# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**ÍNDICE**

## 1. OBJETIVO

1.1. Estabelecer diretrizes relacionadas à segurança cibernética, confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados pela NILCO GESTÃO DE RECURSOS LTDA. (“NILCO”).

1.2. Orientar quanto à adoção de controles e procedimentos para atendimento aos requisitos de Segurança da Informação.

1.3. Prevenir, detectar, reduzir e remediar possíveis incidentes de segurança da informação.

1.4. Minimizar os riscos de perdas financeiras, de imagem ou qualquer outro impacto negativo nos negócios da NILCO, que possam resultar de falhas de Segurança da Informação.

## 2. ABRANGÊNCIA

2.1. Esta Política deve ser observada por todos os colaboradores da NILCO, bem como pelos demais prepostos e prestadores de serviços da NILCO.

## 3. ÁREAS GESTORAS

3.1. Compliance e Segurança da Informação.

## 4. 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 NILCO.
- **Colaboradores**: diretores, funcionários, estagiários, prestadores de serviços terceirizados e quaisquer pessoas que, em virtude de seus cargos, funções ou posições na NILCO, tenham acesso a informações relevantes sobre a empresa, seus clientes, produtos ou estratégias de investimento.
- **Comissão de Valores Mobiliários (CVM)**: autarquia federal criada pela Lei nº 6.385/1976, responsável por regular e fiscalizar o mercado de valores mobiliários.
- **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**: pessoas que realizam acordos comerciais ou associações com a NILCO.
- **Prestador de serviço terceirizado**: pessoa que trabalha na NILCO, mediante contrato firmado pela empresa, com pessoa jurídica prestadora de serviços. O prestador de serviço terceirizado não tem vínculo empregatício com a NILCO, mas sim com a empresa prestadora de serviços, que é a responsável por sua contratação e remuneração.
- **Princípios**: valores que direcionam e orientam a atuação da empresa.
- ***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".

## 5. DIRETRIZES

### 5.1. Acesso à Informação e Criptografia

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

5.1.1.1. A NILCO 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.

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

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

5.1.1.4. A NILCO adota controle de acesso lógico no ambiente dos clientes, a fim de proteger seus dados, bem como sistemas, programas, redes e dados da NILCO, 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.

5.1.1.5. Todas as contas usadas para acessar a rede da NILCO por meio de uma *Virtual Private Network* (VPN), necessariamente devem possuir o Segundo Fator de Autenticação.

5.1.1.6. Contas privilegiadas da infraestrutura de Tecnologia da Informação (TI) da NILCO precisam ter o Segundo Fator de Autenticação habilitado. Entende-se por contas privilegiadas:

- Administradores e Operadores de Domínio;

- Administradores de Console de ambientes de infraestrutura de nuvem;
- Administradores dos Servidores de Produção;
- Administradores de *Firewall*;
- Acesso a ferramenta de suporte remoto.

5.1.1.7. Contas de Sistemas SaaS, obrigatoriamente, precisam ter o Segundo Fator de Autenticação habilitado. A NILCO utiliza-se de soluções de criptografia seguindo padrões dos órgãos reguladores e as melhores práticas de Segurança da Informação.

5.1.1.8. A NILCO implementa rigorosas regras de acesso às informações confidenciais, reservadas ou privilegiadas. O acesso a essas informações é estritamente controlado e concedido apenas a colaboradores autorizados, de acordo com suas funções laborais específicas. O processo de concessão de acesso é formalizado e auditável, visando garantir a transparência e a conformidade com as políticas de segurança da informação da NILCO.

5.1.1.9. Em casos de desligamento do profissional, a NILCO adota procedimentos específicos para garantir a revogação imediata dos acessos do colaborador às informações confidenciais. Esses processos incluem a revisão e atualização periódica dos privilégios de acesso, a desativação rápida de contas de usuário e a implementação de medidas de segurança adicionais, se necessário.

5.1.1.10. Em casos de mudança de atividade dentro da instituição, a NILCO implementa um protocolo detalhado para assegurar a transição segura dos acessos às informações confidenciais. Antes da realocação de um colaborador para uma nova função, a área de segurança realiza uma revisão minuciosa das permissões associadas à sua conta. Qualquer ajuste necessário nos privilégios de acesso é realizado de acordo com as exigências específicas da nova função, garantindo que o colaborador mantenha apenas as permissões estritamente necessárias para o desempenho de suas novas responsabilidades.

5.1.1.11. A NILCO estabelecerá a exigência de que todos os seus profissionais assinem, de forma eletrônica, termo de confidencialidade referente às informações que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais. Essa medida visa reforçar a responsabilidade individual dos colaboradores na preservação da confidencialidade das informações da empresa. Importante ressaltar que, salvo nas hipóteses permitidas em lei, o compromisso de confidencialidade será abrangente, assegurando que todas as informações sensíveis sejam tratadas com a devida cautela e proteção. Essa prática fortalece a cultura organizacional de segurança da informação na NILCO, mitigando riscos internos e contribuindo para a manutenção da integridade e confidencialidade dos dados sob sua responsabilidade.

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

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

5.2.1.1. A classificação deve seguir os seguintes rótulos: Confidencial, Interna ou Pública, considerando as necessidades e relevância relacionadas ao negócio.

5.2.1.2. 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 NILCO, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações.

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

5.2.1.4. 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).

5.3. **No que se refere à gestão de incidentes de segurança da informação, a NILCO deverá:**

5.3.1. 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 Superintendência de Relações com o Mercado e Intermediários (SMI), órgão da Comissão de Valores Mobiliários (CVM) e à Diretoria da NILCO, conforme aplicável.

5.3.2. 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 NILCO.

5.3.3. 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.

5.3.4. 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 NILCO, na forma da legislação e regulamentação vigente, ou em não mais que 48 (quarenta e oito) horas após a conclusão da investigação do evento.

5.3.5. No que tange ao tratamento de vazamento de informações confidenciais, reservadas ou privilegiadas, a NILCO deverá adotar medidas rigorosas para lidar com tais incidentes, mesmo que provenham de ações involuntárias. Essas medidas devem incluir a pronta identificação da origem do vazamento, a implementação imediata de ações corretivas, e a comunicação rápida e eficaz às partes envolvidas, incluindo autoridades competentes e entidades reguladoras. A NILCO deve estabelecer protocolos específicos para lidar com a

exposição de informações sensíveis, garantindo a proteção da integridade e confidencialidade dos dados, bem como a mitigação dos impactos sobre os titulares de dados afetados. Essa abordagem proativa assegura a conformidade com as normas legais e regulatórias, preservando a reputação da empresa diante de seus clientes, parceiros e autoridades competentes.

5.4. **No que se refere à continuidade de negócios, a NILCO deverá:**

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

5.4.1.1. A interrupção do acesso físico dos colaboradores à sede da NILCO.

5.4.1.2. Falta de energia ou indisponibilidade no *Data Center* da sede da NILCO.

5.4.1.3. Queda dos *links* de internet na sede da NILCO.

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

5.4.3. Manter VPNs redundantes para viabilizar o trabalho remoto dos colaboradores em suas residências.

5.4.4. Realizar testes utilizando o PCN no site de contingência.

5.4.5. Comunicar autoridades e entidades reguladoras, inclusive a 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 NILCO, na forma da legislação e regulamentação vigente.

5.5. **No que se refere à gestão de vulnerabilidades, a NILCO deverá:**

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

5.5.2. As vulnerabilidades devem ser classificadas, tratadas e priorizadas, de acordo com o nível de risco apresentado.

5.6. **No que se refere ao Teste de Invasão, a NILCO:**

5.6.1. Realizará, anualmente, com o auxílio de uma consultoria independente, Teste de Invasão (*penetration testing*) na infraestrutura da NILCO, com o objetivo de identificar possíveis vulnerabilidades e brechas que possam ser exploradas por usuários maliciosos.

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

5.6.3. 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.

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

5.7.1. A NILCO utiliza uma ferramenta líder de mercado para proteção das estações de trabalho e servidores contra *malware*, vazamento de dados, *exploits* e *ransomware.* Além de antivírus, a ferramenta monitora a rede para identificação de padrões suspeitos na utilização de *softwares* e navegação da internet.

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

5.7.3. 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.

5.7.4. A ferramenta de proteção das estações de trabalho e servidores deve possuir módulo de DLP (*Data Prevention Loss*), com regras definidas para bloqueio e alertas para tentativas de envio de arquivos contendo dados de uso interno, confidenciais e informações pessoais para fora da rede da NILCO, ou dispositivos de armazenamento.

5.7.5. A NILCO deve configurar regras para bloqueio e alertas em tentativas de envio de arquivos contendo dados de uso interno, confidenciais e informações pessoais em *drivers* de compartilhamento online.

5.8. **Em relação à gestão de *logs* e rastreabilidade:**

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

5.9. **No que se refere à segurança de rede e à segmentação, a NILCO deverá:**

5.9.1. 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*.

5.9.2. A NILCO possui implementada em seus *firewalls* sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS).

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

5.10.1. Todos os *backups* deverão ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de *backup*", ou seja, nos períodos em que não há acesso, ou há pouco acesso de usuários ou processos automatizados aos sistemas de informática.

5.10.2. Na situação de erro de *backup* e/ou *restore*, será necessário que seja feito no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. A NILCO possui rotinas automatizadas que realizam *backups* para recuperação em caso de necessidade.

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

5.11. **Em relação à disseminação da cultura de Segurança da Informação, a NILCO:**

5.11.1. Realizará, com periodicidade mínima anual, treinamentos de Segurança da Informação para todos os seus colaboradores, por meio de ferramenta online que possibilita avaliar o conhecimento dos colaboradores, após cada modulo de treinamento.

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

5.11.2. Periodicamente, com apoio da área de Comunicação Interna, reforçará a importância dos cuidados relacionados à Segurança da Informação, por meio de comunicados internos.

5.12. **No que se refere ao desenvolvimento seguro, a NILCO:**

5.12.1. Anualmente, disponibilizará treinamentos para a sua área de Desenvolvimento, que focam no *Open Web Application Security Project* (*OWASP)* top 10, reunindo as melhores práticas de mercado para contornar as vulnerabilidades mais exploradas por criminosos virtuais.

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

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

5.13.1.1. Verificar se o contrato de prestação de serviços está em conformidade com a legislação e/ou regulamentação em vigor.

5.13.1.2. 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 NILCO.

5.13.1.3. 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.

5.13.1.4. Realizar monitoramento e gestão dos recursos dos serviços prestados.

5.13.1.5. Avaliar se há a identificação e segregação dos dados da NILCO por meio da utilização de controles físicos e/ou lógicos.

5.13.1.6. Verificar se há qualidade dos controles de acesso para proteger os dados e informações da NILCO.

5.13.2. A contratação de serviços de processamento de dados materiais, armazenamento e computação em nuvem relevantes, fornecidos no exterior, deverá atender aos seguintes requisitos:

5.13.2.1. A NILCO 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.

5.13.2.2. A NILCO 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.

5.13.3. A NILCO 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.

5.14. **Sobre contratação de serviços terceirizados relevantes:**

5.14.1. A NILCO somente contratará serviços relevantes prestados por terceiros que possam demonstrar um compromisso com a segurança de informações, por meio de certificações como ISO 27001, SOC 2, PCI DSS e equivalentes, a ser avaliado pela área de Segurança da Informação.

5.14.2. Exigir que os provedores de serviço terceirizado assinem um acordo de confidencialidade e sigam as políticas e padrões de segurança de informações da NILCO.

5.14.3. Revisar e avaliar regularmente os controles de segurança do provedor de serviços terceirizados, para garantir que eles permaneçam efetivos e que o provedor esteja cumprindo as obrigações previstas no acordo de confidencialidade.

5.14.4. Qualquer exceção ao item 5.14.1 deve ser documentado e aprovado pela Diretoria em caso de efetivação da contratação.

5.15. **No que se refere aos procedimentos relacionados a monitoramento dos seus clientes e prevenção de fraudes, a NILCO:**

5.15.1. Coleta, verifica e valida as informações cadastrais de seus clientes e mantêm atualizadas.

5.15.2.

5.15.3.

5.15.4. Recomenda aos seus clientes, através do Portal, evitar a utilização de VPNs gratuitas ou de navegação anônima, ou redes Peer-to-Peer (P2P) com intuito de mascarar a origem dos acessos.

5.15.5. A gerência da área de Segurança da Informação deve fornecer meios e recursos para que a equipe participe de fóruns de discussão e eventos de segurança da informação e tecnologia, onde são compartilhadas informações sobre ameaças e vulnerabilidades relevantes, de maneira a se manterem atualizados.

5.16.

## 6. SEGREGAÇÃO DA ATIVIDADE DE ADMINISTRAÇÃO DE CARTEIRAS DE VALORES MOBILIÁRIOS

6.1. Conforme disposto na Resolução CVM n 21/21, o exercício da atividade de administração de carteiras de valores mobiliários será segregado de eventuais atividades que a NILCO venha a exercer, mesmo que possua apenas um conflito de interesses potencial ou eventual.

6.2. A referida segregação ocorrerá por meio de controles de separação física e tecnologia.

6.3. Os acessos tecnológicos seguem as regras descritas nesta política, sempre com a autorização do líder da área solicitante e o responsável pela área de Segurança da Informação.

6.4. Para garantir a segregação, não haverá compartilhamento, mesmo que parcial, temporário ou excepcional de nenhuma estrutura, equipe, sistemas ou arquivos. Ainda, as linhas de reporte também são segregadas.

## 7. RESPONSABILIDADES

7.1. **Diretoria:**

a) designar perante a CVM o diretor responsável por Segurança da Informação e pelo PCN;

b) aprovar:

i. a Política de Segurança da Informação; e

ii.

o PCN;

c) definir a área responsável por Segurança da Informação;

d) prover a estrutura e os recursos necessários para a implementação da Política e eventuais procedimentos relacionados à Segurança da Informação;

e) analisar e aprovar o Relatório de Implementação do Plano de Ação e de Resposta a Incidentes de Segurança da Informação.

f) deliberar sobre questões relacionadas à Segurança da Informação, que lhe forem apresentadas pelo Diretor responsável pelo tema.

7.2. **Diretor responsável por Segurança da Informação:**

a) manifestar-se sobre propostas de alterações na Política de Segurança da Informação a ser submetida à apreciação da Diretoria;

b) supervisionar a implementação e o cumprimento da Política de Segurança da Informação;

c) subscrever e encaminhar à apreciação da Diretoria o Relatório de Implementação do Plano de Ação e de Resposta a Incidentes de Segurança da Informação.

7.3. **Área de Compliance:**

a) propor alterações e manter atualizados a Política de Segurança da Informação, observadas a legislação e a regulamentação aplicáveis;

b) apoiar eventos de fortalecimento da cultura organizacional e da capacitação sobre o tema Segurança da Informação;

c) coordenar e monitorar a implementação de medidas para sanar as fragilidades relativas ao processo de Segurança da Informação apontadas pela auditoria interna, por auditoria independente e por órgãos de fiscalização e controle;

d) apoiar à área de Segurança da Informação na elaboração do Relatório de Implementação do Plano de Ação e de Resposta a Incidentes de Segurança da Informação, e encaminhá-lo ao Diretor responsável pelo tema para apreciação.

e) Realizar comunicação de incidentes relevantes aos órgãos reguladores.

7.4. **Área de Segurança da Informação:**

a) elaborar a Política de Segurança da Informação, com suporte da Área de Compliance, observadas a legislação e a regulamentação aplicáveis;

b) fomentar eventos de fortalecimento da cultura organizacional e da capacitação sobre o tema Segurança da Informação;

c) implementar medidas para sanar as fragilidades relativas ao processo de Segurança da Informação apontadas pela auditoria interna, por auditoria independente e por órgãos de fiscalização e controle;

d) elaborar o Relatório de Implementação do Plano de Ação e de Resposta a Incidentes de Segurança da Informação.

e) classificação da relevância dos incidentes de acordo com os critérios estabelecidos em documento próprio.

f) manter-se atualizado sobre ameaças, vulnerabilidades relevantes e normas regulatórias aplicadas a NILCO, no que tange a Segurança da Informação.

7.5. **Área de Customer Experience**

a) Comunicação de incidentes relevantes aos clientes afetados de acordo com os critérios estabelecidos em documento próprio.

7.6. **Responsabilidades comuns a todos os Colaboradores:**

7.6.1. Para 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) Não usar senha/assinatura eletrônica 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 (Exemplo: SMS, Token, etc.).

7.6.2. Para antivírus e atualizações

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

b) Caso seja detectado que uma estação de trabalho esteja muito tempo sem reiniciar, a área de Segurança da Informação poderá forçar essa reinicialização para atualização do antivírus e sistema operacional.

7.6.3. Para trabalho remoto

a) Nunca se conectar em redes públicas com o seu notebook NILCO sem conexão VPN.

b) Desligar o *Bluetooth* e a rede *Wi-Fi* quando não estiverem em uso. Os criminosos virtuais podem detectar as redes já conectadas e criar redes falsas com o mesmo nome (depois disso, o seu dispositivo se conecta automaticamente).

c) Utilizar os computadores e dispositivos móveis fornecidos pela NILCO apenas para fins profissionais.

d) Atualizar o nome de usuário e a senha do seu roteador. A maioria dos roteadores vem com credenciais de login padrão que são de conhecimento público, o que significa que qualquer pessoa dentro de seu alcance pode se conectar e alterar suas configurações. É muito importante proteger sua rede com uma senha forte e exclusiva.

e) Em caso de dúvidas em como configurar o roteador doméstico, entrar em contato com a área de Segurança da Informação da NILCO.

f) Trabalhar fora do escritório não isenta o colaborador de cumprir a Política de Segurança da Informação da NILCO. Essa política foi elaborada para evitar violações de dados e manter a privacidade de todos os colaboradores, clientes e parceiros de negócios. Caso necessário, entre em contato com seu superior para garantir que tenha todos os recursos necessários para trabalhar com segurança em sua residência.

7.6.4. Cuidados relacionados a Engenharia Social

a) 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, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

b) Técnicas mais utilizadas:

i. *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.

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

iii. 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.

## 8. SANÇÕES

8.1. As violações relacionadas a esta Política, bem como para as demais normas e procedimentos de segurança da NILCO, serão passíveis de penalidades.

8.2. As sanções serão aplicadas de acordo com o disposto nos normativos internos, e considerando a gravidade da infração cometida.

8.3. No caso de terceiros contratados ou prestadores de serviço, a sanção será aplicada de acordo com os termos previstos em contrato.

8.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em danos à NILCO, o infrator será responsabilizado pelos danos causados, cabendo aplicação das medidas judiciais pertinentes, sem prejuízo do disposto nos itens 8.1, 8.2 e 8.3 desta Política.

## 9. REVISÃO

9.1. Esta Política deve ser revisada, no mínimo, anualmente, ou, a qualquer tempo, sempre que mudanças legais, regulamentares ou corporativas demandarem alterações.

## 10. CASOS OMISSOS

10.1. Os casos omissos serão avaliados pela Diretoria da NILCO.

10.2. As diretrizes estabelecidas nesta Política e nas demais normas e/ou procedimentos de Segurança da Informação, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, é obrigação do colaborador da NILCO adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da NILCO e dos nossos clientes.

## 11. VIGÊNCIA

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

## 12. CONTROLE DE VERSÃO

| Versão | Data da aprovação pela Diretoria | Versão revogada |
|---|---|---|
| **1.0** | 28/11/2023 | Não se aplica |