POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

KAPITALO INVESTIMENTOS LTDA.
KAPITALO CICLO GESTORA DE RECURSOS FINANCEIROS LTDA.
KAPITALO NEXO GESTÃO DE RECURSOS LTDA.

4 de julho de 2022

SUMÁRIO

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. Apresentação

A Política de Segurança Cibernética e da Informação ("Política") da Kapitalo Investimentos Ltda., Kapitalo Ciclo Gestora de Recursos Ltda. e Kapitalo Nexo Gestão de Recursos Ltda ("Gestoras Kapitalo"), aplica-se a todos os colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento ds gestoras, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados desta instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

2. Objetivo

As Gestoras Kapitalo reconhecem que o comprometimento com os princípios éticos e legais é indispensável para que seja mantida uma boa imagem e o alto padrão de confiabilidade de seus negócios e relacionamentos, constituindo tais princípios como a estrutura basilar para seu crescimento a médio e longo prazo dentro dos mercados financeiro e de capitais.

Assim, as políticas das Gestoras Kapitalo refletem a sua filosofia, seus princípios cotidianos, prioridades e valores básicos para os processos de tomada de decisão de investimento.

As Gestoras Kapitalo fazem sua parte ao contribuir para que os mercados financeiro e de capitais estejam fundados na justiça, solidariedade e confiança para benefício de todos os envolvidos. Dentro desta linha, as políticas das Gestoras Kapitalo têm os seguintes objetivos:

(a) assegurar a conformidade com todos os requerimentos e diretrizes legais e regulatórias. É essencial para as Gestoras Kapitalo que as autoridades regulatórias e de supervisão tenham confiança nas estruturas de controles internos e compliance das gestoras; e

(b) regulamentar a independência e eficiência das regras de compliance em relação às demais atividades desenvolvidas pelas Gestoras Kapitalo.

Nesse sentido, a presente Política visa proteger as informações de propriedade e/ou sob guarda das Gestoras Kapitalo, garantindo que os recursos computacionais e os registros sejam, disponíveis, íntegros, seguros, confidenciais, legais, autênticos e auditáveis, conforme art. 4, §8º, da Resolução CVM nº 21 de 25 de fevereiro de 2021 e do Código ANBIMA de Administração de Recursos de Terceiros ("Código ANBIMA ART").

3. Premissas e Definições

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às informações confidencias, o que é de extremo valor para as Gestoras Kapitalo, dado o princípio fundamental de confiança que as gestoras trabalham para manter junto aos seus clientes, as Gestoras Kapitalo utilizam como linha de estruturação de sua Política, o Guia de Cibersegurança da ANBIMA de dezembro de 2017.

O referido documento é um dos principias materiais sobre o tema no mercado financeiro, incluindo as melhores referências sobre proteção de dados e as melhores práticas.

Adiante, as Gestoras Kapitalo abordarão os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, as atividades da gestora.

Todas as diretrizes aqui dispostas são de responsabilidade equipe de compliance das Gestoras Kapitalo, sob a direção do responsável pelo compliance.

Ademais, para implementação e monitoramento contínuo da presente Política, as Gestoras Kapitalo contam com uma equipe de TI própria ("TI Kapitalo").

4. Segurança Cibernética

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.

(i) Identificação de Riscos

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; e
  - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- 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, as Gestoras Kapitalo podem estar sujeitas 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) <u>Ações de Prevenção e Proteção</u>

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para as Gestoras Kapitalo, em caso de incidente de segurança.

Deste modo, as Gestoras Kapitalo segregam as informações geradas pela gestora, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:

- quaisquer informações e/ou dados que a gestora 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 definidas como informações confidenciais;
- *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 pelas Gestoras Kapitalo;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pelas Gestoras Kapitalo ; 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 das Gestoras Kapitalo e/ou de seus sócios e clientes.

A partir da definição acima, a Kapitalo 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*.

(iii) Estrutura de TI

De forma a estabelecer os principais equipamentos, procedimentos e sistemas de tecnologia da informação das Gestoras Kapitalo, segue lista exemplificativa de seus recursos:

- Ambiente de rede Cisco:
  - Switches;
    - Switches Cisco C9200L
    - Switches Cisco 2960-X
  - Firewall;
    - Cisco Firepower 1140 Threat Defense
  - Call Manager;
    - Cisco 2851
    - Cisco 4321
- Storage IBM;
  - Storage IBM Storwize V5000
- Servidores IBM;
  - Servidores IBM SR630
- Servidores HP;
  - Servidores HP DL380e Gen8
- Backup;
  - Unidade de fita LTO HP Ultrium 6250

(iv) Propriedade e Disponibilização:

Todos os recursos computacionais e de sistemas disponibilizados para os colaboradores são de propriedade das Gestoras Kapitalo. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da gestora, salvo expressa permissão da equipe de compliance.

Todos os computadores disponibilizados para os colaboradores das Gestoras Kapitalo têm por objetivo o desempenho das atividades profissionais nas gestoras, não devendo ser utilizado para quaisquer outros fins.

Todo o processo de criação e exclusão de usuários, instalação de softwares e aplicativos, permissões de acesso, entre outras funcionalidades informáticas, devem ser previamente aprovada pela equipe de compliance.

a. a disponibilização e uso dos recursos tecnológicos das Gestoras Kapitalo respeitam as seguintes regras:

- a cada novo colaborador, a equipe 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 TI Kapitalo, mediante supervisão e aprovação da equipe de compliance.
- a equipe 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 TI Kapitalo, mediante supervisão e aprovação da equipe de compliance;
- a identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pelas Gestoras Kapitalo é sua assinatura eletrônica no servidor das Gestoras Kapitalo;
- será apenas permitida senhas com no mínimo 8 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 5 (cinco) vezes;
- não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pelas Gestoras Kapitalo, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo colaborador atue;
- é permitido apenas 5 (cinco) tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação à TI Kapitalo.;
- a senha possui validade de 90 (noventa) dias e sua troca será solicitada automaticamente quando da expiração da mesma; e
- todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pela equipe de compliance à TI Kapitalo.

b. A implantação e configuração de softwares das Gestoras Kapitalo respeitam as seguintes regras:

- todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela TI Kapitalo, mediante supervisão e aprovação da equipe de compliance*;*

- é desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da equipe 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 pelas Gestoras Kapitalo;
- a utilização de equipamentos pessoais por terceiros nas instalações das Gestoras Kapitalo e a conexão destes na rede interna à internet requer autorização prévia e expressa da equipe 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; e
- a conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa da equipe de compliance.

c. Demais Proteções dos Recursos Tecnológicos

- 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).;
- bloqueio de tela do computador automático por inatividade durante o período de 1 hora;
- bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores; e
- bloqueio do acesso a sites de armazenamento de dados em nuvem (*Cloud*).

O colaborador é responsável por todo acesso realizado com a sua autenticação.

As Gestoras Kapitalo mantém por 5 (cinco) 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 gestora, as Gestoras Kapitalo conseguem manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme 4º, §8º, da Resolução CVM nº 21 .

(v) <u>Responsabilidades dos Usuários:</u>

O colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O colaborador também deve garantir a integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pelas Gestoras Kapitalo.

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 das Gestoras Kapitalo 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 pelas Gestoras Kapitalo.

a. 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); e
- bloqueio de sistemas de gerenciamento de computador à distância.

b. Regras 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 das Gestoras Kapitalo, este deve sempre resguardar a imagem da gestora, 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 pela equipe 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 das Gestoras Kapitalo;
- defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física; e
- possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

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

É proibido o uso de serviços de mensagem instantânea (Skype, etc), através dos computadores das Gestoras Kapitalo, exceto em eventuais situações de uso profissional, sendo necessária autorização da equipe de compliance.

Também se faz expressamente proibido o uso de serviços de download de vídeos, filmes e músicas, através dos computadores das Gestoras Kapitalo.

(vi) 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 nas Gestoras Kapitalo.

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 gestora, a sugestão deve ser encaminhada para a equipe de compliance, 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 susceptíveis 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 das Gestoras Kapitalo; e
- sejam incoerentes com o Código de Ética das Gestoras Kapitalo.

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 das Gestoras Kapitalo 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 das Gestoras Kapitalo.

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; e
- ao uso da opção Encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O colaborador deve deixar mensagem de ausência quando for passar um período maior do que 72 (setenta e duas) 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.

5. Segregação de Atividades

As Gestoras Kapitalo reconhecem que a segregação de atividades é um requisito essencial para que seja dado o efetivo cumprimento às suas estratégias de gestão de recursos de terceiros e às suas Políticas de Investimento Pessoal e de Segurança Cibernética e da Informação.

As Gestoras Kapitalo adotam um conjunto de procedimentos estabelecidos pelo reponsável por compliance, com o objetivo de proibir e impedir o acesso e fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou colaboradores,

da instituição que não estejam diretamente envolvidos na atividade de gestão de recursos de terceiros.

Estes procedimentos também buscam(rão) impedir que estas informações possam vir a alcançar quaisquer outras empresas, que pertençam ou possam vir a pertencer ao mesmo grupo econômico ou societário que as Gestoras Kapitalo.

Atualmente, a única e exclusiva atividade exercida pelas Gestoras Kapitalo é a gestão de carteiras de títulos e valores mobiliários, caso outras empresas venham a ingressar no grupo econômico das Gestoras Kapitalo ou às Gestoras Kapitalo futuramente venham a exercer quaisquer outras atividades nos mercados financeiro e de capitais estas atividades deverão ser plena, total e infalivelmente segregadas em todos os níveis, processos administrativos, operacionais e de fluxo de informações, de forma que a higidez e segurança da sua atividade de gestão de carteiras de valores mobiliários seja sempre mantida.

Caso as Gestoras Kapitalo venham a exercer outras atividades nos mercados financeiro e de capitais, a equipe de compliance definirá, de maneira clara e precisa as práticas que assegurarão o bom, racional e eficaz uso de instalações físicas, equipamentos, arquivos e serviços comuns a mais de um setor das Gestoras Kapitalo; bem como definirá como proceder-se-á a utilização do espaço físico em sua sede e demais instalações de maneira que as atividades dos diferentes setores da empresa fiquem plenamente segregados antes, durante e após o exercício de suas atividades diárias.

6. Monitoramento e Testes de Contingência

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela TI Kapitalo, sob supervisão da equipe de compliance. O referido monitoramento acontecerá de forma contínua.

Os testes de contingência serão realizados anualmente, de modo a permitir que as Gestoras Kapitalo estejam preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos testes de contingência estão no Plano de Continuidade de Negócios das gestoras.

7. Plano de Resposta

Conforme as melhores práticas de mercado, as Gestoras Kapitalo desenvolveram 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:

(i) TI Kapitalo:

- verificação e auditoria dos *Logs*;
- criação de laudo pericial contendo as informações que foram potencialmente vazadas;
- execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
- desinstalação de software;
- dxecução de varreduras *offline* para descobrir quaisquer ameaças adicionais;
- formatação e reconstrução do sistema operacional;
- substituição física de dispositivos de armazenamento;
- reconstrução de sistemas e redes;
- restauração de dados provenientes do backup realizado diariamente; e
- entre outros.

(ii) *Compliance* ou Jurídico Contratado:

- 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; e
- em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação às partes impactadas informando o ocorrido.

(iii) BackOffice:

- análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da gestora.
- realizar planejamento dos impactos frente ao ocorrido.

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 equipe de compliance, bem como ser formalizado no relatório de controles internos das Gestoras Kapitalo.

Caso o evento tenha sido causado por algum colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética das Gestoras Kapitalo.

8. Adesão a Política de Segurança Cibernética e da Informação

Todo colaborador, através do Termo de Compromisso ao Código de Ética, Anexo I àquele código, se compromete a seguir os preceitos e regras aqui dispostas.

Ainda, todo colaborador assina o Termo de Responsabilidade e Confidencialidade, Anexo II ao Código de Ética, que ratifica o compromisso de não divulgação das informações confidencias das Gestoras Kapitalo.

9. Vigência e Atualização

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

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