SUESTE CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E SEGURANÇA CIBERNÉTICA

Agosto de 2025
Versão 2.0

ÍNDICE

Introdução

A presente Política de Segurança das Informações e Segurança Cibernética ("Política") reflete o compromisso da Sueste Capital Gestão de Recursos Ltda. ("Sueste" ou "Gestora") com a proteção de informações sigilosas provenientes do exercício da atividade de administração de carteiras e valores mobiliários, tendo em vista que o seu mau uso pode causar danos e prejuízos para a própria Sueste, seus clientes, funcionários e fundos de investimentos e carteiras administradas pela Gestora.

A Política tem como objetivo estabelecer as diretrizes a serem seguidas em relação à adoção de procedimentos e mecanismos relativos à segurança de informações sigilosas. Com isso, os riscos de ocorrência de danos e prejuízos capazes de comprometer os objetivos e os interesses da Sueste e de seus clientes são minimizados.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela Sueste.

É mister salientar que o presente documento está em linha com os seguintes regulamentos:

- Resolução CVM n.º 21/2021;
- Resolução CVM nº 50/2021;
- Resolução CVM nº 30/2021;
- Código ANBIMA de Administração de Recursos de Terceiros;
- Guia de Cibersegurança da ANBIMA; e
- Lei nº 13.709/2018, alterada pela Lei 13.853/2019 (Lei Geral de Proteção de Dados, ou 'LGPD'), e que quaisquer inovações legislativas ou no que tangea boas práticas adotadas, ensejara a adequação e reforma do presente documento.

Aplicabilidade e Responsabilidades

A observância das regras e obrigações contidas neste Manual é dever de todos os colaboradores da Sueste, incluindo sócios, administradores, funcionários e estagiários da Gestora ("Colaboradores"), bem como, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da instituição tem a responsabilidade de proteger a segurança e integridade das informações e dos equipamentos de informática da Sueste.

Nesse sentido, todos os Integrantes deverão:

a) proteger as informações sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Sociedade;
b) assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela Sueste;
c) cumprir fielmente as leis e normas aplicáveis aos aspectos relativos a direito autoral e propriedade intelectual das informações sigilosas;
d) comunicar imediatamente o Diretor de Compliance, Risco e PLD sobre qualquer descumprimento ou violação à presente Política; e
e) caso tenham dúvidas quanto à segurança das informações sigilosas, buscar orientação de seu superior hierárquico imediato.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance da Sueste, sob a direção do Diretor de Compliance, Risco e PLD da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a Sueste conta com o suporte e assessoria da empresa terceirizada de TI.

Princípios Gerais

A fim de garantir a disponibilidade, integridade, confidencialidade, legalidade,

autenticidade e validade para fins contábeis das informações sigilosas provenientes do exercício das atividades da Sueste, sua guarda e segurança, os seguintes princípios serão sempre observados pela Gestora e seus Integrantes:

a) o acesso a informações sigilosas será concedido somente a pessoas devidamente autorizadas pela Sueste;
b) as informações sigilosas manterão sua integridade e serão protegidas contra adulterações, sendo certo que alterações, supressões e adições a tais informações somente poderão ser realizadas se autorizadas pela Sueste; e
c) as informações sigilosas serão disponibilizadas aos Integrantes autorizados sempre que necessário ao bom exercício de suas atividades.

Nenhuma informação sigilosa deverá ser divulgada a qualquer pessoa que não necessite ou não deva ter acesso a tais informações para o exercício de suas atividades profissionais, seja dentro ou fora da Sueste.

Qualquer informação sobre a Sueste, suas atividades, seus sócios, clientes ou fundos de investimento e carteiras por ela geridas, sigilosa ou não, obtida em decorrência do exercício das atividades dos Integrantes, somente poderá ser revelada ou fornecida ao público, à mídia ou a terceiros se em conformidade com as regras previstas nos documentos internos da Gestora.

Na ausência de previsão específica para o tratamento das informações acima referidas, a sua revelação ou o seu fornecimento somente poderão ocorrer mediante prévia autorização do Diretor de Compliance e PLD da Sueste.

A efetitividade desta 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.

Qualquer informação sobre a Sueste, ou de qualquer natureza relativa as 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 Compliance e PLD.

Informações Pessoais de Clientes e LGPD

A Sueste reconhece sua obrigação de respeitar, na prestação de seus serviços, os preceitos da Lei nº 13.709/2018, conforme alterada pela Lei nº 13.853/2019 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD") e todas as demais normas e leis aplicáveis à privacidade e proteção de dados dos seus clientes. Esta seção, sobre a proteção e tratamento dos dados pessoais de clientes, aplica-se a todos os clientes pessoas naturais da Gestora e, nas hipóteses cabíveis, poderá ser aplicada aos representantes e colaboradores de clientes pessoas jurídicas.

Nos termos da LGPD, a expressão "dados pessoais" abrange todas as informações relacionadas a pessoa natural que a torne identificada ou identificável, seja direta ou indiretamente (como, por exemplo, por meio da associação de diferentes informações). Por sua vez, "tratamento de dados" significa toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nos termos da LGPD, considera-se Controlador dos dados pessoais a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. A Sueste desempenha a função de controladora dos dados pessoais de seus clientes na medida em que decide sobre o seu tratamento, exclusivamente com a finalidade de prestar os serviços de gestão de recursos de terceiros.

Nos termos da LGPD, considera-se operador a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do Controlador. Sendo assim, ao Controlador cabe, por um lado, a efetiva tomada de decisões sobre o tratamento de dados pessoais (quando os dados serão tratados, de que forma serão tratados, quem estará envolvido

nesse tratamento, qual o período de tratamento etc.), enquanto ao Operador cabe o tratamento de dados pessoais propriamente dito, sob a orientação do Controlador. Sendo a Sueste o Controlador dos dados pessoais, aqueles que ela contrata para tratá-los são os Operadores, como, por exemplo a empresa contratada para administrar o sistema de controle de informações para armazenamento cadastral e controle do contato com o cliente.

Nos termos da LGPD, o Encarregado é a pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O Encarregado é responsável por algumas atividades específicas, tais como aceitar reclamações e comunicações dos titulares dos dados pessoais, prestar esclarecimentos e adotar providências, receber comunicações da ANPD e adotar providências, orientar os Integrantes a respeito das práticas a serem adotadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

No caso da Sueste, o Encarregado é **Ricardo Xavier de Oliveira Neto**, Diretor de Compliance e PLDFT. Sendo assim, para mais informações sobre o tratamento dos seus dados pessoais, os clientes deverão entrar em contato com por meio do telefone **+55 11 4040-9205** ou do e-mail ricardo.xavier@suestecapital.com.br

A coleta de dados pessoais dos clientes pela Sueste é realizada:

I. Diretamente com o próprio cliente. A partir do cadastro inicial dos clientes e ao longo do seu relacionamento com a Sueste, são coletados e tratados os dados pessoais diretamente disponibilizados por eles. Também é possível que a Gestora obtenha dados pessoais de forma indireta – como, por exemplo, por meio da gravação de chamadas telefônicas e da troca de e-mails – os quais podem ser necessários para cumprir com outras finalidades no futuro, como para atender a investigações e análises de Compliance.

II. Por meio de outras fontes. Os dados pessoais dos clientes da Sueste podem ser obtidos por meio de fontes públicas – como, por exemplo, a imprensa, os sites públicos e os bancos de dados públicos – ou por meio de terceiros que os compartilhem conosco de forma legítima – como, por exemplo, prestadores de serviços.

Conforme mencionado, muitos dos dados tratados são coletados pela Sueste diretamente com os clientes, por meio, por exemplo, do registro inicial na base de dados da gestora e do preenchimento do Questionário para definição do Perfil de Investidor dos clientes. A Gestora tratará, nos limites da legislação e regulamentação vigentes, os seguintes dados pessoais de seus clientes:

I. Dados de identificação e contato: nome completo, data e local de nascimento, nacionalidade, gênero, endereço completo, telefones de contato e endereço de e-mail.

II. Documentos de identificação: cópias e/ou números de documentos de identificação, tais como R.G., CPF, CNH, passaporte e licenças profissionais.

III. Informações financeiras: fonte de renda, patrimônio, e participações acionárias.

IV. Dados de relacionamento com a Sueste: números de identificadores de clientes, detalhes de identificação da conta, extratos de investimentos e validação de aplicação de investimentos. Dados relativos a suas interações com a Gestora, por meio de sites da Internet, páginas de mídia social, reuniões, chamadas, chats, e-mails e conversas telefônicas.

V. Informações familiares: estado civil, filiação, nome e dados de identificação do cônjuge, número de filhos ou dependentes.

VI. Informações profissionais: informações sobre formação acadêmica, profissão e histórico profissional.

VII. Dados de autenticação: tais como assinaturas e senhas.

VIII. Dados de monitoramento: gravações de vídeo e gravações telefônicas.

IX. Dados judiciais informações relacionadas a ações judiciais, protestos emandados de prisão, em observância às normas aplicáveis à Sueste.

X. Identificação como pessoa politicamente exposta: informações relacionadas ao status de pessoa politicamente exposta, quando aplicável.

A LGPD permite o tratamento de dados pessoais nas seguintes hipóteses listadas em seu artigo 7º: (i) mediante o fornecimento de consentimento pelo titular dos dados pessoais; (ii) para o cumprimento de obrigação legal ou regulatória pelo Controlador; (iii) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições da LGPD; (iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular dos dados pessoais, a pedido deste; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); (vii) para a proteção da vida ou da incolumidade física do titular dos dados pessoais ou de terceiro; (viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (ix) quando necessário para atender aos interesses legítimos do Controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular dos dados pessoais que exijam a proteção dessas informações; ou (x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No âmbito da atividade de gestão de recursos desenvolvida pela Sueste, foram identificadas as principais hipóteses em que a gestora realiza o tratamento dos dados pessoais de seus clientes. Tais hipóteses encontram-se descritas a seguir, sem prejuízo das demais hipóteses previstas na LGPD.

I. Para o cumprimento de obrigações legais e regulatórias que demandem tal tratamento.

A Sueste se encontra submetida a uma série de obrigações legais e regulatórias que demandam a coleta e tratamento de informações dos seus clientes, como, por exemplo (i) resoluções e instruções editadas pela Comissão de Valores Mobiliários aplicáveis a gestoras de investimentos; (ii) leis relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo; (iii) obrigações tributárias. Além disso, é importante destacar que a Gestora se sujeita ao cumprimento de ordens judiciais e administrativas.

Exemplificativamente, a Sueste coletará e tratará dados pessoais dos seus clientes para (i) validar a identidade destes e colocar em prática mecanismos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, conforme as exigências da Lei nº 9.613/1998, conforme alterada pela Lei nº 12.683/2012, e da Resolução CVM nº 50/2021; (ii) identificar o perfil de risco dos seus clientes e verificar a adequação deste com os produtos, serviços e operações que lhes forem oferecidos, conforme as exigências da Resolução CVM nº 30/2021; e (iii) atender a determinada exigência proferida por juízo estatal ou arbitral.

Havendo a terceirização de determinados serviços pela Sueste no âmbito das suas atividades reguladas, e desde que permitido pela regulamentação em vigor, por exemplo, a eventual guarda de documentos cadastrais e realização de providências para fins de PLDFT (como exemplo, "*background check*" do cliente), as empresas terceirizadas deverão seguir a LGPD e será importante que, no contrato a ser firmado com tais empresas, sejam contempladas cláusulas específicas, objetivas e claras sobre a observância da legislação aplicável.

II. Para executar o contrato de prestação de serviços com os seus clientes e procedimentos preliminares relacionados ao contrato.

A Sueste realizará o tratamento dos dados pessoais de seus clientes para cumprir com as obrigações ou exercer os direitos previstos no contrato de prestação de serviços firmado com os clientes, bem como para adotar medidas pré-contratuais necessárias à

celebração desse contrato e para proceder ao encerramento da relação contratual com os clientes – a pedido destes ou por decisão da Gestora.

III. Para defender os seus direitos em processos judiciais, administrativos ou arbitrais.

Nos casos em que a Sueste seja parte em processo judicial, administrativo ou arbitral, poderá tratar os dados dos seus clientes para defender os seus interesses em juízo, não havendo necessidade de obter consentimento prévio dos clientes, desde que os dados pessoais sejam utilizados exclusivamente para esse fim.

IV. Para outras situações e finalidades, desde que mediante obtenção do consentimento do cliente.

Em determinadas situações, é possível que a Sueste solicite o consentimento de clientes para tratar seus dados pessoais. Ainda que tenha consentido, o cliente poderá retirar seu consentimento a qualquer momento, por meio de procedimento gratuito e facilitado, entrando em contato com o Encarregado, cujos dados de contato encontram-se no início desta seção. A retirada do consentimento, no entanto, não afeta a legalidade do processamento de dados realizado à época em que o consentimento ainda estava válido.

Nos termos da LGPD, o Controlador que obteve o consentimento dos titulares de dados pessoais para o seu tratamento só poderá comunicar ou compartilhar dados pessoais com outros Controladores caso obtenha o consentimento específico dos titulares para este fim, exceto nos casos em que a LGPD dispensa a obtenção de consentimento do titular de dados pessoais para o seu tratamento. Dentre as hipóteses de dispensa de consentimento encontra-se (i) o tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória; (ii) o tratamento de dados pessoais para a execução de contrato do qual o titular faça parte; e (iii) o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Em determinadas circunstâncias, é possível que a Sueste transfira os dados pessoais de seus clientes para outro país. Reconhecendo que a legislação de proteção de dados em

outros países pode não garantir o mesmo nível de proteção de dados que a legislação brasileira, a Gestora compromete-se a observar a disposição a seguir.

Para transferências dos dados pessoais para países terceiros em que não houver um reconhecimento governamental de que possuam um nível adequado de proteção de dados em comparação à LGPD, a Sueste implementará mecanismos contratuais e operacionais de transferência de dados que atendam ao padrão imposto pela LGPD.

O cliente poderá entrar em contato com o Encarregado, cujo número de telefone e endereço de e-mail se encontram no início desta seção, para obter mais detalhes sobre as salvaguardas específicas aplicadas ao compartilhamento internacional dos dados pessoais.

Uma vez terminado o tratamento dos dados pessoais, estes deverão, como regra, ser eliminados. No entanto, a LGPD admite a preservação dos dados para as seguintes finalidades: (i) cumprimento de obrigação legal ou regulatória pelo Controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou (iv) uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Sendo assim, dentro das hipóteses legalmente admitidas, a Sueste manterá os dados pessoais de seus clientes:

I. Pelo tempo exigido por lei;
II. Até o término do tratamento de dados pessoais, conforme mencionado abaixo;
III. Pelo tempo necessário a preservar o legítimo interesse da Sueste;
IV. Pelo tempo necessário para resguardar o exercício regular de direitos da Sueste em processo judicial, administrativo ou arbitral.

O término do tratamento de dados pessoais ocorrerá nos seguintes casos:

I. Quando a finalidade pela qual os dados pessoais do Cliente foram coletados for

alcançada e/ou os dados pessoais coletados deixarem de ser necessários ou pertinentes ao alcance de tal finalidade;

II. Quando o Cliente exercer legitimamente o seu direito de solicitar o término do tratamento e a exclusão de seus dados pessoais; e

III. Quando houver uma determinação legal nesse sentido.

Nos casos de término de tratamento de dados pessoais, ressalvadas as hipóteses estabelecidas pela legislação aplicável ou pela presente Política de Segurança das Informações, os dados pessoais dos clientes serão eliminados.

Em consonância com a LGPD, os clientes da Sueste detêm direitos sobre os seus próprios dados pessoais tratados pela gestora, os quais incluem, mas não se limitam a:

I. Receber informações claras e completas sobre o tratamento de seus dados pessoais, incluindo maiores detalhes sobre as hipóteses de compartilhamento dos seusdados pessoais com terceiros;

II. Solicitar o acesso a seus dados pessoais e/ou a confirmação da existência de tratamento de dados pessoais pela Sueste;

III. Solicitar que retifiquemos quaisquer dados pessoais imprecisos, incompletos e desatualizados;

IV. Opor-se às atividades de tratamento, solicitar a anonimização e eliminação de dados pessoais, em circunstâncias específicas;

V. Revogar o consentimento a qualquer momento, quando a Sueste tratar seus dados pessoais com base no consentimento;

VI. Peticionar em relação aos seus dados contra o Controlador, isto é, a Sueste, perante a autoridade nacional.

Em determinadas circunstâncias legais, é possível que não seja autorizado o exercício de alguns dos direitos acima listados, ou quando o fornecimento das informações puder revelar algum segredo de negócio da Sueste.

Tais direitos podem ser exercidos pelos clientes da Sueste por meio de comunicação

direta com o Encarregado, por meio do número de telefone e endereço de e-mail constantes do início desta seção.

A Sueste utiliza medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra tratamento desautorizado ou ilegal e contra perda acidental, destruição ou danos dos mesmos. Seus dados pessoais são armazenados de maneira segura em equipamentos protegidos. Apenas um número limitado de pessoas terá acesso a tais equipamentos e apenas indivíduos com motivos legítimos terão acesso a seus dados pessoais.

As medidas previstas nesta Política de Segurança das Informações para a proteção dos dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito são aplicáveis ao tratamento e proteção dos dados pessoais dos clientes da Sueste.

Identificação de Riscos (Risk Assessment)

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

- Dados e Informações: as Informações Confidenciais, na forma do que já foi explicitado nos tópicos anteriores e incluindo informações a respeito de investidores, clientes, Integrantes e da própria Sueste, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondênciaseletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Sueste e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Sueste; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Sueste quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Sueste identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes;
- *Vírus: software* que causa danos a máquina, rede, *softwares* e banco de dados;
- *Cavalo de Troia*: aparece dentro de outro software e cria uma porta para a invasão do computador;
- *Spyware:* software malicioso para coletar e monitorar o uso de informações; e
- *Ransomware:* software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- 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.
- Engenharia social: métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados utili zando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.
- 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.

Ainda, além de ataques cibernéticos, a Sueste pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

Neste sentido, a Sueste 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.

Medidas de 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 Sueste, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Sueste, em caso de incidente de segurança.

Deste modo, a Sueste 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 3 (três) classes diferentes, quais sejam:

a) *Green Flag:*

- Quaisquer informações e/ou dados que a Sueste teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag:*

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag:*

- Todas as Informações Confidenciais, a saber:
- *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Sueste;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Sueste; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Sueste e/ou de seus sócios e clientes.

A partir da definição acima, a Sueste se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag, Yellow Flag* e *Green Flag*.

Posto isto, além de adotar condutas proativas e engajadas no que diz respeito à proteção das informações, os seguintes procedimentos devem ser observados por todos os Integrantes no exercício de suas atividades:

a) os Integrantes devem conhecer e evitar as ameaças externas capazes de afetar a segurança das informações sigilosas, como, por exemplo, vírus de computador, interceptação de mensagens eletrônicas e grampos telefônicos, além de fraudes e tentativas de roubo de senhas de acesso a sistemas de tecnologia da informação e a servidores. Para tanto, haverá treinamento anual dos Integrantes relativo à presente

Política, supervisionado pelo Diretor de Compliance e PLD;

b) todo e qualquer acesso a dados e informações da Sueste que não for expressamente autorizado é vedado;

c) assuntos relativos ao desempenho de atividades e funções na Sueste somente podem ser discutidos no espaço interno da Gestora ou em ambientes reservados que garantam a segurança das informações tratadas, e não em ambientes públicos ou em áreas expostas (como aviões, restaurantes, encontros sociais etc.);

d) as senhas conferidas aos Integrantes para o exercício de suas atribuições na Sueste são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Integrantes) nem anotadas em papéis ou em sistemas visíveis ou de acesso desprotegido;

e) os Integrantes devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

f) somente *softwares* e equipamentos homologados e previamente aprovados pela Sueste podem ser instalados e utilizados nas estações de trabalho, o que deve ser feito com exclusividade por pessoas indicadas pelo Diretor de Compliancee PLD;

g) a aquisição de softwares e hardwares para a Sueste serão objeto de prévio estudo de viabilidade, conduzido pelos sócios e pelo TI, levando em conta o alinhamento com os negócios e padrões da Gestora e o aumento da produtividade proporcionado.

h) a utilização de equipamentos pessoais nas instalações da Sueste e a sua conexão à rede interna e à internet, bem como a conexão de dispositivos móveis de armazenamento, requer autorização prévia e expressa do Diretor de Compliance e PLD;

i) os Integrantes não devem abrir e/ou executar, em seus computadores, arquivos eletrônicos de origem desconhecida;

j) a utilização do endereço de e-mail corporativo deve ser direcionada

exclusivamente aos negócios conduzidos pela Sueste, sendo permitido o uso residual de tal endereço para assuntos particulares, desde que de forma não abusiva;

k) não é permitido o envio de mensagens e arquivos que possam constranger terceiros, que tenham conteúdo político ou que possam colocar a Sueste em risco;

l) toda e qualquer mensagem eletrônica e seus anexos são para uso exclusivo do seu remetente e destinatário, não podendo ser parcial ou totalmente divulgadas, utilizadas ou reproduzidas sem o consentimento prévio do remetente ou do autor, dependendo do caso;

O Diretor de Compliance e PLD também é responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede), sendo certo que os seguintes conteúdos serão considerados como de alto risco pelo firewall e automaticamente bloqueados:

(i) Adulto;
(ii) Sexual;
(iii) Jogos e Apostas;
(iv) Ofensivos;
(v) Atividade criminal;
(vi) Armas;
(vii) Fraude;
(viii) Drogas;
(ix) Relacionamento.

É terminantemente proibido que os Integrantes façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Sueste e circulem em ambientes externos à empresa, sem prévia autorização do Diretor de Compliance e PLD. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais e/ou sensíveis. Cabe ressaltar que, em relação a informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e Compliance da Gestora.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Sueste. Nestes casos, o Integrante que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade. Ainda, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Sueste.

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

Adicionalmente, os Integrantes devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Sueste.

É proibida a conexão de equipamentos na rede da Sueste que não estejam previamente autorizados. Novos equipamentos e/ou sistemas deverão ter suas configurações pela equipe de TI. Todo acesso a USB para armazenamento e bloqueado via software nos equipamentos.

Cada Integrante é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) ao menos a cada seis meses, utilizando modelo de definição de senha de difícil identificação por parte de potenciais “hackers” externos. Tal processo será auditável e rastreável eletronicamente baseado no sistema de log-on do servidor e serviços de informação.

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que

contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Sueste.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida a instalação de nenhum software ilegal, que possua direitos autorais protegidos, ou mesmo legal, sem prévia autorização do Diretor de Compliance e PLD. Não e permitido a instalação de software nos equipamentos sendo restrito a equipe de tecnologia.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de Compliance e PLD caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas. O acesso a rede e restrito baseado na liberação definida previamente.

A Sueste mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, *worms, spyware*). Serão conduzidas varreduras semestrais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora.

A Sueste utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance e PLD é responsável por patches regulares nos sistemas da Sueste.

As informações da Sueste armazenadas em rede corporativa são atualmente objeto de

backup diário com o uso de computação na nuvem, cuja liberação para restaurar arquivos e dados perdidos depende de liberação prévia do TI.

A revelação de informações sigilosas 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, que decidirá sobre a forma mais adequada para a referida revelação.

Anualmente, a Sueste realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos Integrantes, individualização dos usuários, dentre outros.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no Relatório Anual de Controles Internos da Sueste. Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes pontos:

- identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;

- estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
- detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

- aprimoramento do plano de resposta e recuperação de incidentes (Continuidade de Negócios);

- manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e Compliance como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê de Compliance, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

Controle de Fluxo das Informações Sigilosas

A Sueste, por meio de equipe definida pelo Diretor de Compliance e PLD e/ou por meio de prestador de serviço externo, monitora continuamente o uso das informações sigilosas, dos recursos de tecnologia, dos sistemas e dos dados por ela disponibilizados e poderá usar os registros advindos desse monitoramento para atestar a observância e a adequação das regras presentes nesta Política.

Adicionalmente, todo acesso a informações sigilosas, aos ambientes estratégicos e à sede da Sueste é controlado para permitir acesso apenas às pessoas expressamente autorizadas pelo Diretor de Compliance e PLD. O controle de acesso é documentado e formalizado e contempla as seguintes metodologias:

a) necessidade de pedido formal para concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) utilização de identificador para cada Integrante, de forma a assegurar a individualização da responsabilidade de cada um por suas ações e omissões;
c) verificação da adequação do nível de acesso concedido ao perfil do Integrante;
d) remoção imediata de autorizações concedidas aos Integrantes afastados ou

desligados da Sueste;

e) adaptação das autorizações concedidas aos Integrantes que tenham mudado de função internamente na Sueste, se for o caso; e

f) revisão periódica das autorizações concedidas.

Os ramais telefônicos utilizados pelos Integrantes que exercerem funções comerciais, de gestão de carteiras de títulos e valores mobiliários terão suas ligações gravadas, sendo o respectivo conteúdo armazenado em arquivos nos servidores da Sueste. O Diretor de Compliance e PLD possui livre acesso às gravações.

Ao término de cada verificação, a Diretoria de Compliance e PLD indicará e documentará, por escrito, o arquivo acessado, a data de acesso e a eventual identificação de indícios que possam indicar eventual infração a esta Política ou a outras regras aplicáveis à Sueste.

A utilização de telefones celulares e a comunicação por mensagens instantâneas de texto e voz pela internet nas instalações internas da Sueste durante o expediente devem ser evitadas pelos Integrantes.

Além disso, os Integrantes, ao ingressarem na Sueste, deverão firmar um Termo de Confidencialidade, nos termos do Anexo I à presente Política, atestando sua ciência e compromisso relativo à preservação das informações eventualmente obtidas em razão de sua posição na Sueste.

O Diretor de Compliance e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Sueste 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) Avaliaçãoda 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, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciaisde fundo de investimento sob gestão da Sueste, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

(vii) Determinação do responsável (ou seja, a Sueste ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Sueste (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, Risco e PLD prontamente. O Diretor de Compliance, Risco e PLD determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance e PLD determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

Disposições Gerais

A presente Política encontra-se disponível para consulta pública no website da Sueste: www.suestecapital.com.br.

Quaisquer dúvidas dela decorrentes poderão ser submetidas ao Diretor de Compliance e PLD da Sueste por meio de correspondência física enviada à Avenida Presidente Juscelino Kubitschek, nº 180, Conjunto 172, Vila Nova Conceição, São Paulo/SP, CEP 04543-000, por meio do correio eletrônico

Vigência e Atualização

Esta Política será revisada anualmente e sempre que necessário, devendo ser alterada a qualquer tempo caso seu conteúdo deva ser atualizado ou em razão de circunstâncias especiais.

Anexo I

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu,_____, inscrito no CPF sob o nº _____, doravante denominado Colaborador, e **SUESTE CAPITAL GESTÃO DE RECURSOS LTDA.**, inscrita no CNPJ sob o nº 29.036.872/0001-91 ("**Sueste**").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Sueste, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1 - São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Sueste, seus sócios e clientes, aqui também contemplados os próprios FUNDOS, incluindo:

a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Sueste;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Sueste;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Sueste ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores eprestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Sueste e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

g) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Sueste ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2 - O Integrante compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Sueste, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Integrantes não autorizados, mídia, ou pessoas estranhas à Sueste, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 - O Integrante se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Sueste, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "Insider Trading", "Dicas" e "Front Running", seja atuando em benefício próprio, da Sueste ou de terceiros.

2.2 - A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3 - O Integrante entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Integrante obrigado a indenizar a Sueste, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 - O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2 - O Integrante tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4 - O Integrante reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações aclientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de

avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Sueste são e permanecerão sendo propriedade exclusiva da Sueste e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Sueste, devendo todos os documentos permanecer em poder e sob a custódia da Sueste, salvo se em virtude de interesses da Sueste for necessário que o Integrante mantenha guarda de tais documentos ou de suas cópias fora das instalações da Sueste;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Integrante, o mesmo deverá restituir imediatamente à Sueste todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Sueste, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

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

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

Integranteesteja obrigado a divulgar.

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

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

7 - A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Integrante às sanções que lhe forem atribuídas pelos sócios da Sueste.

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

[CIDADE], _____ de _____ de [ANO].

_____	_____
Colaborador	**Sueste Capital Gestão de Recursos Ltda.**

Testemunhas:

_____	_____
Nome:	Nome:
CPF:	CPF: