diferentes níveis de acesso aos arquivos da empresa, podendo chegar a restrições de nível de pasta e arquivo. Dessa forma, garantimos uma maior confidencialidade das informações e reduzimos o risco de uso indevido das informações; e **(c)** backup diário das informações armazenadas localmente e redundância no armazenamento das informações e arquivos nos servidores remotos. Na ocorrência de problemas como perda de dados, os arquivos e as informações podem ser recuperados rapidamente dos servidores remotos sem grandes interrupções nas atividades da equipe.

- Trituração de material confidencial: Documentos considerados sensíveis são triturados previamente ao seu descarte, evitando assim o acesso fraudulento a nossas informações.
- Segregação de informações decorrentes de atividades distintas: A Kaeté Investimentos possui segregação física dos espaços de forma a evitar que Colaboradores de um departamento tenham acesso à informação confidencial de Colaboradores de outro departamento. Para tal, a empresa dispõe em suas dependências de 2 (duas) salas segregadas e 1 (uma) sala de reunião. A segregação ocorre também por meio do nosso sistema de armazenamento de dados em que cada departamento/equipe terá acesso apenas às informações do seu devido departamento, com controle de acesso e senhas individuais.

3.9 Classificação das informações

A fim de determinar o nível de proteção e garantir a segurança do compartilhamento de informações, a Kaeté Investimentos classifica as informações que transitam em seu ambiente físico e eletrônico da seguinte maneira:

- Pública: informação sobre a qual não há restrições quanto à divulgação, acessível a qualquer pessoa sem causar quaisquer consequências danosas aos processos da empresa;

- Interna: informação que a organização não tem interesse de divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso esta informação seja disponibilizada, não haverá danos sérios à empresa;

- Confidencial: informação interna da organização, cuja divulgação pode causar danos financeiros ou à imagem da empresa. A divulgação ainda pode gerar vantagens a eventuais concorrentes e perda de clientes.

4. Plano de Identificação e Resposta

4.1 Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance e Controles Internos prontamente. O Diretor de Compliance e Controles Internos determinará quais pessoas e, se aplicável, agências reguladoras e de segurança pública, deverão ser notificados. Ademais, o Diretor de Compliance e Compliance Internos determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

4.2 Procedimentos de Resposta

O Diretor de Compliance e Controles Internos responderá a qualquer informação de suspeita de violação, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

i. Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

ii. Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

iii. Determinação dos papéis e responsabilidades do pessoal apropriado;

iv. Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

v. Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

vi. 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);

vii. e Determinação do responsável que arcará com as perdas decorrentes do incidente, a cargo do Diretor de Compliance e Controles Internos, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

5. Arquivamento de Informações

Em cumprimento ao disposto nesta Política, os Colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos reguladores em torno de possíveis atuações da Gestora, investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com a legislação vigente.

6. Revisão desta Política

A presente política passa a vigorar a partir da data de sua aprovação por parte do Diretor de Compliance e Controles Internos.

O documento poderá ser alterado a qualquer momento e deverá passar por processo de revisão, no mínimo, a cada 2 (dois) anos. Qualquer alteração ou revisão deverá ser submetida ao Diretor de Compliance e Controles Internos.

Eventuais alterações serão prontamente comunicadas a todos os Colaboradores e partes relacionadas da Kaeté Investimentos por meio dos veículos disponíveis.