KAPAM
GESTORA DE RECURSOS

Manual de *Compliance*

Março/2024

Sumário

1. Aplicabilidade do Manual de *Compliance*

1.1. O presente Manual de *Compliance* ("Manual") aplica-se compulsoriamente a todos os integrantes ("Integrantes") da KAPAM GESTORA DE RECURSOS LTDA ("KAPAM"). Os Integrantes, dentre os quais estão incluídos os sócios ("Sócios"), colaboradores, *trainees*, estagiários e demais Integrantes da KAPAM, devem aderir a este Código. A adesão formal dos Integrantes a este Código dar-se-á mediante a assinatura de "Termo de Adesão", na forma do modelo constante do Anexo I.

1.2. Os Integrantes devem se assegurar acerca do perfeito e completo entendimento do conteúdo deste Manual. Em caso de dúvidas ou necessidade de aconselhamento, é importante que se busque auxílio imediato junto ao Diretor de *Compliance* da KAPAM, o qual é o responsável pela aplicação deste Manual.

1.3. O presente Manual tem por objetivo estabelecer as regras pertinentes ao cumprimento, por parte dos Integrantes, das políticas, procedimentos e controles internos, no âmbito da KAPAM.

2. Diretoria de *Compliance*

2.1. Sem prejuízo das demais obrigações atribuídas ao Diretor de *Compliance* nos termos deste Manual, caberá ao referido comitê desempenhar as seguintes atribuições:

- administrar o cumprimento, pelos Integrantes, das disposições contidas neste Manual; e
- implementar os sistemas de controle e procedimentos internos necessários para o atendimento do disposto no item anterior.

2.2. O Diretor de *Compliance* exerce as suas funções com independência e não pode atuar em funções relacionadas à administração de carteiras de valores mobiliários, à intermediação e distribuição ou à consultoria de valores mobiliários, ou em qualquer atividade que limite a sua independência, na KAPAM ou fora dela.

2.3. O Diretor de *Compliance* deve encaminhar às Diretorias integrantes da KAPAM, até o último dia útil do mês de janeiro de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) as conclusões dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação do Diretor de Investimentos ou, quando for o caso, pelo Diretor de Risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las. Referido relatório deve ficar disponível para a Comissão de Valores Mobiliários – CVM na sede da KAPAM.

3. Política para Seleção de Prestadores de Serviços

3.1. O agente prestador dos serviços de administração, escrituração e custódia dos fundos e dos investimentos deve ser selecionado utilizando-se, no mínimo, os seguintes critérios:

- expertise comprovada em carteira de clientes no Brasil;
- posição no ranking da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais - ANBIMA;
- avaliação de reais ou potenciais conflitos de interesses entre os serviços de administração e de custódia dos ativos da KAPAM;
- clareza nas informações prestadas em relatórios gerenciais de risco e enquadramento;
- cumprimento de prazos; e
- custo dos serviços.

3.2. Como pré-qualificação para administrar as carteiras dos fundos, o candidato deve possuir um patrimônio compatível com sua atividade bem como estar devidamente autorizado pela CVM e, especificamente, quanto a fundos de ações e multimercado, o candidato deverá administrar outros fundos similares no mercado brasileiro com histórico de cotas mínimo de 12 (doze) meses.

3.3. A KAPAM tem o dever para com os clientes de buscar a melhor execução para todas as operações dos produtos de investimentos. Não só os fatores quantitativos, mas também fatores qualitativos devem ser observados. Ao se avaliar a melhor execução, o Diretor de Investimentos deve considerar toda a oferta de serviços da corretora avaliada, incluindo, entre outras coisas, a capacidade de execução da ordem, a qualidade dos departamentos de análises, a corretagem cobrada e a solidez financeira da instituição.

3.4. São características necessárias para efeito de aprovação das corretoras: a expertise operacional; a infraestrutura operacional; e os relatórios de *research*.

4. Política de *Soft Dollar*

4.1. É proibido aos integrantes oferecerem ou aceitarem presentes ou outros itens de valor sob circunstâncias em que os próprios integrantes ou clientes ou demais colaboradores possam ser influenciados.

4.2. Itens de valor incluem dinheiro, títulos, oportunidades de negócios, mercadorias, serviços, descontos em mercadorias ou serviços, entretenimento, alimentos ou bebidas.

4.3. É proibido aos integrantes, ainda:

- solicitar para si próprio ou para terceiros qualquer coisa de valor em troca de negócios com a KAPAM ou fornecimento de informação confidencial;
- dar ou aceitar dinheiro de clientes, fornecedores, prestadores de serviços, ou qualquer outra pessoa ou entidade com a qual a KAPAM mantenha relacionamento;
- utilizar a posição na KAPAM para obter qualquer coisa de valor de um cliente, fornecedor, prestador de serviço, ou qualquer outra pessoa ou entidade com a qual a empresa mantenha relacionamento; e
- exceto pelos itens abaixo relacionados, aceitar qualquer coisa de valor de qualquer pessoa ou entidade que mantenha relacionamento com a KAPAM.

4.4. Como Integrante, é permitido que se aceite:

- refeições, bebidas, acordos de viagens ou estadia de valor razoável durante o curso de uma reunião ou qualquer outro encontro de negócios; para analisar a razoabilidade do valor, deve se levar em consideração, por exemplo, se estas despesas seriam reembolsadas pela KAPAM como despesas de viagens e negócios;
- materiais de propaganda ou promocional, tais como canetas, lápis, blocos de notas, chaveiros, calendários ou outros itens similares;
- descontos ou rebates em mercadorias ou serviços que não excedam àqueles disponíveis para outros clientes;
- presentes que estejam relacionados a eventos publicamente conhecidos, tais como conferências, eventos desportivos, promoções, casamentos, aposentadorias; e
- premiações de natureza filantrópica por reconhecimento ou por serviços prestados a uma determinada comunidade.

4.5. Em caso de recebimento ou da iminência de se receber qualquer coisa de valor de um cliente, fornecedor, prestador de serviço ou qualquer outra pessoa ou entidade com quem a KAPAM mantenha relacionamento e, em circunstâncias que não estejam previstas neste Código, a Diretoria de *Compliance* deverá ser comunicada, por escrito, para a devida análise.

5. Plano de Continuidade

5.1. A KAPAM contará com sistema de *backup* em nuvem, dotado de periodicidade semanal, por meio do qual será realizado o processamento de cópias de seus respectivos sistemas de dados e das ligações telefônicas efetuadas no desempenho da atividade de administração de recursos de terceiros. A KAPAM possuirá um sistema de armazenamento que possui possibilidade de recuperação de dados remotamente através de login e senha, as quais serão disponibilizadas aos Diretores da KAPAM.

5.2. A KAPAM desenvolveu planos de contingência para efeito de gerenciamento de situações de crise, de forma a garantir a continuidade de seus negócios, até a sua completa superação.

Caso ocorra algum evento extraordinário que impossibilite a utilização de suas instalações e estrutura físicas, a KAPAM continuará as suas atividades em um escritório remoto, situado próximo a sua sede e que poderá ser utilizado em caso de contingências.

5.3. A KAPAM contratará uma empresa prestadora de serviços especializados quanto à realização de suporte técnico nas áreas de telefonia e informática, a qual será acionada sempre que necessário.

6. Política de Avaliação e Monitoramento de Ativos Privados

6.1. A KAPAM mantém Política de Avaliação e Monitoramento de Ativos Privados, observando, para tanto, os Riscos de Crédito e Contrapartes previstos no seu Manual de Gerenciamento de Riscos, no qual referidos conceitos estão explicitados.

6.2. Esta política tem início antes da realização das operações, quando é realizada a avaliação, por analistas internos da KAPAM, dos ativos privados, com base em critérios quantitativos, como a capacidade financeira dos seus emissores, e qualitativos, como a reputação, governança, estrutura da emissão e qualidade das garantias. Como apoio, podem ser utilizados também os *ratings* e pareceres emitidos por agências de classificação de risco.

6.3. Todos os ativos e emissores privados devem ser reavaliados com frequência mínima semestral. Nestas revisões, devem ser analisadas as premissas utilizadas na aprovação inicial, eventual evolução dos critérios qualitativos e quantitativos.

6.4. No caso de desenquadramento dos ativos privados, o Diretor de Gestão deverá definir as linhas de ação em relação à posição em questão. Nestas condições, o fundo fica impossibilitado de aumentar suas posições na métrica que foi excedida.

7. Política de Anticorrupção

7.1. A presente Política de Anticorrupção visa promover a adequação das atividades operacionais da KAPAM com as normas pertinentes à anticorrupção.

7.1.1. É de responsabilidade de todos os Integrantes, o conhecimento, a compreensão e a busca de meios para proteger a empresa contra procedimentos de corrupção e suborno, não sendo admitido comportamentos omissos em relação a esses assuntos. As leis e regulamentos atrelados a estes delitos, bem como as regras desta Política de Anticorrupção devem ser obrigatoriamente cumpridos.

7.1.2. Esta Política de Anticorrupção identificará a responsabilização das pessoas jurídica e individual, relacionada ao compromisso relacionado à anticorrupção.

7.1.3. O conhecimento de algum indício de ato corrupto deverá ser comunicado ao Diretor de *Compliance*, sendo este responsável por averiguar as informações reportadas e, caso aplicável, comunicar aos órgãos reguladores.

7.1.4. Os Integrantes devem obrigatoriamente reportar os casos de suspeita de atos corruptos ao Diretor de *Compliance* que será responsável por respeitar o sigilo do reporte e proporcionar a devida averiguação dos fatos.

7.1.5. O Diretor de *Compliance* será igualmente responsável por disponibilizar aos Integrantes da KAPAM treinamentos e palestras que promovam a conscientização sobre as normas anticorrupção e desenvolver campanhas/atividades que auxiliem na detecção de operações que caracterizem indícios de atos corruptos.

7.1.6. Integrantes estão proibidos de receber, oferecer, prometer, fazer, autorizar ou proporcionar (direta ou indiretamente) qualquer vantagem indevida, pagamentos, presentes ou a transferência de qualquer coisa de valor para qualquer pessoa, seja ela agente público ou não, para influenciar ou

recompensar qualquer ação oficial ou decisão de tal pessoa em benefício da KAPAM.

7.2. A Lei nº 12.846/13, em vigor desde 29 de janeiro de 2014 (a "Lei Anticorrupção"), dispõe sobre a responsabilização administrativa e civil das pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

7.2.1. O principal objeto da Lei Anticorrupção é punir as pessoas jurídicas que participem de atos de corrupção contra a administração pública, nacionais ou estrangeiros e não apenas as pessoas físicas como acontecia antes do advento da Lei.

7.2.2. A responsabilização da pessoa jurídica não exclui a responsabilidade individual de seus administradores, dirigentes ou de qualquer pessoa física que tenha participado do delito.

7.2.3. A Lei Anticorrupção determina os atos lesivos à administração pública, nacional ou estrangeira, passíveis de punição. A saber:

- prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
- comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos na mencionada lei;
- comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados.

7.3. A Lei Anticorrupção se aplica a:

- sociedades empresariais e simples;
- fundações;
- associações de entidades ou pessoas;
- sociedades estrangeiras, que tenham sede, filial ou representação no território brasileiro.

7.3.1. A responsabilidade da pessoa jurídica dos atos praticados pela administração pública continua mesmo que haja alteração contratual, transformação, incorporação, fusão ou cisão societária.

7.4. As penalidades previstas na Lei Anticorrupção são:

- multa de até 20% do faturamento bruto do último exercício anterior ao da instauração do processo administrativo, excluídos os tributos, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação;
- multa de R$ 6 mil a R$ 60 milhões, quando não for possível identificar o faturamento bruto da pessoa jurídica;
- suspensão ou interdição parcial de suas atividades;
- dissolução compulsória da pessoa jurídica;
- proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo de mínimo 1 e máximo de 5 anos;
- perda dos bens, direitos ou valores que repassem vantagem ou proveito, obtidos de forma direta ou indiretamente com a infração;
- indisponibilidade de bens, direitos ou valores necessários à garantia do pagamento da multa ou reparação do dano causado;
- registro das empresas punidas pela lei no Cadastro Nacional de Empresas Punidas (CNEP), que dará publicidade às sanções aplicadas pelos órgãos do governo, os acordos de leniência firmados, bem como seus cumprimentos ou não; e
- registro das empresas no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS).

7.4.1. As sanções se aplicam mesmo que o ato de corrupção não se concretize, somente a intenção já é passível de punições.

7.5. O descumprimento da Política de Anticorrupção implicará em:

- demissão dos Integrantes envolvidos no descumprimento em questão, incluindo aqueles que tinham conhecimento do descumprimento em questão e foram omissos em reportá-lo a seus superiores; e
- responsabilização dos Integrantes envolvidos no descumprimento por eventuais danos que a KAPAM venha a sofrer em razão de sua conduta.

7.5.1. A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos na Política de Anticorrupção.

8. Política de Segurança da Informação

8.1. Introdução

Este capítulo trata da Política de Segurança da Informação da. A informação é um ativo que possui grande valor para a KAPAM, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A Política de Segurança da Informação da KAPAM é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Seu propósito é estabelecer as diretrizes a serem seguidas pela KAPAM no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
- integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
- disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado

8.2. Objetivos

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da KAPAM.

8.3. Abrangência

A Política de Segurança da Informação da KAPAM deve estar disposta de maneira que seu conteúdo possa ser consultado a qualquer momento e aplica-se a todos os funcionários e prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da KAPAM,

ou o acesso a informações pertencentes à KAPAM. Todo e qualquer usuário de recursos computadorizados da KAPAM tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, de informações ou ainda da perda de equipamento;
- envolva a revelação de dados confidenciais, incluindo negociações e uso não autorizado de dados corporativos, ou a violação de direitos autorais ou patentes; e
- envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

É dever de todos na empresa considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a KAPAM e que deve sempre ser tratada de maneira profissional. Cabe ao colaborador buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à Segurança da Informação da KAPAM e assinar o Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação da KAPAM, bem como assumindo responsabilidade por seu cumprimento.

8.4. Aprovação e Revisão

A aprovação da Política de Segurança da Informação da KAPAM é de responsabilidade da Diretoria de *Compliance*, tendo periodicidade de revisão anual. Também é de competência da Diretoria de *Compliance* tomar as decisões administrativas referentes aos casos de descumprimento da Política.

8.5. Classificação da Informação

É de responsabilidade Diretoria de *Compliance* estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

a) Informação Pública

É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e pelo público em geral.

b) Informação Interna

É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

c) Informação Confidencial

É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

d) Informação Restrita

É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. O Diretor de *Compliance* deve orientar seus subordinados e demais integrantes a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

8.6. Dados dos Funcionários

A KAPAM se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários que porventura sejam armazenados serão considerados dados confidenciais e não serão usados para fins diferentes daqueles para os quais foram coletados. Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (*e-mails*) usados pelos funcionários.

Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da empresa, sem prévia e expressa autorização por parte da Diretoria de *Compliance*. Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos servidores de empresa, e jamais poderão fazer parte da rotina de backup da empresa. Ainda, os funcionários se comprometem a não realizar a instalação de *softwares* nos computadores da empresa sem que exista autorização prévia para tal.

8.7. Admissão e demissão de funcionários/temporários/estagiários

O setor de Recrutamento e Seleção de Pessoal da KAPAM deverá informar à Diretoria de *Compliance* e toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da empresa. Isto inclui o fornecimento de sua senha ("*password*") e registro do seu nome como usuário no sistema (*user-id*), pela Diretoria de *Compliance*.

Cabe ao setor solicitante da contratação a comunicação à Diretoria de *Compliance* sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários, deverá também ser informado o tempo em que o mesmo prestará serviço à Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas à autorização de seu acesso ao sistema. No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da KAPAM. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

9. Política de Segurança Cibernética

9.1. Definições

A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

Há diversas razões para que esses ataques ocorram e os principais motivos são:

- obter recursos financeiros;
- roubar e manipular informações;
- obter informações privilegiadas;
- sabotagem à instituição;
- disseminar falsas notícias; e
- disseminar o caos.

A segurança cibernética deve garantir:

- a segurança dos sistemas e dos bancos de dados;
- o gerenciamento das pessoas autorizadas;
- a segurança dos sistemas e informações que estão na nuvem;
- a segurança para todos os dispositivos/equipamentos;
- o planejamento da continuidade do negócio; e
- o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade
- da organização.

São exemplos de consequências/danos que podem ser causados pela falha na segurança cibernética:

- risco de imagem;
- risco de continuidade do negócio; e
- prejuízos financeiros.

9.2. Programas Ilegais

A empresa respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na KAPAM.

Periodicamente, a Diretoria de *Compliance* fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados se responsabilizam perante a companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos as sanções previstas neste documento.

9.3. Permissões e Senhas

Todo usuário para acessar os dados da rede da KAPAM, deverá possuir um login e senha previamente cadastrados pela Diretoria de Compliance e Controles Internos. Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações etc.) deverão comunicar ao seu superior imediato e à Diretoria de *Compliance* qual será o seu substituto quando de sua ausência da empresa, para que as permissões possam ser alteradas (delegação de poderes).

Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pela Diretoria de *Compliance*.

9.4. Compartilhamento de Dados

Não é permitido o compartilhamento de pastas nos computadores e desktops da empresa sem autorização prévia. Todos os dados deverão ser armazenados nos servidores da rede, e a autorização para acessá-los deverá ser fornecida pela Diretoria de *Compliance*. Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso da Diretoria de *Compliance*. Não é permitido na empresa o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

9.5. *Backup* (Cópia de Segurança dos Dados)

Todos os dados da empresa deverão ser protegidos através de rotinas sistemáticas de *backup*. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da Diretoria de *Compliance* e deverão ser feitas diariamente em um servidor na nuvem e semanalmente em um servidor externo. O backup externo não tem risco de vazamento porque é criptografado.

9.6. Cópias de Segurança de Arquivos em *Desktops*

Não é política da KAPAM o armazenamento de dados em *desktops* individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("*backups*") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da KAPAM.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da KAPAM, a Diretoria de *Compliance* disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações.

9.7. Segurança e Integridade dos dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva da Diretoria de *Compliance*, assim como a manutenção, alteração e atualização de equipamentos e programas.

9.8. Acesso à Internet

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na KAPAM. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição pela Diretoria de *Compliance* da KAPAM.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licenças de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (*downloads*), cópia ou qualquer outro tipo de acesso a sites:

- de conteúdo pornográfico ou relacionado a sexo;
- que defendam atividades ilegais;
- que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- que promovam a participação em salas de discussão de assuntos não relacionados aos
- negócios da KAPAM;
- que promovam discussão pública sobre os negócios da KAPAM, a menos que autorizado pela Diretoria de *Compliance*;
- que possibilitem a distribuição de informações de nível “Interno” ou “Confidencial”; e
- que permitam a transferência (*downloads*) de arquivos e/ou programas ilegais.

9.9. Uso do Correio Eletrônico (*e-mail*)

O correio eletrônico fornecido pela KAPAM é um instrumento de comunicação interna e externa para a realização do negócio da KAPAM. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da KAPAM, não podem ser contrárias à legislação vigente e nem aos princípios éticos da KAPAM.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- contenham declarações difamatórias e linguagem ofensiva;
- possam trazer prejuízos a outras pessoas;
- sejam hostis e inúteis;
- sejam relativas a qualquer "correntes" de *e-mail*;
- possam prejudicar a imagem da organização;
- possam prejudicar a imagem de outras empresas ou de clientes; e
- sejam incoerentes com as políticas da KAPAM.

Para incluir um novo usuário no correio eletrônico, a respectiva gerência deverá fazer um pedido formal à Diretoria de *Compliance*, que providenciará a inclusão do mesmo.

9.10. Sistemas de Telecomunicações

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da KAPAM, assim como, o uso de eventuais ramais virtuais instalados nos computadores, são de responsabilidade da Diretoria de *Compliance*, de acordo com as definições da Diretoria de *Compliance* da KAPAM.

9.11. Uso de Antivírus

Todo arquivo em mídia não proveniente da KAPAM deve ser verificado por programa antivírus. Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela Diretoria de *Compliance*, Atenção, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

9.12. Proteção da Base de Dados e Procedimentos Internos para Tratar Casos de Vazamento de Informações Confidenciais

A proteção da base de dados no âmbito da KAPAM estará lastreada nas bases legais da Lei de Proteção de Dados Pessoais, as quais, a saber estão descritas a seguir: (i) fornecimento de consentimento pelo investidor; (ii) cumprimento de obrigação legal e/ou regulatória pela KAPAM; (iii) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iv) o tratamento de dados se dará a pedido do próprio de titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares; (v) o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vi) o tratamento de dados para a tutela da saúde, desde que realizado por

profissionais de saúde, serviços de saúde ou autoridade sanitária; e (vii) a proteção do crédito, em observância às regras especificas para este tema.

Riscos de vazamento de dados serão minimizados por meio da utilização de criptografia, certificados digitais e autenticações duplas. Os melhores meios de impedir violações de dados envolvem boas práticas e noções básicas de segurança bem conhecidas, tais como: A realização de testes contínuos de vulnerabilidade e penetração: (i) aplicação de proteções, que inclui processos e políticas de segurança; (ii) Uso de senhas fortes; (iii) uso de hardware de armazenamento seguro de chaves; (iv) uso de hardware para gerenciamento de chaves e proteção de dados; e (vi) aplicação consistente dos patches de software para todos os sistemas.

Vazamentos, mesmo que involuntários, serão penalizados mediante o afastamento/demissão/desligamento imediato dos colaboradores responsáveis pelas áreas da KAPAM nas quais se deram essas violações.

10. Histórico de Revisões

Revisão	Data	Observações	Responsável
1ª	Agosto/2023	Elaboração do documento.	João Carlos Della Rocca
2ª	Abril/2024	Adequação e padronização da formatação do documento, atualização de informações e revisão geral.	João Carlos Della Rocca

Florianópolis, 26 de abril de 2024

Diretor de *Compliance*

ANEXO I

TERMO DE ADESÃO AO MANUAL DE *COMPLIANCE* DA KAPAM GESTORA DE RECURSOS LTDA.

Pelo presente instrumento, [nome do(a) declarante], inscrito no CPF/MF sob o nº [número do CPF] e portador(a) da Cédula de Identidade nº [número do RG], residente e domiciliado(a) na [endereço completo], [CEP], na cidade de [nome da cidade] e Estado de [nome do Estado] ("Declarante"), na qualidade de [nome do cargo] da KAPAM GESTORA DE RECURSOS LTDA., sociedade empresária limitada, inscrita no CNPJ/MF sob o nº 51.224.521/000163, com sede na cidade de Florianópolis, Estado de Santa Catarina ("KAPAM"), vem, por meio deste Termo de Adesão, declarar ter integral conhecimento das regras constantes do Manual de *Compliance*, obrigando-se a pautar as suas ações na KAPAM em conformidade com tais regras, sujeitando-se, ainda, às penalidades cabíveis.

Florianópolis, [dia] de [mês] de [ano]

_____

[nome do Declarante]

03. Manual de Compliance_v2.pdf

Documento número #3b70eea0-0edf-4885-a716-302fdd3998de

Hash do documento original (SHA256): 37a4bcc740da839b5460ad088c2fcec47de4c76943077025e13c7c30a76e4a5d

Assinaturas

João Carlos Della Rocca
CPF: 343.208.739-04
Assinou em 26 abr 2024 às 20:05:00

Log

26 abr 2024, 15:51:59	Operador com email matheus@kapam.com.br na Conta ab7e07c4-4b06-4ad7-b794-65786416ce25 criou este documento número 3b70eea0-0edf-4885-a716-302fdd3998de. Data limite para assinatura do documento: 26 de maio de 2024 (15:49). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
26 abr 2024, 15:52:00	Operador com email matheus@kapam.com.br na Conta ab7e07c4-4b06-4ad7-b794-65786416ce25 adicionou à Lista de Assinatura: dellarocca@kapam.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo João Carlos Della Rocca e CPF 343.208.739-04.
26 abr 2024, 20:05:00	João Carlos Della Rocca assinou. Pontos de autenticação: Token via E-mail dellarocca@kapam.com.br. CPF informado: 343.208.739-04. IP: 187.181.181.239. Componente de assinatura versão 1.836.1 disponibilizado em https://app.clicksign.com.
26 abr 2024, 20:05:01	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 3b70eea0-0edf-4885-a716-302fdd3998de.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 3b70eea0-0edf-4885-a716-302fdd3998de, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.