1 OBJETIVO

A Política de Segurança da Informação ("Política" ou "PSI") visa a estabelecer diretrizes, princípios e responsabilidades, além de orientar na execução das ações relacionadas ao tratamento das informações e ao uso adequado de ativos e/ou informações pelo público-alvo, a fim de mitigar eventuais riscos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar as informações da NiO quanto à sua integridade, confidencialidade e disponibilidade.

2 PÚBLICO-ALVO

Esta PSI é aplicável a toda NiO, contemplando todo uso de dispositivos, acesso a servidores, conexões à rede e à internet e quaisquer outros usos de recursos tecnológicos ou que contenham informações da NiO. Deve, portanto, ser cumprida e aplicada em todas as áreas da Companhia, inclusive por todas as pessoas físicas ou jurídicas, sejam sócios, diretores, administradores, funcionários, menores aprendizes e estagiários ("Colaboradores Internos"), bem como prestadores de serviços, terceiros, fornecedores e parceiros da Companhia ("Colaboradores Externos") que, no âmbito de sua relação com a NiO, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da Companhia. Para fins de interpretação da presente Política, Colaboradores Internos e Colaboradores Externos serão denominados em conjunto simplesmente "Colaboradores".

3 DIRETRIZES

Informação é Patrimônio: toda informação e qualquer dado ou ativo gerados, adquiridos, manuseados, armazenados, sob a guarda, transportados e/ou descartados pelos Colaboradores nas dependências e/ou em ativos da Companhia, em virtude de seu vínculo com a NiO ou do desempenho de suas atividades contratadas pela Companhia ("Informação Protegida"), são considerados patrimônio da NiO e devem ser utilizados exclusivamente para os interesses corporativos. A NiO dispõe de uma Política de Classificação de Dados voltada aos Colaboradores Internos e um Manual de Privacidade e Proteção de Dados Pessoais para Terceiros voltado aos Colaboradores Externos, que estabelecem regras e obrigações específicas sobre o uso das Informações Protegidas, aplicando-se em complemento a esta PSI.

A responsabilidade e o comprometimento deve ser de todos: todos os Colaboradores são responsáveis pela proteção e salvaguarda das Informações Protegidas, assim como dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas. O uso aceitável da infraestrutura de redes e serviços da Companhia é sempre ético, honesto, e respeita os direitos individuais, inclusive os direitos à privacidade e proteção de dados.

O acesso à informação deve ser gerenciado: o acesso lógico, o controle de acesso físico e o uso da informação serão aprovados, controlados, registrados, armazenados e monitorados, de forma a adequar a Segurança da Informação com a execução das tarefas inerentes ao seu cargo ou função.

Incidentes de segurança precisam ser prevenidos ou combatidos: os incidentes de Segurança da Informação, quando não puderem ser prevenidos, devem ser identificados, monitorados, comunicados e devidamente combatidos de forma a reduzir riscos no ambiente, evitando interrupção das atividades, e não afetar o alcance dos objetivos estratégicos da Companhia e atendimento dos seus clientes.

Os ativos da NiO e sua utilização podem ser monitorados: a Companhia pode, nos limites da lei aplicável e conforme necessário, monitorar, gravar e registrar o acesso e a utilização de seus ativos tecnológicos, bem como dos ambientes, serviços, equipamentos e sistemas da informação, incluindo, mas não se limitando a e-mails, arquivos, impressões, histórico de navegação e, no geral, redes e computadores, de forma que ações indesejáveis ou não autorizadas sejam detectadas.

A NiO pode auditar a conformidade com as práticas de segurança: a Companhia pode auditar periodicamente sem aviso prévio, as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus Colaboradores em relação ao estabelecido nesta Política, nas demais diretrizes que a compõem e na legislação aplicável, inclusive por meio das práticas de monitoramento mencionadas nesta PSI.

3.1 Princípios de Segurança da Informação

São as ações ou linhas de conduta de segurança que atuam como guia para a sua implementação e a gestão da Segurança da Informação:

Estabelecer a Segurança da Informação em toda a NiO: a Segurança da Informação é tratada em nível organizacional, de acordo com a tomada de decisões que levem em consideração todos os processos críticos de negócio da NiO.

Adotar uma abordagem baseada em riscos: a Segurança da Informação é fundamentada em decisões baseadas em riscos como perda da vantagem competitiva, conformidade, responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras, uso indevido, fraudes, sabotagens, roubo e ataques cibernéticos.

Promover um ambiente positivo de segurança: a Segurança da Informação é estruturada com base na análise do comportamento humano, observando as crescentes necessidades de todas as partes interessadas, através da conscientização, educação e maturidade do capital humano, fortalecendo um dos elementos fundamentais para manter o nível apropriado de Segurança da Informação.

3.2 Privacidade e Proteção de Dados Pessoais

Esta PSI aplica-se a dados, incluindo dados pessoais e dados pessoais sensíveis, sobre os Colaboradores, clientes, clientes finais e prestadores de serviços relacionados à NiO. É vedado, sem a prévia autorização da NiO, o uso desses dados para finalidades diversas das que lastrearam a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados, nos termos desta PSI e das demais política referentes à privacidade e proteção de dados pessoais.

A NiO usa provedores de serviços externos. Se os dados que estão sendo processados são pessoais, firmamos acordos contratuais apropriados e medidas organizacionais são implementadas de acordo com a legislação aplicável para assegurar a proteção dos dados.

O Colaborador garante que todos os dados pessoais a que tiver acesso não serão divulgados ou compartilhados sem autorização expressa da Companhia, bem como não serão transmitidos ou acessados por terceiros não autorizados. O Colaborador garante, ainda, que adotará as melhores práticas de Segurança da Informação durante todo o ciclo de vida dos dados dentro da NiO, não se limitando apenas àquelas descritas nesta PSI.

3.3 Monitoramento e Auditoria do Ambiente

Todo ambiente físico e digital da NiO é ou poderá ser monitorado, respeitados os limites previstos na legislação vigente, incluindo o acesso, uso ou tráfego de informações em tal ambiente por qualquer meio (tal qual, por exemplo, e-mail) com o objetivo de apurar o cumprimento das normas de segurança e proteção de dados da Companhia.

Os Colaboradores estão cientes de que a NiO poderá:

- Monitorar todos os servidores, redes, conexões de internet, software, equipamentos e dispositivos corporativos, móveis ou não, conectados à rede corporativa;
- Realizar inspeções físicas nos equipamentos e nas estações de trabalho do colaborador, periodicamente ou sob fundada suspeita de infração às normas internas da Companhia.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica da NiO e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do monitoramento são guardadas nos backups da Companhia para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela NiO ou pela legislação em vigor. Caso solicitado pelos órgãos competentes, essas informações poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O Colaborador entende que o monitoramento é realizado para resguardar a segurança não só dos sistemas da Companhia e das Informações Protegidas, como também do próprio Colaborador. Os dados e as informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas, como a apuração de denúncias e condução de investigações no ambiente laboral. Todo e qualquer tratamento de dados para esses fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto e cumprirá as normas específicas sobre privacidade e proteção de dados pessoais.

3.4 Manuseio das Informações Protegidas

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de Segurança da Informação.

3.4.1 Cuidados com Impressoras e Copiadoras

Os Colaboradores estão cientes de que todo e qualquer uso dos equipamentos, como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado o uso para fins pessoais. Deve-se evitar imprimir documentos contendo certos tipos de Informações Protegidas, sendo certo que o Colaborador Interno deverá seguir as diretrizes da Política de Classificação de Dados e o Colaborador Externo deverá seguir as diretrizes do Manual de Privacidade e Proteção de Dados Pessoais para Terceiros. Qualquer tipo de documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos.

3.4.2 Uso de Informações Protegidas

O Colaborador deve tomar o máximo de cuidado com o uso que faz das Informações Protegidas, atentando-se para não deixar anotações ou manipular documentos que contenham Informações Protegidas em locais de circulação, como salas de reunião ou espaços públicos, como cafés e aviões. É proibida a reutilização de papéis para rascunho que contenham Informações Protegidas.

Nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade de compartilhamento de Informações Protegidas, estas somente poderão ser compartilhadas após a assinatura de acordo de confidencialidade ou de outros instrumentos contratuais pertinentes firmados com tais terceiros.

3.4.3 Recebimento, Envio e Compartilhamento de Arquivos

O Colaborador é responsável pelos arquivos que recebe, envia e compartilha por meio eletrônico e pela infraestrutura tecnológica da Companhia, seja equipamentos de propriedade da Companhia disponibilizados para o uso do Colaborador, equipamentos do próprio Colaborador, ou ainda, serviços de *cloud* (nuvem).

Para garantir níveis mínimos de segurança da infraestrutura tecnológica da NiO, é vedado ao Colaborador:

- **receber, enviar e compartilhar arquivos que**: (a) tenham finalidades diversas e não relacionadas às atividades de interesse da Companhia ou relativas aos seus negócios; (b) contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação em vigor, a moral e os bons costumes; (c) violem direitos de terceiros, em especial direitos de propriedade intelectual, direitos autorais, direitos de imagem, entre outros; (d) caracterizem infração civil ou penal e/ou possam causar prejuízos à NiO e a terceiros; e (e) configurem concorrência desleal ou quebra de sigilo profissional;
- **enviar, compartilhar e baixar**: (a) arquivos que contenham malware, como vírus e outros códigos maliciosos; (b) Informações Internas, Confidenciais ou Secretas em ambiente externo; e (c) qualquer arquivo executável (.exe) que não seja autorizado pela NiO.

3.4.4 Guarda e Transferência de Informações

Todas as Informações Protegidas que devam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar regras de ciclo de vida dos dados da NiO, bem como os seguintes cuidados, de acordo com a classificação da informação:

- **Suporte físico**. Todos os documentos contendo certas Informações Protegidas devem ser armazenados em arquivos físicos próprios indicados pela NiO, de acordo com os métodos de identificação do conteúdo, também indicados pela Companhia, incluindo sua data de arquivamento. Documentos utilizados pelo Colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, garantindo que tais gavetas e armários permaneçam trancados quando se tratar de informações mais críticas. Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o Colaborador estiver presente. Quando o Colaborador não estiver nas dependências da Companhia, os documentos contendo informações mais críticas não devem ficar expostos.
- **Suporte digital**. Todo e qualquer arquivo que contenha Informações Protegidas deve ser salvo na rede corporativa da NiO, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Caso o arquivo deva ser armazenado em dispositivo móvel (como, por exemplo, em notebooks, por conta de reuniões externas), é indispensável que o Colaborador remova o arquivo do dispositivo após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Protegidas somente poderá ser alterado, copiado e/ou movimentado se houver a possibilidade de recuperação, controle de versão ou

análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

3.4.5 Descarte de Informações

O descarte de um documento físico e/ou a exclusão de um arquivo digital da rede da NiO que contenha Informações Protegidas deverá seguir as seguintes regras de descarte:

- **Suporte físico.** Os documentos que tiverem informações públicas poderão ser descartados no lixo comum; já aqueles que possuírem Informações Protegidas devem ser destruídos manualmente ou, preferencialmente, por um aparelho fragmentador antes do descarte. No caso de informações mais críticas, o uso de aparelho fragmentador é obrigatório e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que este tome as medidas cabíveis.
- **Suporte digital.** Arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível, tais como CD ou DVD, deverão ser destruídos por meio de aparelho fragmentador e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que sejam tomadas as medidas necessárias. Já aqueles arquivos armazenados em suporte digital rígidos, como disco rígido (HD) e pen drive, devem ser encaminhados ao Departamento de Tecnologia, em caixa lacrada, para destruição adequada, conforme o procedimento interno adotado.

Somente o responsável pela geração ou pelo armazenamento do arquivo ou documento a ser descartado tem competência para descartá-lo ou deletá-lo, salvo quando o responsável conferir expressa autorização para que terceiro o faça. Ainda, todo descarte deve ser registrado, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário. No caso de informações que envolvam dados pessoais, o Colaborador Interno seguirá as diretrizes descritas na Política de Retenção de Dados da NiO e o Colaborador Externo seguirá o Manual de Privacidade e Proteção de Dados Pessoais para Terceiros.

3.5 E-mail Corporativo

Os endereços de e-mail fornecidos pela NiO aos Colaboradores são individuais e destinados exclusivamente para fins corporativos e relacionados às atividades do Colaborador dentro da Companhia. As mensagens de e-mail sempre deverão incluir assinatura com o formato padrão da NiO. Acrescentamos que é proibido aos Colaboradores o uso do e-mail da NiO para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da NiO;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a NiO e as suas unidades vulneráveis a ações judiciais e/ou administrativas;

- divulgar informações não autorizadas, incluindo, sem limitação, imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo responsável;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de e-mail quando qualquer uma das unidades ou Colaboradores da NiO estiverem sujeitas a algum tipo de investigação.

3.6 Internet

Todas as regras da NiO visam basicamente ao desenvolvimento de um comportamento ético e profissional no uso da internet. Para garantir a utilização racional desses recursos, bem como a segurança dos dados e softwares, a Companhia se reserva o direito de utilizar ferramentas para verificar o conteúdo dos e-mails corporativos e monitorar o uso da internet e da rede corporativa.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que, nesses casos, a Companhia cooperará ativamente com as autoridades competentes.

Os Colaboradores com acesso à internet poderão fazer o download somente de software homologados na NiO e ligados diretamente às suas atividades.

Os Colaboradores não poderão:

- utilizar os recursos da NiO para fazer o download ou a distribuição de softwares ou dados sem as licenças adequadas;
- efetuar upload (“subir”), para seus clientes, parceiros e outros terceiros, de qualquer software licenciado à NiO ou dados de sua propriedade, sem expressa autorização do responsável pelo software ou pelos dados;

3.7 Redes Sociais e E-Mails Pessoais

A NiO poderá suspender, sem aviso prévio e a seu exclusivo critério, o uso e o acesso a redes sociais, e-mails pessoais e serviços de mensagens para fins pessoais, nas dependências físicas e nos dispositivos da Companhia, por questões de governança e/ou de Segurança da Informação.

3.8 Acesso à rede de arquivos

O acesso às informações armazenadas na infraestrutura técnica da NiO poderá ser realizado de maneira diferente (por meio físico, lógico ou remoto), a depender do tipo de formato. Para cada tipo de formato serão aplicadas regras de conduta distintas, a saber:

3.8.1 Acesso Físico às Informações

Os locais onde estão instalados os datacenters ou armazenados os arquivos físicos da Companhia são considerados parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado. Há diferentes tipos de acessos e, para cada um deles, diferentes regras e restrições, conforme consta abaixo:

- **acessos permanentes**: permitidos somente aos empregados e funcionários da Companhia que tenham a necessidade de acesso liberado para executar suas atividades;
- **acessos esporádicos**: permitidos a outros Colaboradores ou a visitantes externos, mediante autorização prévia da NiO, com acesso registrado (nome, data e hora).
- **acessos externos**: permitidos àqueles que não sejam Colaboradores internos da Companhia (contratantes externos), mediante autorização e registro (nome, data e hora), desde que justifique esse acesso.

3.8.2 Acesso Lógico

O acesso às informações armazenadas na infraestrutura tecnológica da Companhia será restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído pelo Departamento de Tecnologia, conforme as regras dispostas no item 3.9 – *Identificação e Senhas*. Cada perfil pressupõe a liberação do acesso de determinados diretórios dentro da rede da Companhia, que são atribuídos pelo Departamento de Tecnologia, de modo que as informações poderão ser acessadas de acordo com o nível de acesso definido pela NiO.

3.8.3 Acesso Remoto

Quando o Colaborador não se encontrar nas dependências da NiO, ele poderá acessar a rede privada da Companhia de forma remota, por meio de tecnologias autorizadas pela NiO, podendo incluir o uso de VPN. O acesso remoto somente será concedido ao Colaborador nos casos em que houver necessidade comprovada. Verificada a necessidade, o acesso remoto e será concedido pelo sistema de Gestão de acesso de acordo com o perfil do Colaborador.

O acesso remoto somente é permitido para a execução das atividades profissionais do Colaborador que estejam vinculadas à NiO. O Colaborador é responsável por todas as atividades realizadas quando do seu acesso remoto, respondendo por qualquer uso irregular, inclusive por outra pessoa na posse de seu

acesso. No caso de furto, roubo ou extravio de equipamento móvel que tenha o acesso remoto à VPN da Companhia configurado, o Colaborador deverá imediatamente procurar uma autoridade policial para lavrar um boletim de ocorrência e, na sequência, comunicar o incidente à equipe de Tecnologia, apresentando cópia do boletim de ocorrência lavrado.

Todos os acessos remotos serão registrados pela equipe de Tecnologia e tais registros ficarão disponíveis para consulta em caso de auditoria.

3.9 Identificação e Senhas

Todos os Colaboradores têm determinados privilégios de acesso a Informações Protegidas, de acordo com seu cargo e as suas atribuições, conforme as regras dispostas no item 3.8 – *Acesso à Rede de Arquivos*. Alguns exemplos de privilégio são acesso externo ao e-mail, liberações no acesso à internet e no acesso lógico, utilização externa de determinados equipamentos da NiO, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que lhe permitirá ser identificado quando do acesso à infraestrutura da Companhia. Assim, o Colaborador somente terá acesso às áreas da infraestrutura da NiO que forem autorizadas considerando o seu perfil. A NiO reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio dos departamentos competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de Segurança da Informação da Companhia.

O login e a senha do Colaborador são pessoais e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à Companhia.

Além do login do Colaborador, ele também receberá uma identificação física que lhe concederá acesso a determinadas áreas físicas da Companhia. Tal identificação será feita por meio de um crachá, cujo uso é pessoal e intransferível, e terá por finalidade registrar a entrada e saída das dependências da NiO.

3.10 Dispositivos

Os dispositivos físicos capazes de armazenar Informações Protegidas, como computadores, notebooks, tablets e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da NiO, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Companhia, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelo Departamento de Tecnologia.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Os computadores devem ter o recurso de atualizações automáticas do sistema operacional habilitada por padrão e software antivírus instalado, ativado e atualizado frequentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de Tecnologia.

Arquivos pessoais e/ou não pertinentes ao negócio da NiO (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento no disco do computador. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.

Documentos imprescindíveis para as atividades dos Colaboradores e/ou para os negócios da Companhia deverão ser salvos em diretório com serviço de backup e com disponibilidade para acesso. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo ou culpa, e está ciente e concorda em observar as seguintes regras:

- O Colaborador é responsável pelos equipamentos e se compromete a empregar todos os cuidados necessários, como se o dispositivo fosse seu;
- Os dispositivos devem estar sempre a seu alcance e não podem ser deixados em locais públicos, em veículos ou em qualquer outro local, fora das dependências da NiO, em que possa haver acesso do equipamento por pessoas não autorizadas, a fim de evitar o furto e/ou roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas;
- Os Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico de TI da NiO ou por terceiros devidamente contratados para o serviço;
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela NiO, seguindo os devidos controles de segurança exigidos por esta Política e pelas normas específicas da Companhia, assumindo a responsabilidade como custodiante de informações. Em caso de alteração/adulteração de configuração estará sujeito as sanções aplicáveis conforme item 3.14.
- Deverão ser protegidos por senha (bloqueados) todos os dispositivos, incluindo, terminais de computador e impressoras, quando não estiverem sendo utilizados;

- Todos os recursos tecnológicos adquiridos pela NiO devem ter imediatamente suas senhas padrões (default) alteradas;
- Se, no decorrer do uso do dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem a necessidade de sua substituição ou manutenção, o Colaborador deverá abrir um chamado junto ao Departamento de Tecnologia que, por sua vez, além de fornecer os esclarecimentos necessários, deverá orientá-lo a entregar o equipamento no local indicado para sua substituição ou conserto;
- Caso o uso de um dispositivo seja esporádico, o Colaborador deverá devolvê-lo ao Departamento de Tecnologia em perfeitas condições de uso, juntamente com eventuais acessórios que lhe tenham sido entregues, como bolsas, cases, películas etc., tão logo termine o período necessário para o uso. Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Companhia, sem prejuízo de outras medidas legais e administrativas a serem tomadas pela NiO; e
- No caso de perda, furto, roubo ou dano ao equipamento, o Colaborador deve comunicar imediatamente o Departamento de Tecnologia, que procederá com a remoção do conteúdo corporativo contido no dispositivo.

O uso indevido dos dispositivos da NiO sujeitará o Colaborador às sanções aplicáveis, a depender da gravidade da conduta praticada. São algumas hipóteses de uso indevido:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem a explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou software, como, por exemplo, analisadores de pacotes (*sniffers*);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de crimes ou atos ilícitos, como os de assédio sexual, constrangimento, perseguição (*stalking*) ou manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro conteúdo que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública; e
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

3.11 Data Center e Cloud

A NiO utiliza diversos software próprios e de terceiros no curso de suas operações e o Colaborador não poderá:

- utilizar tais software para fins pessoais ou de qualquer forma que comprometa a segurança da infraestrutura da Companhia;
- excluir, modificar, copiar, transferir, realizar engenharia reversa ou ceder o acesso de tais software a terceiros, ou praticar qualquer ato que esteja em desacordo com a legislação aplicável;
- instalar na rede ou nos dispositivos da Companhia qualquer software pirata, não licenciado ou não autorizado pela área TI, sendo que qualquer software não autorizado baixado pelo Colaborador será excluído pela equipe de Tecnologia.

A NiO disponibiliza apenas o(s) recurso(s) para o armazenamento externo de arquivos, software e sistemas. Assim, é proibido a utilização pelo Colaborador de serviços de armazenamento na nuvem não disponibilizados por meio da infraestrutura tecnológica da Companhia.

3.12 Desligamento ou Movimentação do Colaborador

Ao término do vínculo do Colaborador com a NiO, o seu acesso à infraestrutura tecnológica da Companhia será revogado. O Colaborador deverá devolver, em perfeitas condições de uso, todos e quaisquer dispositivos de propriedade da NiO que estejam em sua posse, juntamente com eventuais acessórios lhe tenham sido entregues. As obrigações de sigilo e não reprodução das Informações Protegidas, assumidas pelo Colaborador nessa PSI, permanecerão em vigor mesmo após o desligamento do Colaborador.

Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à NiO.

Caso o Colaborador mude de departamento ou de função dentro da NiO, este também deverá ter seus acessos revistos, passando a visualizar apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

3.13 Reporte de Incidentes de Segurança da Informação

Para evitar a exposição indevida das Informações Protegidas, a NiO emprega medidas de segurança, tanto internas quanto externas, as quais atendem as obrigações legais vigentes. Entretanto, é fundamental que o Colaborador cumpra com as obrigações de segurança assumidas nesta Política, uma vez que tais incidentes podem ocorrer em razão de falhas humanas, tecnológicas ou sistêmicas.

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da Companhia, ele deverá imediatamente

comunicar ao Canal Confidencial. A NiO irá apurar as causas e os efeitos do incidente ocorrido, para, então, tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas, conforme o Procedimento de Resposta a Incidentes de Segurança da Informação envolvendo Dados Pessoais da NiO.

Para que seja realizada uma auditoria sobre o incidente, a NiO analisará toda e qualquer informação, bem como as evidências disponíveis que possam identificar a causa do problema. As informações e evidências serão compiladas e anexadas a um relatório para formalização do ocorrido.

3.14 Compromissos e Penalidades

Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os Colaboradores da NiO.

O descumprimento da Política é considerado uma falta grave e poderá acarretar a aplicação de sanções previstas em lei, assim como advertências, suspensões ou encerramento do contrato de trabalho, conforme procedimentos internos e disposições contratuais.

Todas as disposições legais e demais normas da NiO, como o Código de Ética e Conduta, devem ser rigorosamente observadas.

3.15 Treinamento, Atualização e Divulgação

A NiO conta com um programa contínuo de conscientização de segurança que tem como objetivo conscientizar, treinar e instruir as pessoas, seguindo as melhores práticas internacionais, contribuindo para disseminação da cultura de Segurança da Informação para os Colaboradores da NiO.

O conteúdo da Política é amplo e frequentemente atualizado e divulgado. A releitura desta Política, mesmo que não seja diretamente solicitada, deve ser feita periodicamente para melhor entendimento.

3.16 Disposições Finais

As exceções às regras estabelecidas por esta Política para atender alguma demanda específica, devem ser apresentadas à NiO para avaliação e aprovação.

Essa Política poderá ser revista, atualizada e alterada a qualquer tempo, a exclusivo critério da NiO, sempre que algum fato relevante ou evento motive sua revisão.

4 PAPÉIS E RESPONSABILIDADES

Conselho de Administração

- Aprovar esta Política, reforçando o compromisso da alta direção com a melhoria contínua dos processos de segurança e designar em sua estrutura corporativa um diretor responsável pela sua gestão.

Área de Segurança da Informação

- Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na NiO, promovendo ações de interesse para o negócio, programas educacionais e de conscientização do capital humano.

Colaboradores

- Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais diretrizes que a compõem;
- Informar as situações que comprometam ou possam comprometer a segurança das informações através do Canal Confidencial disponibilizado pela NiO para essa finalidade;
- Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da NiO, não devendo ser considerada como particular ou confidencial, mesmo que arquivadas na pasta pessoal dos Colaboradores;
- Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares);
- Revisar seus acessos sempre que mude de departamento ou de função dentro da NiO;
- Garantir que os requisitos, políticas e processos de Segurança da Informação e de proteção de dados constem nas aquisições e/ou implementações tecnológicas e se mantenham durante seu ciclo de vida.

5 REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

Canal Confidencial: 0800 721 0783 (https://www.canalconfidencial.com.br/vtal/)

NIST Cybersecurity Framework Version 1.1.

Política de Classificação de Dados

Política de Retenção de Dados

Manual de Privacidade e Proteção de Dados Pessoais para Terceiros

6 GLOSSÁRIO

- Autenticidade: garantia da veracidade da autoria da informação;
- Colaboradores: todos os Colaboradores Internos e Colaboradores Externos que, no âmbito de sua relação com a NiO, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da Companhia;
- Colaboradores Externos: todos os funcionários contratados indiretamente pela Companhia, sejam eles prestadores de serviços, terceiros, fornecedores e parceiros da Companhia;
- Colaboradores Internos: todos os empregados contratados diretamente pela Companhia, sejam eles sócios, diretores, administradores, funcionários, menores aprendizes e estagiários;
- Confidencialidade: a informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;
- Conformidade: processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração;
- Disponibilidade: as pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes sempre que necessário;
- Integridade: salvaguarda da exatidão da informação e dos métodos de processamento;
- Informação: é a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou NiO de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;
- Informação Protegida: toda informação e qualquer dado ou ativo gerados, adquiridos, manuseados, armazenados, sob a guarda, transportados e/ou descartados pelos Colaboradores nas dependências e/ou em ativos da Companhia, em virtude de seu vínculo com a NiO ou do desempenho de suas atividades contratadas pela Companhia.
- Incidente de Segurança da Informação: toda e qualquer violação de segurança que, de forma acidental ou não, leva ou seja capaz de levar à destruição, perda, alteração, bloqueio, divulgação ou ao uso ou acesso não autorizados aos dados pessoais ou outras informações tratadas pela NiO e pelos Colaboradores;

- Risco de Segurança da Informação: riscos associados à violação da autenticidade, confidencialidade e integridade, bem como da disponibilidade das informações nos meios físicos e digitais ou de outras propriedades da informação;
- Segurança da Informação (SI): é o conjunto de ações e controles que tem como objetivo a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da NiO e atendimento dos seus clientes.

7 ANEXOS

Não se aplica

ESTE DOCUMENTO REVOGA VERSÕES ANTERIORES