Política de Segurança Cibernética

SUMÁRIO

1. OBJETIVO

1.1. Estabelecer diretrizes relacionadas à segurança cibernética, confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados pela Nikos Distribuidora de Títulos e Valores Mobiliários LTDA. (“Nikos”).

2. DEFINIÇÕES

- Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709/2018.

- Banco Central do Brasil (BCB): autarquia federal criada pela Lei nº 4.595/1964, responsável por regular e fiscalizar as instituições financeiras e demais instituições por ela autorizadas a funcionar.

- Cliente: investidor que mantém relacionamento comercial com a Nikos.

- Colaboradores: diretores, funcionários, estagiários, prestadores de serviços terceirizados e quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Nikos, tenham acesso a informações relevantes sobre a empresa, seus clientes, produtos ou estratégias de investimento.

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

- Diretrizes: orientações, instruções para a condução dos negócios e implementação de controles internos.

- Engenharia Social: é um método de ataque utilizado por criminosos virtuais, com base em técnicas de persuasão e/ou investigativas, que exploram a confiança ou a falta de conhecimento das pessoas, e que têm o objetivo de obter dos usuários dados confidenciais e/ou importantes, infectar seus computadores com malware ou abrir links para sites infectados.

- *Exploits*: são programas ou códigos projetados para abusar de vulnerabilidades de *softwares* ou *hardwares* e causar efeitos indesejados pelos desenvolvedores ou fabricantes.

- *Malware*: abreviatura da expressão em inglês “*malicious software*”, que significa "*software* malicioso", e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário e prejudicá-lo de diversas formas.

- Parceiros ou Prestador de serviço relevante: pessoas que realizam acordos comerciais ou associações com a Nikos, mediante contrato firmado pela empresa com ou sem não vínculo empregatício com a Nikos.

- *Ransomware*: é um tipo de malware que restringe o acesso ao sistema ou computador infectado, com uma espécie de bloqueio, e cobra um resgate para que o acesso possa ser restabelecido.

- SaaS: abreviatura da expressão em inglês "*Software as a Service*", é uma forma de disponibilizar softwares e soluções de tecnologia diretamente por meio da internet.

- Segundo Fator de Autenticação: é um recurso que pode ser oferecido por prestadores de serviços que exige que o usuário forneça duas formas de autenticação para confirmar sua identidade (Exemplo: O usuário fornece sua senha e um código enviado para o seu e-mail cadastrado).

- Titular de dados pessoais: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- VPN: abreviatura da expressão em inglês "*Virtual Private Network*", que significa "Rede Virtual Privada".

3. ABRANGÊNCIA

3.1. Esta Política deve ser observada por todos os colaboradores da Nikos.

4. DIRETRIZES

4.1. A Nikos comprometida com a melhoria contínua dos procedimentos relacionados à Segurança da Informação, de modo que os requisitos básicos de confidencialidade, integridade e disponibilidade dos dados e dos sistemas utilizados pela Nikos sejam atingidos por meio da adoção de controles contra ameaças provenientes de fontes externas e internas.

4.2. **No que se refere à gestão de acessos e à autenticação:**

4.2.1. A Nikos 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.

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

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

4.2.4. A Nikos adota controle de acesso lógico, a fim de proteger seus dados, bem como sistemas, programas, redes e dados, 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.

4.2.5. A Nikos utiliza soluções de criptografia seguindo padrões dos órgãos reguladores e as melhores práticas de Segurança da Informação.

4.3. **No que se refere ao tratamento da informação:**

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

4.3.2. A classificação deve seguir os seguintes rótulos (i) confidencial; (ii) interna ou (iii) pública, considerando as necessidades e relevância relacionadas ao negócio.

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

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

4.3.5. 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 (Lei nº 13.709/2018).

4.4. **No que se refere a procedimento de gestão de incidentes de segurança da informação:**

4.4.1. Tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente detectados, registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades competentes.

4.4.2. 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 Nikos.

4.4.3. 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.

4.4.4. Documentar, em formulário próprio, a ocorrência de incidentes relevantes, desde sua detecção até sua resposta, inclusive registros de logs, colaboradores envolvidos e decisões tomadas, de forma a permitir a análise de suas causas e impactos e preservar evidências para futuras auditorias.

4.4.5. Notificar entidades reguladoras e autoridades, inclusive a Autoridade Nacional de Proteção de Dados (ANPD), parceiros comerciais, titulares de dados pessoais, clientes, quando aplicável e desde que não sejam informações protegidas por sigilo, sobre os incidentes que tenham potencial ou comprovado comprometimento de dados dos clientes, parceiros, colaboradores, ou quaisquer titulares de dados pessoais tratados pela Nikos, na forma da legislação e regulamentação vigente, ou em não mais que 48 (quarenta e oito) horas após a conclusão da investigação do evento.

4.5. **No que se refere a procedimento referente à continuidade de negócios:**

4.5.1. Elaborar e manter atualizado um Plano de Continuidade de Negócios (“PCN”), com base em diferentes cenários de incidentes, onde minimamente serão contemplados:

a) a interrupção do acesso físico dos colaboradores à sede da Nikos.

b) falta de energia ou indisponibilidade no Data Center da sede da Nikos.

c) queda dos links de internet na sede da Nikos.

4.5.2. Assegurar a continuidade do negócio por meio da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

4.5.3. Manter *Virtual Private Networks* (VPNs) redundantes para viabilizar o trabalho remoto dos colaboradores em suas residências.

4.5.4. Elaborar testes utilizando o PCN no site de contingência.

4.5.5. Comunicar autoridades e entidades reguladoras, inclusive a Comissão de Valores Mobiliários (CVM), parceiros comerciais, clientes, 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 os casos de interrupção dos processos críticos de negócio da Nikos, na forma da legislação e regulamentação vigente.

4.6. **No que se refere a gestão de vulnerabilidades:**

4.6.1. Periodicamente, realizar varreduras em suas redes internas e externas para identificação de vulnerabilidades conhecidas.

4.6.2. Classificar, tratar e priorizar as vulnerabilidades identificadas, de acordo com o nível de risco apresentado.

4.7. **No que se refere a teste de invasão:**

4.7.1. A Nikos realizará, anualmente, com o auxílio de uma consultoria independente, um Teste de Invasão (*penetration testing*) na infraestrutura da Nikos, com o objetivo de identificar possíveis vulnerabilidades e brechas que possam ser exploradas por usuários maliciosos, bem como tratará, com alta prioridade pela área de Segurança da Informação da Nikos, todas as brechas identificadas no referido teste.

4.7.2. Ademais, as vulnerabilidades identificadas nos testes periódicos, classificadas como alto risco, deverão ser informadas aos testadores para direcionamento do ataque e avaliação da tratativa da vulnerabilidade.

4.8. **No que se refere a proteção contra *malware*, vazamento de dados, *exploit* e *ransomware:***

4.8.1. A Nikos utiliza uma ferramenta líder de mercado para proteção das estações de trabalho e servidores. Além de antivírus, a ferramenta monitora a rede para identificação de padrões suspeitos na utilização de softwares e navegação da internet.

4.8.2. Os alertas emitidos pela ferramenta deverão ser prontamente analisados e tratados pelos responsáveis pela área de Segurança da Informação.

4.8.3. As atualizações de segurança de sistemas operacionais, ferramentas e demais sistemas devem ser prontamente aplicadas, sendo analisadas e distribuídas pela área de Segurança da Informação.

4.9. **No que se refere a gestão de logs e rastreabilidade:**

4.9.1. As trilhas de auditoria deverão ser habilitadas para todos os elementos na infraestrutura de Tecnologia da Informação (TI) da Nikos, que deverão ser armazenadas em ambiente segregado e correlacionadas para monitoramento e auditorias.

4.10. **No que se refere a segurança de rede e segmentação:**

4.10.1. A Nikos manterá a sua rede segmentada e restringirá o acesso direto à internet das estações de trabalho e servidores por meio de *firewall*.

4.10.2. A área de Segurança da Informação é responsável por controlar as regras de firewall e gerir as demandas de alteração do firewall.

4.11. **No que se refere a backups e testes de restauração do ambiente:**

4.11.1. A Nikos possui rotinas automatizadas que realizam backups para recuperação em caso de necessidade.

4.11.2. Periodicamente, são realizados testes de recuperação dos backups para treinamento dos profissionais responsáveis pelo procedimento, bem como para minimizar eventuais problemas em caso de necessidade.

4.12. **No que se refere a armazenamento de dados e computação em nuvem:**

4.12.1. A Nikos, os serviços de processamento, armazenamento de dados e computação em nuvem são oferecidos pela empresa *Oracle Cloud Infraestructure*.

4.12.2. Os controles e procedimentos da (OCI) *Oracle Cloud Infraestructure* relacionados Segurança Cibernética podem ser consultados no link www.oracle.com/br/corporate/security-practices/cloud/.

4.13. **Em relação à disseminação da cultura de Segurança da Informação, a Nikos:**

4.13.1. Realizará, com periodicidade mínima anual, treinamentos obrigatórios de Segurança da Informação para todos os seus colaboradores, por meio de ferramenta contratada, contemplando, não apenas a avaliação de conhecimentos, mas também a capacitação prática e teórica por meio de conteúdos didáticos e exercícios práticos em cada módulo.

4.13.2. Realizará, anualmente, testes de *phishing* para mensurar a qualidade e a absorção da cultura de Segurança da Informação por parte de seus colaboradores.

4.13.3. Periodicamente, reforçará a importância dos cuidados relacionados à Segurança da Informação, por meio de comunicados internos.

5. RECOMENDAÇÕES AOS CLIENTES

5.1. A Nikos realiza as seguintes recomendações aos seus clientes para a devida autenticação:

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

b) Certificar-se de não estar sendo observado ao digitar a sua senha/assinatura eletrônica;

c) Alterar a senha/assinatura eletrônica sempre que existir qualquer suspeita do seu comprometimento;

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

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

f) Evitar o uso de senhas/assinaturas eletrônicas comuns, como nomes de familiares, datas comemorativas e senhas “camufladas” (p@ssw0rd, s3nh@);

g) Bloquear sempre o equipamento ao se ausentar;

h) Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Google *Authenticator, Smart Card*, *Token* etc.);

i) Manter a sua conta de e-mail utilizada para cadastro da conta Nikos segura; e

j) Aplicar as recomendações de senha e, primordialmente, utilizar o duplo fator de autenticação.

5.2. A Nikos realiza recomenda manter uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pela Nikos, e manter o sistema operacional sempre atualizado.

6. CUIDADOS RELACIONADOS A ENGENHARIA SOCIAL

6.1. A Engenharia Social, no contexto de Segurança da Informação, refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança do usuário, com o objetivo de ludibriar, aplicar golpes ou obter informações sigilosas.

6.2. As falsas mensagens ou contato telefônico é uma técnica utilizada pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI), ou qualquer outro tipo de informação para a prática da fraude. Para evitá-lo:

a) não forneça seus dados antes de confirmar a veracidade do número por onde recebeu solicitações; e

b) não compartilhe códigos recebidos via SMS e não clique em nenhum link fornecido.

6.3. O *Phishing* também é uma das técnicas mais utilizadas por criminosos virtuais para enganar os usuários, através do envio de e-mails maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias e envio de arquivos infectados. Para evitá-lo:

a) não clique em *links* que não sejam legítimos. O fraudador se utiliza de disfarces para a vítima acreditar que o *link* é verdadeiro; e

b) verifique sempre se a ortografia e gramática estão corretas e se o endereço de e-mail do remetente é aparentemente legítimo, ou se ele(a) está tentando se passar por alguém conhecido.

6.4. Os exemplos elencados acima não são exaustivos. Em caso de dúvida da veracidade de qualquer comunicação recebida, contate imediatamente a Nikos por meio dos seus canais de atendimento disponibilizados em seu site (www.nikos.com.br).

6.5. Destaca-se que a Nikos não envia mensagens aos seus clientes solicitando informações pessoais ou transferência de valores para sua conta.

7. CANAL DE DENÚNCIAS

7.1. A Nikos disponibiliza um Canal de Denúncias em sua página na internet onde os clientes podem reportar situações com indícios de ilicitude, de qualquer natureza, relacionadas à Segurança Cibernética.

8. REVISÃO

8.1. Está Política deve ser revisada anualmente, ou extraordinariamente, a qualquer tempo, sempre que mudanças legais, regulamentares ou corporativas demandem alterações.

9. VIGÊNCIA

17.1. Esta Política entrará em vigor na data de sua aprovação pela Diretoria da Nikos.

10. CONTROLE DE VERSÕES

Versão	Data	Versão revogada
1.0	02/05/2024	Não se aplica
1.1	01/10/2024	1.0
1.2	04/08/2025	1.1
1.3	31/03/2026	1.2