POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

1.1. O objetivo desta política é estabelecer as diretrizes de segurança da informação e cibernética da Nikos Gestão de Recursos Ltda. ("Política" e "Gestora", respectivamente), visando garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas da instituição, definir controles e procedimentos para prevenir, detectar e tratar incidentes de segurança, e reduzir riscos de perdas financeiras, danos à imagem ou impactos operacionais decorrentes de falhas de segurança da informação.

2. ABRANGÊNCIA

2.1. Esta abrange todos os Colaboradores da Gestora.

3. DIRETRIZES

3.1. Com relação à gestão de acessos e autenticação:

i. a Gestora fornece aos seus colaboradores contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais por meio de processo formalizado e auditável;

ii. as contas de acesso são fornecidas exclusivamente para que os colaboradores possam executar suas atividades laborais.

iii. as senhas associadas às contas de acesso, aos ativos/serviços de informação ou aos recursos computacionais da Gestora são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

iv. a Gestora adota controle de acesso lógico no ambiente dos clientes, a fim de proteger seus dados, bem como sistemas, programas, redes e dados da Gestora, contra acessos por pessoas ou computadores não autorizados, envolvendo medidas como a adequada identificação dos usuários, a prevenção e desabilitação de acessos e o monitoramento de privilégios;

v. todas as contas usadas para acessar a rede da Gestora por meio de uma Virtual Private Network (VPN), necessariamente devem possuir o Segundo Fator de Autenticação; e

vi. a Gestora utiliza-se de soluções de criptografia seguindo padrões dos órgãos reguladores e as melhores práticas de Segurança da Informação.

3.2. Para assegurar a proteção adequada às informações da Gestora, deve existir um método de classificação e rotulagem da informação, de acordo com o grau de confidencialidade, relevância e criticidade para os negócios da Gestora.

3.2.1. A classificação deve seguir os seguintes rótulos: (a) Confidencial; (b) Interna; ou (c) Pública, considerando as necessidades e relevância relacionadas ao negócio.

3.2.2. Os colaboradores devem manter a confidencialidade sobre assuntos relacionados à Gestora, adquiridos durante a execução de suas funções. Informações confidenciais devem ser compartilhadas apenas internamente e somente com as pessoas que realmente precisem ter acesso a esses dados, ou, se necessário, mediante autorização do Diretor responsável pela gestão, sempre em conformidade com esta Política. A obrigação de preservar a confidencialidade se estende inclusive após o término do vínculo do colaborador com a Gestora.

3.2.3. Além disso, os colaboradores precisam evitar a divulgação desnecessária de qualquer dado interno da Gestora, utilizando tais informações de maneira criteriosa e adequada, sempre em alinhamento com os interesses da Gestora.

3.2.4. Informações referentes às carteiras de quaisquer classes de fundos geridos pela Gestora são classificadas como confidenciais e não devem ser compartilhadas com terceiros, salvo se houver autorização expressa de algum diretor da Gestora ou ainda por exigência legal ou regulatória de autoridade competente.

3.2.5. Serão, ainda, classificados como sensíveis e deverão ter prioridade quanto à sua proteção, segurança e confidencialidade os dados cadastrais e demais dados dos fundos geridos pela Gestora, bem como suas operações e posições de custódia, além de dados pessoais de outros titulares, como parceiros e colaboradores, tratados pela Gestora, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações.

3.2.6. Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da Gestora em todo o seu ciclo de vida, compreendendo, mas não se limitando à geração ou coleta, manuseio, armazenamento, transporte e descarte.

3.2.7. A informação deve ser utilizada de forma transparente, priorizando sua minimização, e apenas para a finalidade e pelo tempo necessário para que foi coletada e/ou para usos estatísticos, evitando-se, sempre que possível, a possibilidade de identificação dos clientes e, na hipótese de dados pessoais, atendendo à legislação aplicável, notadamente a Lei Geral de Proteção de Dados ("LGPD").

3.2.8. A reprodução ou transferência de informações confidenciais e sigilosas, sob qualquer formato, será considerada infração grave se não estiver de acordo com as atribuições delegadas aos colaboradores, ou quando contrária às diretrizes estabelecidas nesta Política.

3.2.9. O Diretor de Risco e Compliance irá apurar os casos de divulgação indevida de informação confidencial e o responsável por tal divulgação estará sujeito às penalidades descritas nesta Política, sem prejuízo de sanções na esfera cível e criminal.

3.3. Com relação à gestão de incidentes de segurança da informação, deve-se:

i. tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente detectados, registrados, classificados, investigados, corrigidos, documentados e, quando da ocorrência de incidente relevante que afete sistemas críticos e tenha impacto significativo sobre os clientes, comunicados tempestivamente às autoridades competentes, à Comissão de Valores Mobiliários ("CVM") e à Diretoria da Gestora, conforme aplicável;

ii. definir procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das atividades operacionais da Gestora;

iii. definir critérios para avaliação da relevância de incidentes de segurança da informação, levando em conta aspectos como a criticidade do processo atingido, o potencial de impacto sobre dados pessoais, sua natureza, categoria e quantidade de titulares afetados, bem como as consequências concretas e prováveis do incidente;

iv. notificar entidades reguladoras e autoridades, inclusive a Autoridade Nacional de Proteção de Dados ("ANPD"), parceiros comerciais, titulares de dados pessoais, clientes, incluindo instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil ("BCB"), quando aplicável e desde que não sejam informações protegidas por sigilo, sobre todos os incidentes que tenham potencial ou comprovado comprometimento de dados dos clientes, parceiros, colaboradores, ou quaisquer titulares de dados pessoais tratados pela Gestora, na forma da legislação e regulamentação vigente, ou em não mais que 48 (quarenta e oito) horas após a conclusão da investigação do evento.

3.4. Periodicamente, a Gestora realizará varreduras em suas redes internas e externas para identificação de vulnerabilidades conhecidas.

3.4.1. As vulnerabilidades serão classificadas, tratadas e priorizadas, de acordo com o nível de risco apresentado. O Diretor de Risco e Compliance realiza, sempre que julgar necessário, o monitoramento por amostragem do acesso dos Colaboradores a: (i) sites, blogs, fotologs, webmails; e (ii) e-mails enviados e recebidos. Também por amostragem, verificará as informações de acesso a: (i) espaço do escritório; e (ii) desktops, pastas e sistemas utilizados.

3.4.2. O objetivo é avaliar a aderência às regras de restrição de acesso e escalonamento. O Diretor de Risco e Compliance, pode adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos previstos, avaliando seu cumprimento e eficácia

3.5. Softwares antivírus atualizados são responsáveis por detectar, prevenir e eliminar programas maliciosos (como vírus, worms e spyware) nos dispositivos da Gestora. Verificações frequentes identificam e removem qualquer software que tente obter acesso não autorizado à rede

3.6. Os colaboradores apenas irão conseguir realizar o acesso as suas ferramentas de trabalho através de desktop ou notebook, o qual deverá conter uma senha pessoal e intransferível ou outro dispositivo autorizado pela área de Risco e Compliance. Cada colaborador, quando de sua entrada na Gestora, receberá uma permissão específica para entrar nas pastas e diretórios de rede aplicáveis à sua atividade. Caso seja necessário acessar um documento e/ou pasta que não possua permissão, deverá solicitar o acesso ao Diretor de Risco e Compliance.

3.7. A Gestora conta atualmente com um backup diário, em que todas as informações disponíveis para acesso no servidor da Gestora ficam disponíveis na nuvem.

3.8. A Gestora: (a) realizará treinamentos de Segurança da Informação para todos os seus Colaboradores, por meio de ferramenta online que possibilita avaliar o conhecimento dos Colaboradores, após cada módulo de treinamento; e (b) periodicamente, com apoio da área de Risco e Compliance, reforçará a importância dos cuidados relacionados à Segurança da Informação, por meio de comunicados internos.

3.9. Ao se utilizar de serviços de processamento, armazenamento de dados e computação em nuvem, a Gestora deverá:

i. verificar se o contrato de prestação de serviços está em conformidade com a legislação e/ou regulamentação em vigor;

ii. avaliar se o prestador de serviço oferece meios de fornecer confidencialidade, integridade, disponibilidade e recuperação de dados para as informações processadas e/ou armazenadas da Gestora;

iii. solicitar aos prestadores acesso aos relatórios (elaborados por empresas de auditoria independentes e especializadas, contratadas pelo provedor de serviços) relacionados aos procedimentos e controles utilizados para fornecer os serviços contratados;

iv. realizar monitoramento e gestão dos recursos dos serviços prestados;

v. avaliar se há a identificação e segregação dos dados da Gestora por meio da utilização de controles físicos e/ou lógicos;

vi. verificar se há qualidade dos controles de acesso para proteger os dados e informações da Gestora;

vii. A contratação de serviços de processamento de dados materiais, armazenamento e computação em nuvem relevantes, fornecidos no exterior, deverá atender aos seguintes requisitos: (a) a Gestora deverá assegurar que a prestação dos serviços não cause danos à operação regular da Instituição, nem constrangimento à atuação de entidades ou dos órgãos reguladores; (b) a Gestora deverá definir, antes da contratação, os países e regiões em cada país onde os serviços podem ser prestados e nos quais os dados podem ser armazenados, processados e gerenciados; e (c) a Gestora deverá estabelecer alternativas para a continuidade do negócio, em caso de impossibilidade de manutenção ou rescisão do contrato de prestação de serviços de processamento, armazenamento de dados e computação em nuvem.

3.10. Os terceiros contratados deverão assinar, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei, caso não esteja previsto no contrato de prestação de serviços cláusula de confidencialidade. Para fins desta Política, os terceiros considerados pela Gestora como relevantes são aqueles que em razão de suas atividades e funções precisam ter controle sobre as informações a que tenham acesso.

4. PROPRIEDADE INTELECTUAL

4.1. A Gestora valoriza a proteção de sua propriedade intelectual e informações confidenciais. Para assegurar práticas éticas, transparentes e seguras em relação aos seus ativos, a Gestora implementa as seguintes diretrizes para todos os Colaboradores:

i. Documentos e Arquivos: Todo material produzido ou utilizado no âmbito das atividades da Gestora — incluindo minutas contratuais, e-mails, planilhas e modelos de avaliação — constitui propriedade exclusiva da Gestora. É vedada ao colaborador a utilização desses arquivos para fins pessoais, inclusive após seu desligamento da empresa. Dessa forma, todos os documentos permanecem sob a posse e a guarda exclusiva da Gestora;

ii. Documentos do Colaborador: Se o colaborador entregar documentos, planilhas ou modelos de avaliação para uso em seu trabalho na Gestora, deverá declarar que: (i) a utilização de tais documentos não infringe contratos ou acordos de confidencialidade anteriores; e (ii) quaisquer alterações realizadas nesses materiais terão como única proprietária a Gestora. O uso dessas versões modificadas pelo colaborador, após seu desligamento, só poderá ocorrer mediante autorização formal da Gestora;

iii. Relevância da Propriedade Intelectual e da Confidencialidade: Essas diretrizes protegem os ativos e informações da Gestora contra uso indevido, vazamento de informações confidenciais e práticas de concorrência desleal, promovendo a ética e a transparência nas relações com colaboradores, clientes e parceiros; e

iv. Compromisso do Colaborador: Ao ingressar na Gestora, o colaborador compromete-se a proteger a propriedade intelectual e a confidencialidade da empresa, utilizando documentos e arquivos de forma ética, responsável e restrita às suas funções profissionais. Em caso de desligamento, é obrigatória a devolução de todos os documentos e materiais da Gestora sob sua guarda, inclusive os produzidos no exercício de suas funções.

5. RESPONSABILIDADES

5.1. É de responsabilidade da Diretoria:

i. Prover a estrutura e os recursos necessários para a implementação da Política e eventuais procedimentos relacionados à Segurança da Informação;

ii. Deliberar sobre questões relacionadas à Segurança da Informação;

iii. Manifestar-se sobre propostas de alterações na Política de Segurança da Informação; e

iv. Supervisionar a implementação e o cumprimento da Política de Segurança da Informação.

5.2. Área de Risco e Compliance deverá:

i. Elaborar, e manter esta Política atualizada, observadas a legislação e a regulamentação aplicáveis;

ii. Propor alterações e manter atualizada esta Política, observadas a legislação e a regulamentação aplicáveis;

iii. Apoiar eventos de fortalecimento da cultura organizacional e da capacitação sobre o tema Segurança da Informação;

iv. Realizar verificações periódicas de segurança para os sistemas de informação, a fim de (a) minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto no Código de Administração de Recursos de Terceiros, na Resolução CVM nº 21 e nesta Política; e (b) garantir que a estrutura tecnológica conte com proteção a tentativas de ataques;

v. Implementar de medidas para sanar as fragilidades relativas ao processo de Segurança da Informação apontadas pela auditoria interna, por auditoria independente e/ou por órgãos de fiscalização e controle;

vi. Realizar comunicação de incidentes relevantes aos órgãos reguladores;

vii. Fomentar eventos de fortalecimento da cultura organizacional e da capacitação sobre o tema Segurança da Informação; e

viii. Manter-se atualizado sobre ameaças, vulnerabilidades relevantes e normas regulatórias aplicadas a Gestora, no que tange à Segurança da Informação.

5.3. Os colaboradores deverão assinar, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei, caso não esteja previsto no contrato de trabalho cláusula de confidencialidade. Ainda, deverão observar o seguinte:

5.3.1. Para autenticação:

i. Não fornecer a sua senha/assinatura eletrônica para outra pessoa;

ii. Certificar-se de não estar sendo observado ao digitar sua senha/assinatura eletrônica;

iii. Alterar a senha/assinatura eletrônica sempre que existir qualquer suspeita do seu comprometimento;

iv. Elaborar senha/assinatura eletrônica de qualidade, de modo que sejam complexas e de difícil adivinhação;

v. Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;

vi. Não usar senha/assinatura eletrônica comuns, como nomes de familiares, datas comemorativas e senhas “camufladas” (p@ssw0rd, s3nh@);

vii. Bloquear sempre o equipamento ao se ausentar; e

viii. Sempre que possível, habilitar um Segundo Fator de Autenticação (Exemplo: SMS, Token etc.).

5.3.2. Para Antivírus e Atualizações:

i. Diariamente, ao final do expediente, o colaborador deverá desligar a sua estação de trabalho (notebook ou desktop), ou reiniciá-la possibilitando que o seu antivírus e sistema operacional estejam sempre atualizados.

ii. Caso seja detectado que uma estação de trabalho esteja muito tempo sem reiniciar, a Gestora poderá forçar essa reinicialização para atualização do antivírus e sistema operacional.

5.3.3. Para trabalho remoto:

i. Nunca conectar o notebook Gestora em redes públicas sem conexão VPN;

ii. Desligar o Bluetooth e a rede Wi-Fi quando não estiverem em uso;

iii. Utilizar os computadores e dispositivos móveis fornecidos pela Gestora apenas para fins profissionais;

iv. Atualizar o nome de usuário e a senha do seu roteador; e

v. Em caso de dúvidas em como configurar o roteador doméstico, entrar em contato com a área de Risco e Compliance da Gestora.

5.3.4. Os colaboradores deverão observar, obrigatoriamente, as seguintes diretrizes relacionadas a tentativas de Engenharia Social:

i. Phishing: é vedado ao colaborador fornecer, por qualquer meio, informações sensíveis, tais como senhas, dados de cartão de crédito, CPF, informações bancárias ou quaisquer credenciais de acesso, em resposta a comunicações eletrônicas não verificadas ou suspeitas, bem como realizar o download ou abertura de arquivos de origem desconhecida;

ii. Links maliciosos: o colaborador não deverá acessar links recebidos por e-mail, mensagens ou quaisquer outros meios quando não for possível atestar, de forma segura, a legitimidade do remetente e do conteúdo. Antes de qualquer acesso, deverá ser verificada a autenticidade do endereço eletrônico, bem como eventuais inconsistências de linguagem ou formatação que indiquem tentativa de fraude;

iii. Falsas mensagens ou contatos telefônicos (vishing/smishing): é vedado ao colaborador compartilhar dados pessoais, credenciais, tokens, códigos de autenticação, IMEI ou quaisquer informações sensíveis em resposta a solicitações realizadas por telefone, mensagens ou outros meios, sem a devida confirmação da identidade do solicitante por canais oficiais; e

iv. Dever de diligência e reporte: o colaborador deverá adotar postura cautelosa e diligente diante de qualquer solicitação de informações sensíveis, devendo, em caso de suspeita de tentativa de fraude ou Engenharia Social, abster-se de qualquer interação e reportar imediatamente o ocorrido à área de Segurança da Informação e/ou Compliance.

6. DAS PENALIDADES

6.1. A violação por parte de qualquer colaborador às restrições impostas por esta política e demais políticas internas da instituição, bem como pela legislação vigente, resultará, conforme o grau de

gravidade, em advertência, revisão das responsabilidades, suspensão ou desligamento, além das penalidades legais aplicáveis.

6.2. As penas aplicadas aos casos concretos serão definidas conjuntamente pelos membros da Diretoria da Gestora, bem como serão comunicadas ao colaborador apenado pelo Diretor de Compliance.

6.3. Caso algum membro da Diretoria viole total ou parcialmente qualquer política interna da instituição, este membro ficará impedido de participar da avaliação pelos demais Diretores da conduta praticada por ele, situação em que o colaborador responsável pela Área de Compliance será convocado para compor extraordinariamente o conclave que avaliará a referida conduta para fins de aplicação, se for o caso, da sanção cabível.

7. VIGÊNCIA E REVISÃO

7.1. Esta Política entra em vigor na data de sua aprovação pela Diretoria da Gestora.

7.2. Esta Política deve ser revisada a cada dois anos, ou extraordinariamente, a qualquer tempo, sempre que mudanças legais, regulamentares ou corporativas demandem alterações.

8. CONTROLE DE VERSÃO

Versão	Data	Versão revogada
1.0	02/05/2024	Não se aplica
1.1	21/01/2026	1.0
1.2	07/04/2026	1.1