# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA DA ALPHAKEY CAPITAL MANAGEMENT INVESTIMENTOS LTDA.

Abril- 2026

Esta Política de Segurança da Informação e Cibernética ("Política") estabelece diretrizes aplicáveis a todos os Colaboradores Internos da **ALPHAKEY CAPITAL MANAGEMENT INVESTIMENTOS LTDA.** ("AlphaKey").

Os Colaboradores devem observar integralmente as disposições desta Política e assumem a responsabilidade profissional de atuar de forma ética em todas as atividades que desempenhem, zelando pela proteção das informações da AlphaKey.

Para fins da presente Política, serão aplicadas as definições listadas no Item I do Código de Ética e de Políticas Internas da AlphaKey, salvo se outro significado lhes for expressamente atribuído neste documento.

Adicionalmente ao disposto no presente documento, serão aplicadas as políticas do prestador de serviços de TI (Norma de Utilização de Recursos da Rede Corporativa e Diretrizes de Segurança da Informação da Tecnoqualify) que prestam serviço de TI para a AlphaKey.

## 1. Objetivos

Esta Política tem por objetivo estabelecer diretrizes para a proteção das informações confidenciais, dados, equipamentos e sistemas utilizados ou sob a responsabilidade da AlphaKey, visando prevenir o acesso não autorizado, o uso indevido, a perda, a indisponibilidade, o sequestro de dados e outros incidentes de segurança da informação e cibernéticos.

## 2. Responsabilidades

### 2.1. Da Administração

(i) Direcionar os esforços e recursos para a segurança da informação, de acordo com a estratégia de negócios da empresa;

(ii) Aprovar as normas de segurança da informação e suas atualizações;

(iii) Aprovar os controles a serem utilizados para garantir a segurança das informações, bem como a implementação e aplicação efetiva dos princípios e direitos previstos na Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 - LGPD), na condição de Encarregado;

(iv) Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI e pela Diretoria de *Compliance*;

(v) Comunicar a Diretoria de *Compliance* os casos de violações ou indícios de violação das Políticas Internas relativas à informação;

(vi) Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados, inclusive no que diz respeito à capacitação dos Colaboradores sobre o tema;

(vii) Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;

(viii) Delegar as funções de segurança da informação aos profissionais responsáveis;

(ix) Coordenar a elaboração do relatório de impacto à proteção de dados pessoais, sempre que exigido pelas autoridades competentes.

### 2.2. Da Empresa Prestadora de Serviços de TI

(i) Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;

(ii) Orientar os testes da infraestrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;

(iii) Assessorar as demais áreas da empresa no processo de classificação das informações;

(iv) Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;

(v) Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;

(vi) Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;

(vii) Manter a infraestrutura que suporta o ambiente controlado;

(viii) Manter a infraestrutura e sistemas atualizados;

(ix) Garantir a implementação e operação dos indicadores de segurança;

(x) Notificar imediatamente os incidentes de segurança à diretoria;

(xi) Garantir a rápida tomada de ações em caso de incidentes de segurança.

### 2.3. Da Diretoria de *Compliance*

(i) Desenvolver, manter e implementar programas de treinamento e de conscientização aos Colaboradores Internos e Externos sobre as normas de segurança da informação, a forma como ela está estruturada e os principais conceitos de segurança da informação;

(ii) Decidir o tratamento que será dispensado aos dados de terceiros coletados e/ou armazenados nos diretórios da AlphaKey, na condição de Controlador a que se refere a LGPD, bem como realizá-lo, na qualidade de Operador previsto naquela legislação;

(iii) Obter o consentimento dos titulares para uso de dados pessoais não decorrentes de obrigação legal;

(iv) Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;

(v) Em conjunto com a Administração, determinar as sanções cabíveis;

(vi) Revisar periodicamente as políticas internas relacionadas à Segurança da Informação e sugerir as alterações necessárias.

## 3. Segurança da Informação

### 3.1. Aspectos Gerais

São consideradas informações confidenciais, nos termos do Código de Ética e de Políticas Internas da AlphaKey, todas as informações relacionadas a sistemas, negócios, estratégias, posições, operações ou clientes da AlphaKey.

Todos os Colaboradores e terceiros que tenham acesso a informações confidenciais da AlphaKey devem zelar pela sua confidencialidade, adotando as cautelas necessárias para evitar divulgação, acesso ou uso indevido.

### 3.2. Gestão da Segurança da Informação

Conforme já abordado, as informações e os dados da AlphaKey constituem ativos relevantes e essenciais para o desenvolvimento de suas atividades. Dessa forma, é de extrema importância que tais informações sejam armazenadas, tratadas e processadas em ambientes seguros, bem como que todas as pessoas que tenham acesso a essas informações sejam responsáveis pelo cumprimento dos processos de segurança definidos neste documento.

Todos os colaboradores e/ou terceiros que tiverem acesso a informações confidenciais da AlphaKey devem zelar pela manutenção de sua confidencialidade. Assim, recomenda-se que os Colaboradores não comentem informações obtidas no ambiente de trabalho em locais públicos e adotem as devidas precauções para que conversas telefônicas sejam mantidas em sigilo e não possam ser ouvidas por terceiros.

Cada Colaborador é responsável por manter o controle e a segurança das informações armazenadas ou disponibilizadas nos equipamentos, sistemas e softwares sob sua responsabilidade. Para acesso à rede, aos sistemas e ao correio eletrônico corporativo, cada Colaborador dispõe de um login individual e deverá criar e manter senha de acesso pessoal, sigilosa e intransferível.

É proibido que os Colaboradores realizem cópias (físicas ou eletrônicas), transmitam ou imprimam arquivos utilizados, gerados ou disponíveis na rede da AlphaKey, bem como circulem com eles em ambientes externos à empresa, uma vez que possuem Informações Confidenciais. As exceções devem ser autorizadas pela Diretora de *Compliance*, pelo CEO ou pelo Diretor de Gestão.

A vedação acima não se aplica quando as cópias e/ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da AlphaKey. Nesses casos, o

Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo será o responsável direto por sua adequada conservação, integridade e manutenção de sua confidencialidade.

Toda impressão de documentos deverá ser retirada imediatamente da máquina impressora, uma vez que pode conter informações restritas e/ou confidenciais, inclusive no ambiente interno da AlphaKey.

O descarte de informações confidenciais em meio digital deverá ser realizado de forma a impossibilitar sua recuperação, ou seja, mediante a exclusão permanente do arquivo, inclusive na pasta "Lixeira/Trash" do computador. Os documentos físicos que contenham informações confidenciais, bem como suas cópias, deverão ser destruídos por trituradora ou qualquer outro método que impeça e a sua recuperação ou leitura.

É proibida a conexão de equipamentos na rede da AlphaKey que não estejam previamente autorizados pelo responsável pela área de informática e pela Diretora de *Compliance*.

Somente os arquivos de interesse da AlphaKey poderão ser armazenados na rede corporativa. É proibido o armazenamento de arquivos de conteúdo pornográfico, jogos, filmes, arquivos de áudio e/ou vídeo, *softwares* não autorizados e documentos sem relação com as atividades profissionais da AlphaKey, sejam mensagens de correio eletrônico, *drives* de rede ou nas estações corporativas.

O uso do serviço de *internet* nos equipamentos fornecidos pela AlphaKey não é autorizado para:

(i) Acesso a *sites, blogs, fotologs, webmails*, entre outros, que contenham conteúdo discriminatórios, preconceituosos (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), abusivos, ameaçadores, obscenos, pornográficos, ofensivos ou de qualquer outra forma censurável;

(ii) d*ownload* de aplicativos de qualquer natureza ou procedência sem o consentimento da Diretora de *Compliance* da AlphaKey;

(iii) fins comerciais ou de ganho pessoal, que sejam incompatíveis com a finalidade da ferramenta ou da função do usuário.

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

Embora o recebimento de e-mails muitas vezes não dependa da vontade do Colaborador, espera-se que, na eventualidade do recebimento de mensagens com as características acima descritas, estas sejam apagadas imediatamente, de modo que permanecerem o menor tempo possível nos servidores e computadores da AlphaKey.

O acesso à internet e o uso do correio eletrônico corporativo não são privativos e poderão ser monitorados quando necessário, podendo o serviço ser bloqueado sem aviso prévio em caso de violação às disposições desta Política.

Os Colaboradores envidar seus melhores esforços para assegurar que os prestadores de serviços que venham a ter acesso a Informações Confidenciais da AlphaKey, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham o devido sigilo e confidencialidade das informações recebidas.

## 4. Equipamentos

Os equipamentos objeto desta Política são os de propriedade da AlphaKey, tais como *desktops*, monitores, teclados, *mouses*, telefone, impressoras, desfragmentador de papéis e outros destinados ao uso pessoal ou comum dos Colaboradores da AlphaKey. Eles deverão ser utilizados exclusivamente para fins profissionais, estão sujeitos ao monitoramento pela Diretoria de *Compliance* e o uso indevido está sujeito às penalidades previstas no Código de Ética.

Em caso de quebra ou indisponibilidade de equipamento (*desktop*, teclado, *mouse*, monitor, telefone), estarão disponíveis para uso imediato os equipamentos de contingência. Para isso, é necessário informar o responsável pela infraestrutura, para que ele atue rapidamente para sanar o problema.

Nas hipóteses em que for necessário acionar uma infraestrutura replicada - física ou virtualizada - que garanta a substituição de um servidor, roteador, *nobreak* e/ou outro equipamento de TI que falhe ou esteja inacessível (Redundância de TI) entrará em operação a Política de Continuidade dos Negócios da AlphaKey.

## 5. Controle de acesso ao escritório e a Rede

Os Colaboradores terão acesso identificado às dependências da AlphaKey por meio de controle biométrico.

O acesso de pessoas estranhas às instalações físicas da AlphaKey, deverá ser previamente autorizado pelo Colaborador que as convidou e ele será responsável por tais pessoas durante todo o período de sua permanência no escritório. O acesso de pessoas não autorizadas – seja ela interna ou externa - nas áreas restritas somente será permitida com a autorização expressa da Administração e/ou da Diretoria de *Compliance*.

Quaisquer trabalhos que envolvam informações confidenciais deverão ser realizados exclusivamente em áreas seguras e por meio de sistemas e dispositivos devidamente protegidos.

Cada Colaborador terá acesso, na rede interna, apenas aos arquivos, sistemas e pastas estritamente necessários ao desempenho de suas atividades. A segregação de acessos será definida pela Alta Administração e pelos heads de cada área, sendo implementada pelo time de Tecnologia da Informação (TI). A área de Compliance deverá, periodicamente, verificar se os acessos concedidos permanecem adequados às funções exercidas.

Não obstante a segregação de acessos, determinadas informações poderão ser compartilhadas quando necessárias ao eficiente exercício das atividades da gestora, hipótese em que os Colaboradores que a elas tiverem acesso deverão zelar pelo seu uso adequado e pela manutenção de seu caráter confidencial.Os computadores, telefones, acesso à internet, *e-mail* e demais facilidades disponíveis no espaço físico da AlphaKey são de sua propriedade e se destinam-se exclusivamente a fins profissionais. Cada Colaborador é responsável por zelar pela segurança das informações armazenadas ou acessadas por meio dos equipamentos sob sua responsabilidade.

Todo Colaborador deverá utilizar de forma adequada os equipamentos e sistemas a ele disponibilizados, bem como zelar pela correta utilização dos demais ativos da AlphaKey. Caso seja identificada  má conservação, uso indevido ou inadequado de qualquer ativo ou sistema, o fato deverá ser imediatamente comunicado à Diretora de *Compliance*.

O acesso remoto a arquivos, sistemas internos ou em nuvem deve observar controles adequados, definidos a critério do responsável pela segurança cibernética, sendo realizado exclusivamente por meio de credenciais individuais de acesso (usuário e senha próprios).

## 6. Instalações elétricas e o sistema de refrigeração

A fim de assegurar as condições ideais de funcionamento da Infraestrutura de TI, evitando perda de dados por falta ou sobrecarga de energia ou superaquecimento; e danos aos equipamentos de informática, é imprescindível instalações elétricas e sistema de refrigeração adequados.

Ambos foram dimensionados de acordo com a estrutura instalada sob orientação de profissionais especializados e é feita manutenção periódica, para garantir que as instalações continuam funcionando adequadamente.

## 7. Funcionamento contínuo dos Recursos de TI

Os Recursos de TI em sistema *no-stop* será feito por *nobreak,* que garante o funcionamento da infraestrutura por tempo suficiente para que nenhuma informação seja perdida quando ocorre falta de energia elétrica. Os critérios de funcionamento e o procedimento para realização dos testes de verificação estão descritos na Política de Continuidade dos Negócios.

Adicionalmente, vale ressaltar que o prédio em que o escritório da AlphaKey está localizado possui gerador, que em caso de interrupção no fornecimento de energia, passa a funcionar imediatamente de maneira ininterrupta, até o fornecimento de energia voltar a funcionar. O gerador abastece tanto as áreas comuns do prédio, como o escritório da gestora.

## 8. *Firewall*

As intrusões ou invasões são praticadas por pessoas que pretendem acessar, roubar ou sequestrar dados confidenciais e/ou informações privilegiadas, capturar dados para realização de fraudes, causar danos a sistemas e aplicativos.

A fim de evitar esses riscos, a AlphaKey conta com um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e desses com redes externas ("*Firewall*"). Ele trabalha segundo protocolos de segurança que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

Seu funcionamento é contínuo, as atualizações são programadas e realizadas automaticamente pelo sistema.

## 9. Senhas

A AlphaKey adota uma estrutura e configuração que induz a criação de senhas fortes, a fim de dificultar o acesso de pessoas mal-intencionadas em seus sistemas. Há, ainda, um mecanismo automático que obriga os usuários ativos a realizarem a troca periódica de suas e cancela as senhas de usuários inativos/desligados da organização.

A senha e o *login* para acesso aos dados contidos em todos os computadores, bem como nos *e-mails*, são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Assim, o Colaborador pode ser penalizado caso os compartilhe com terceiros para quaisquer fins.

## 10. *Softwares*

A AlphaKey possui as licenças de uso de todos os *softwares* que utiliza. A Administração é responsável pelas renovações nos prazos e termos definidos em cada contrato.

É proibido o *download* de aplicativos de qualquer natureza ou procedência sem o consentimento da Diretoria de *Compliance*.

## 11. Correspondências eletrônicas ("*e-mails*" e *chats*)

Apenas os Colaboradores Internos e sócios da AlphaKey possuirão contas de *e-mail* corporativo, que serão criadas pela empresa responsável pela Infraestrutura de TI no momento da contratação ou integralização de cotas sociais.

O responsável pela conta de *e-mail* individual ou da área deverá lhe atribuir uma senha de acesso pessoal, sigilosa e intransferível.

Todos os e-mails trocados utilizando as contas da AlphaKey poderão ser acessados para fins de monitoramento pela Diretoria de *Compliance.*

Em caso de desligamento do Colaborador ou retirada do sócio, o acesso ao respectivo *e-mail* será imediatamente bloqueado pelo profissional de TI por orientação da Diretoria de *Compliance*.

Os *e-mails* serão armazenados pela Microsoft, que proverá também os serviços de Anti*Spam,* antivírus, recuperação de informação, *site* de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

As ordens de negociação de ativos e demais comunicações realizadas pela equipe de gestão por meio do *chat* do Bloomberg, que são baixadas periodicamente e podem ser analisadas pelo time de *Compliance*.

## 12. Armazenamento duplo de dados *(back up)*

Com vistas a evitar a perda de informações proprietárias, confidenciais e/ou privilegiadas, a AlphaKey adota a armazenagem duplicada de dados em HD externo e, ainda, em *cloud*. O *backup* de dados em HD externo é realizado automaticamente, abrange todos os dados do servidor local e é mantido por período mínimo de 180 dias. O *back up* em *cloud* é mantido por tempo indeterminado sendo limitado apenas ao espaço disponível.

## 13. Telefone

A AlphaKey definirá os Colaboradores que terão acesso à linha telefônica corporativa, conforme a atividade que desempenhem.

O uso do telefone deverá se restringir às atividades profissionais em prol da AlphaKey e estará sujeita à gravação automática que será mantida por até 90 dias, para fins de monitoramento e confirmação de operações.

O monitoramento poderá ser feito periodicamente à critério da Diretoria de *Compliance,* mediante acesso ao portal do provedor de telefonia contratado, a fim de fazer cumprir o Código de Ética.

AlphaKey conta com 7 linhas VOIP e 1 linha analógica, que serve como backup e que só será utilizada e ligada em caso de contingência. Em caso de falhas nas linhas telefônicas VOIP, poderão ser utilizadas as linhas analógicas.

## 14. Internet

O acesso à internet é disponibilizado por 2 links de velocidade: um link dedicado (Mundivox) de 200 mbps e 1 link ADSL (VIVO). Os sistemas estão permanentemente disponíveis e são ativados automaticamente em caso de perda de sinal do outro provedor.

## 15. Dados de terceiros

A AlphaKey trata dados pessoais primordialmente para o cumprimento de obrigação legal. Nos demais casos, será obtido consentimento do titular.

Os dados de terceiros, quer sejam Colaboradores ou Clientes, que venham a ser compartilhados com a AlphaKey, deverão ser tratados como confidenciais, nos termos da Política

descrita no item 12 do Código de Ética, A Política de Privacidade e de acordo com as especificidades da LGPD.

## 16. Erros de procedimentos internos

Procedimentos de gestão da segurança da informação mal estruturados ou desatualizados podem acarretar vulnerabilidades e perdas de dados. Essas vulnerabilidades se manifestam por falhas no desenvolvimento, na implementação ou na configuração de mecanismos de segurança em *softwares,* no funcionamento dos *hardwares* ou em exposição a ameaças previsíveis.

A AlphaKey conta com equipe especializada para a execução dos protocolos de manutenção e segurança de seus Recursos de TI, como apontado acima.

## 17. Crises ou situações críticas

### 17.1. Vazamento de Informações

Caso ocorra o vazamento de quaisquer Informações, ainda que de forma involuntária, a Diretora de Compliance deverá ser informada, assim que possível. Com base das informações, ela irá tomar as medidas necessárias para conter o vazamento e as consequências deles. Caso julgue necessário, poderão ser contratados consultores e/ou advogados externos, para auxiliar a AlphaKey nesse processo.

a) No caso de vazamento de Informações relativas aos Fundos ou às suas Classes:

A AlphaKey irá liberar em seu site um fato relevante, conforme exposto na regulamentação vigente. Esse procedimento visa garantir que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao Fundo ou às suas Classes.

b) No caso de vazamento de Informações relativas aos cotistas:

A AlphaKey irá seguir com a análise do vazamento, elaborando um relatório contendo as informações vazadas, a abrangência e os potenciais impactos. Junto com isso, ela irá trabalhar para conter possíveis danos, elaborando um plano. A gestora, caso possível, irá comunicar todos os cotistas impactados, explicando a ocorrência e as atitudes tomadas pela gestora para conter os impactos.

### 17.2. Outros

Na hipótese de situações não rotineiras em que os mecanismos descritos nesta Política se tornarem insuficientes ou ficarem indisponíveis, será acionada a Política de Continuidade dos Negócios, no que couber.

## 18. Revisão

A presente Política será revisada, no mínimo, anualmente, considerando, dentre outras questões, mudanças regulatórias ou eventuais deficiências encontradas. Esta Política poderá ser também revista a qualquer momento, sempre que a Diretora de Compliance e Risco entender necessário.

****

| Alteração inserida | Ano | Responsável | Aprovação |
|---|---|---|---|
| Atualização da forma de back up (HD externo) | 2020 | Simone de Grandis | Diretor-Presidente |
| Menção aos canais de comunicação | 2020 | Simone de Grandis | Diretor-Presidente |
| Explicitação do sistema de gravação de ramais, monitoramento de emails e gravação do chat Bloomberg | 2020 | Simone de Grandis | Diretor-Presidente |
| Fornecedor do link dedicado | 2021 | Simone de Grandis | Diretor-Presidente |
| Revisão Anual | 2022 | Simone de Grandis | Diretor-Presidente |
| Revisão Anual | 2024 | Daniela Sessa | Comitê de Compliance |
| Revisão Anual | 2025 | Daniela Sessa | Comitê de Compliance |