POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

Vínea Investimentos Ltda.

Janeiro/2025 – Versão 1.0

ÍNDICE

APRESENTAÇÃO 3
OBJETIVOS 3
ABRANGÊNCIA 3
PREMISSAS E DEFINIÇÕES .....
4 PROGRAMA DE SEGURANÇA DA VÍNEA .....
4 MONITORAMENTO E TESTES PERIÓDICOS .....
12 PLANO DE RESPOSTA 13
PROTEÇÃO DE DADOS PESSOAIS .....
14 VIGÊNCIA E ATUALIZAÇÃO .....
17 ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA .....
18

APRESENTAÇÃO

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética ("Política") da Vínea Investimentos Ltda. ("Vínea"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Vínea, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Vínea.

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 Vínea.

OBJETIVOS

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Vínea, 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 n.º 19/2021 e as melhores práticas de mercado, assim como à Lei 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados) a Vínea 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 Vínea, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Vínea, 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 *Compliance*.

ABRANGÊNCIA

Este procedimento se aplica a Vínea, 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 e dos Ativos disponibilizados pela Vínea ao Colaborador.
Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Vínea, sendo de responsabilidade individual e coletiva o seu cumprimento.

Qualquer informação sobre a Vínea, 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*.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que é de extremo valor para a Vínea, dado o princípio fundamental de confiança que a instituição trabalha para manter junto aos seus clientes, a Vínea utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA, datado de junho de 2021.

O referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a Vínea 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 Vínea, sob a direção do Diretor de *Compliance* da instituição.

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

PROGRAMA DE SEGURANÇA DA VÍNEA

(i) Identificação de Riscos:

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: • *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.
- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
- 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.

- *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.
- 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 Vínea 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.

(ii) Ações 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 Vínea, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Vínea, em caso de incidente de segurança.

Deste modo, a Vínea 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 Vínea 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 atividades da Vínea; 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 Vínea e/ou de

seus sócios e clientes.

A partir da definição acima, a Vínea 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.*

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Vínea:

Estrutura de TI

I. Propriedade dos Recursos de TI

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

II. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da Vínea têm por objetivo o desempenho das atividades profissionais da Vínea, não devendo ser utilizado para quaisquer outros fins.

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 área responsável, mediante aprovação do Diretor de *Compliance*.
A disponibilização e uso dos computadores da Vínea respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de *Compliance* autorizará, mediante solicitação, 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 área responsável, mediante supervisão e aprovação do Diretor de *Compliance*;
- O Diretor de *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável, mediante supervisão e aprovação do Diretor de *Compliance*;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela Vínea é sua assinatura eletrônica no servidor da Vínea;
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Vínea, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de *Compliance* à área responsável.

III. Softwares

A implantação e configuração de *softwares* da Vínea respeitam as seguintes regras:

- Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão e aprovação do Diretor de *Compliance;*
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada do Diretor de *Compliance*;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Vínea;
- A utilização de equipamentos pessoais por terceiros nas instalações da Vínea e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de *Compliance*. 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;
- A conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de *Compliance*.

IV. Registros

A Vínea mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela Vínea, a empresa consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM n.º 19/2021.

V. Responsabilidades 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 Vínea.

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 Vínea 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 conhecida;

• 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 Vínea.

VI. Outras Proteções aos Computadores

• Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);

• "Log-*off*" automático por inatividade durante o período de 24 horas;

• Bloqueio do acesso as portas *USB* dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;

• Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud*); • Bloqueio de sistemas de gerenciamento de computador à distância.

VII. 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 Vínea, este deve sempre resguardar a imagem da Vínea, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de *Compliance*.

O usuário é proibido de 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;

• Contenham informações que não colaborem para o alcance dos objetivos da Vínea;

• 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;

• 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 (MSN, *Skype*, etc), através dos computadores da Vínea, exceto em eventuais situações de uso profissional, sendo necessária autorização do Diretor de *Compliance*.

Também se faz expressamente proibido o uso de serviços de rádio, streaming, download de vídeos, filmes e músicas, através dos computadores da Vínea.

VIII. Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Vínea.

IX. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

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

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Vínea.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Vínea.

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

X. Endereço eletrônico de programas ou de 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 Vínea, 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 Vínea.

XI. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Vínea 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 Vínea.

XII. Responsabilidades e forma de uso de 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 Vínea.

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 Vínea, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;

• 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 Vínea; e

• Sejam incoerentes com o Código de Ética Corporativa da Vínea.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Vínea 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 Vínea.

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 Oculto/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;

• 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.

XIII. 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 servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de *Compliance*.

XIV. Armazenamento em Nuvem (*Cloud*)

A Vínea 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.

XV. Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a Vínea em relação à Cibersegurança. Neste sentido, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem.

Necessário iniciar um devido processo de *Due diligence* do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e Cibersegurança.

Com isto em mente, a empresa objeto de contratação deverá enviar a Vínea:

(i) Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;
(ii) Último relatório de teste/auditoria periódica;
(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de *Compliance* analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela Vínea.

Somente após a aprovação pela Área de *Compliance*, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à Vínea, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de *Due Dilligence* aos provedores destes serviços, tal como, porém, não exclusivamente:

(i) Software as a Service (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;

(ii) Platform *as a Service* (PaaS) – desenvolvimento, teste, uso e controle sobre *softwares* próprios; e

(iii) Infrastructure *as a Service* (IaaS) – utilização e controles sobre *softwares* próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

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 *Compliance*. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Vínea esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais.

Ademais, serão realizados Testes Periódicos de Segurança, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos logs de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Vínea, em especial os confidenciais. Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da Vínea.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Vínea desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

Estas providências consistem em:

<u>Empresa de TI Terceirizada (Sob Supervisão do *Compliance*):</u>

a) Verificação e Auditoria dos *Logs*;

b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

d) Desinstalação de *software*;

e) Execução de varreduras *offline* para descobrir quaisquer

ameaças adicionais; f) Formatação e reconstrução do sistema

operacional;

g) Substituição física de dispositivos de armazenamento;

h) Reconstrução de sistemas e redes;

i) Restauração de dados provenientes do backup realizado diariamente;

j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;

b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.
Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de *Compliance*, bem como ser formalizado no Relatório de Controles Internos da Vínea.

A Vínea deverá realizar, em caso de incidente que afetem os dados pessoais que realize tratamento, a comunicação tempestiva às partes afetadas, bem como à Autoridade Nacional de Proteção de Dados (“ANPD”)

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Vínea.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A Vínea está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou

por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Vínea, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Vínea.

Importante observar que o escopo da proteção de dados pessoais no âmbito da Vínea está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas, com especial menção ao cumprimento da regulação aplicável à consultoria de valores mobiliários. Também estão abrangidos por esta proteção os dados de clientes, fornecedores e outros com os quais a Vínea manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Vínea está pautado nos requisitos do artigo 7º da Lei 13.709/2018 (“LGPD”), assim como nas premissas do artigo 11 da mesma Lei, quando aplicável.

Princípios Norteadores:

A Vínea compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da LGPD:
I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais tem direito de solicitar à Vínea, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) confirmação de existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizado;

d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;

e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;

g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) revogação do consentimento, nos termos da Lei.

O Encarregado pelo Tratamento de Dados Pessoais da Vínea receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância a sua Política de Privacidade. O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o

responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Vínea, os titulares dos dados (pessoas físicas) e a ANPD.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Vínea durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Vínea estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Vínea, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Vínea cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:
As matérias relacionadas aos dados pessoais, dados sigilosos e aos tratamentos destes serão apresentados pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de *Compliance*.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Vínea para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38º da LGPD.

Treinamento:

A Vínea treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos periodicamente, com frequência mínima anual, podendo ser reavaliada a frequência mediante a necessidade de adequação as regras desta Política.

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.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Jan/2025	RRZ Consultoria	Versão inicial

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/MF sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informações e Segurança Cibernética da Vínea. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

[CIDADE], _____ de _____ de [ano].

_____

[Assinatura]