Política De Segurança Cibernética

1. OBJETIVO

1.1. A NILCO DTVM LTDA. ("Nikos") está 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.

2. DISPOSIÇÕES GERAIS

2.1. Acesso à Informação e Criptografia

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

2.1.1.1. 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.

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

2.1.1.3. 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.

2.1.1.4. A Nikos adota controle de acesso lógico no ambiente dos clientes, 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.

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

2.2. No que se refere ao tratamento da informação:

2.2.1. 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.

2.2.2. A classificação das informações deve seguir os seguintes rótulos: Confidencial, Interna ou Pública, considerando as necessidades relacionadas ao negócio.

2.2.3. 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.

2.2.4. 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.

2.2.5. 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).

3. **PROCEDIMENTO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

3.1. A Nikos deverá:

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

3.1.5. 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. **PROCEDIMENTO REFERENTE À CONTINUIDADE DE NEGÓCIOS**

4.1. A Nikos deverá:

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

- A interrupção do acesso físico dos colaboradores à sede da Nikos.
- Falta de energia ou indisponibilidade no Data Center da sede da Nikos.
- Queda dos links de internet na sede da Nikos.
- Assegurar a continuidade do negócio por meio da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.
- Manter Virtual Private Networks (VPNs) redundantes para viabilizar o trabalho remoto dos colaboradores em suas residências.
- Realizar testes utilizando o PCN no site de contingência.
- 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.

5. GESTÃO DE VULNERABILIDADES

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

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

6. TESTE DE INVASÃO

6.1. 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.

6.2. Tratará, com alta prioridade pela área de Segurança da Informação da Nikos, todas as brechas identificadas no referido teste.

6.3. 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.

6.4. Em relação à proteção contra malware, vazamento de dados, exploits e ransomware:

6.5. 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.

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

6.7. 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.

6.8. Em relação à gestão de logs e rastreabilidade:

6.9. 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.

7. No que se refere à segurança de rede e à segmentação, a Nikos deverá:

7.1. Manter sua rede segmentada e restringir o acesso direto à internet das estações de trabalho e servidores por meio de firewall. A área de Segurança da Informação é responsável por controlar as regras de firewall e gerir as demandas de alteração do firewall.

8. Em relação à gestão de backups e aos testes de restauração de ambiente:

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

8.2. 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.

8.3. No que se refere ao processamento, armazenamento de dados e computação em nuvem:

8.4. Na Nikos, os serviços de processamento, armazenamento de dados e computação em nuvem são oferecidos pela empresa Amazon Web Services (AWS) e Oracle Cloud Infraestructure.

8.5. Os controles e procedimentos da Amazon Web Services (AWS) relacionados à Segurança Cibernética podem ser consultados no link:

https://d1.awsstatic.com/whitepapers/compliance/PT_Whitepapers/AWS_User_Guide_for_Financial_Services_in_Brazil.pdf.

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

9. RECOMENDAÇÕES AOS CLIENTES

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

- Não fornecer a sua senha/assinatura eletrônica para outra pessoa.
- Certificar-se de não estar sendo observado ao digitar a sua senha/assinatura eletrônica.
- Alterar a senha/assinatura eletrônica sempre que existir qualquer suspeita do seu comprometimento.
- Elaborar senha/assinatura eletrônica de qualidade, de modo que sejam complexas e de difícil adivinhação.
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação.
- Evitar o uso de senhas/assinaturas eletrônicas comuns, como nomes de familiares, datas comemorativas e senhas “camufladas” (p@ssw0rd, s3nh@).
- Bloquear sempre o equipamento ao se ausentar.
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Google Authenticator, Smart Card, Token etc.).
- Manter a sua conta de e-mail utilizada para cadastro da conta Nikos segura. Aplicar as recomendações de senha e, primordialmente, utilizar o duplo fator de autenticação.

9.2. A Nikos realiza as seguintes recomendações aos seus clientes sobre o uso de antivírus e atualizações necessárias:

9.3. 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.

9.4. A Nikos realiza os seguintes alertas e recomendações aos seus clientes para evitar que eles sejam persuadidos por criminosos virtuais, por meio da Engenharia Social:

9.4.1. 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.

9.4.2. Abaixo, seguem outras técnicas utilizadas pelos criminosos virtuais e os cuidados que devem ser adotados pelos clientes:

- Phishing: Técnica utilizada 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.
- Não clicar em links que não sejam legítimos, pois o fraudador utiliza disfarces para a vítima acreditar que o link é verdadeiro. Verificar sempre se a ortografia e a 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.

- 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.

9.5. A Nikos informa que não envia mensagens aos seus clientes solicitando informações pessoais ou transferência de valores para sua conta. Em caso de dúvidas, favor entrar em contato pelos canais de atendimento oficiais da Instituição.

10. CANAL DE DENÚNCIAS

10.1. 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.

11. DISPOSIÇÕES FINAIS

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

Versão	Data	Última Alteração
1.0	02/05/2024	Não se aplica