NORTE SOLUÇÕES ELÉTRICAS

Política de Segurança da Informação

Versão 1.
Julho/2023

NORTE SOLUÇÕES ELÉTRICAS – CNPJ: 489.057.39/0001-79
RUA DAS PRIMAVERAS 2792 – SETOR RESIDENCIAL SUL 78550-021
(66) 9 9603-1437

NORTE SOLUÇÕES ELÉTRICAS

SUMÁRIO

INTRODUÇÃO

A segurança da informação é um tema muito importante. E apesar dos avanços tecnológicos em um mundo cada vez mais digital, infelizmente, a incidência de fraudes, perdas e roubos de informações também está aumentando.

A Norte Soluções Elétricas enxerga que os procedimentos e padrões de segurança para nossas informações e, principalmente, para nossos clientes, sejam sólidos e eficazes. Assim, recomendamos que esta Política seja sempre consultada a garantir que qualquer decisão esteja baseada nos critérios aqui estabelecidos.

Este documento é para uso interno, o que significa que as informações não devem ser acessadas ou divulgadas fora do ambiente da NSE.

ABRANGÊNCIA

Esta Política é aplicável a toda empresa Norte Soluções Elétricas, seus colaboradores (sócios, colaboradores, estagiários), partes relacionadas e quaisquer terceiros que possuam alguma relação laboral conosco.

OBJETIVO

O objetivo desta política é o de estabelecer regras para a segurança de nossas informações, sejam elas em etapas de processamentos, transmissão ou armazenamento físico ou digitalmente em sistemas próprios ou contratados pela empresa.

As regras aqui definidas buscam estabelecer processos seguros para:

- ✓ O armazenamento, transmissão, processamento e descarte de dados;
- ✓ A manutenção da segurança dos sistemas;
- ✓ A prevenção da ocorrência de atos ilícitos;
- ✓ O uso de dispositivos e aplicações vinculados a empresa NSE;
- ✓ As segregações de acesso;
- ✓ O descarte de dispositivos e mídias;
- ✓ A classificação de informações, com base em critérios de confidencialidade, disponibilidade e integridade; e
- ✓ O monitoramento de sistemas e dispositivos pertencentes a NSE.

Assim, garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização do negócio da empresa NSE.

PRINCIPAIS REFERÊNCIAS REGULATÓRIAS E INTERNAS

A presente Política estabelece as diretrizes da empresa para resguardo e uso de dados pessoais que venham a ser tratados em suas atividades, tendo como referência as Leis que tratam da Proteção de Dados Pessoais.

- ✓ **Lei 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD)** – Dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado.
- ✓ **LEI Nº 12.965/2014 (Marco Civil da Internet)** – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- ✓ **Código de Ética e Conduta;**

1. ESTRUTURA

A estrutura de segurança da informação da empresa é autónoma, permitindo tomar as medidas necessárias à plena implementação e manutenção da eficácia dos mecanismos de proteção.

1.1 FUNÇÕES E RESPONSABILIDADES

É imprescindível para a eficácia das medidas de segurança da informação que as principais funções de cada área estejam devidamente previstas, de maneira clara e objetiva.

1.1.1. ADMINISTRATIVO

- ✓ Realizar o controle do acesso às instalações físicas da empresa, colaboradores, prestadores de serviços e visitantes;
- ✓ Exercer a gestão dos contratos com as empresas independentes de prestação de serviço;
- ✓ Propor projetos e iniciativas referentes à proteção das informações armazenadas em arquivos físicos;
- ✓ Mapear e definir perfis de acesso a sistemas;
- ✓ Assegurar que processos estejam atualizados;

1.1.2. DIRETORIA

- ✓ O controle de exceções de concessão e o mapeamento de perfis de acessos;
- ✓ Revisão da presente política.

1.1.3. COLABORADORES EM GERAL

- ✓ Obedecer às regras estabelecidas pela presente política, bem como notificar eventuais falhas de segurança para o setor administrativo e/ou TI (quando houver);
- ✓ Os usuários (logins) individuais dos colaboradores serão de responsabilidade do próprio colaborador;
- ✓ Respeitar os controles e mecanismos de segurança existentes, na forma especificada pelos perfis de acesso definidos;
- ✓ Não utilizar, copiar ou armazenar softwares não validados por TI ou em violação à legislação de propriedade intelectual;
- ✓ Auxiliar na divulgação e incorporação das normas e boas práticas de segurança da informação em suas respectivas áreas de atuação.

1.1.4. COMERCIAL

- ✓ Dar o tratamento adequado às informações recebidas e enviadas para clientes e demais partes relacionadas, bem como observar o estrito cumprimento das regras de segurança da informação e outras atribuições que forem pertinentes.

1.1.5. ENCARREGADOS

Os encarregados devem ser o exemplo de conduta a ser seguido pelos colaboradores de suas equipes e o fiscalizador da conduta. As responsabilidades dos encarregados são:

- ✓ Observar o comportamento dos seus colaboradores, atentando-se, à conduta de trabalho e uso dos equipamentos eletrônicos e credenciais de acesso;
- ✓ Informar previamente à área administrativa para a concessão de acessos lógicos a terceiros contratados;
- ✓ Replicar as políticas de segurança para todos de sua equipe;
- ✓ Notificar para a ocorrência de falha de segurança e/ou incidentes.

1.1.6. RECURSOS HUMANOS

O RH é responsável pela gestão dos colaboradores, bem como pelas funções atribuídas a cada um deles. A comunicação entre RH e as demais áreas é essencial para sistemas de controle de acesso eficazes. Cabe ao RH:

- ✓ O controle de colaboradores ativos e da função que exercem, devendo informar os casos de admissão, demissão, transferência ou suspensão de colaboradores;
- ✓ Coordenar os treinamentos de conscientização de colaboradores acerca das regras de segurança da informação;
- ✓ Comunicar e orientar, na fase de contratação, sobre os procedimentos de segurança, bem como o uso correto dos ativos de tecnologia;
- ✓ Arquivar eventuais Termos de Compromisso e Responsabilidade assinados pelos colaboradores junto à respectiva pasta cadastral.

1.1.7. TECNOLOGIA DA INFORMAÇÃO

A TI é o responsável pela implementação das medidas de segurança cibernética, bem como na correção de falhas, dentre outras funções à efetividade desta política, sendo responsáveis por:

- ✓ A implementação e aplicação das medidas previstas nesta Política;

- ✓ Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais observados;
- ✓ Coordenar os processos de correção de vulnerabilidades identificadas no ambiente, bem como efetuar alertas acerca de novas ameaças;
- ✓ Tomar ações emergenciais preventivas e/ou corretivas em casos de ameaças da integridade dos dados e/ou sistemas;
- ✓ Validar requisitos técnicos na contratação de produtos ou serviços de tecnologia;
- ✓ Coordenar a obtenção e atualização de certificados de segurança eventualmente necessários;
- ✓ Conceder os acessos à rede, e-mail, intranet e sistemas aplicáveis, de acordo com a função de cada colaborador e eventuais determinações de Controles Internos;
- ✓ Manter controles de segurança da informação definidos nesta política;
- ✓ Sugerir melhorias nesta política e procedimentos relacionados;
- ✓ Conduzir respostas a incidentes, juntamente com o auxílio dos departamentos necessários à resolução do problema;
- ✓ Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- ✓ Assegurar que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;
- ✓ Corrigir e mitigar vulnerabilidades sistêmicas detectadas;
- ✓ Realizar manutenção da disponibilidade dos serviços, bem como de internet, telefonia, e-mail;
- ✓ Observar requisitos técnicos indispensáveis para manter a estabilidade, segurança, integridade e funcionalidade à prestação adequada dos nossos serviços.

2. CLASSIFICAÇÃO DAS INFORMAÇÕES

A classificação do sigilo das informações consiste na definição de níveis de proteção que cada tipo de informação deve receber.

Ela serve para garantir que nenhuma informação seja divulgada indevidamente e que apenas os colaboradores que têm direito recebam acesso à informação.

A segurança da informação deve garantir que as informações sejam classificadas de acordo com seu valor, requisitos legais, criticidade e sensibilidade.

Existem na empresa 03 (três) tipos de informação, de acordo com a sua classificação:

- ✓ **Confidencial:** informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da empresa ou causar impactos graves, sob o aspecto financeiro, legal e normativo.
- ✓ **Pública:** As informações podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.
- ✓ **Interna:** as informações não devem ser acessadas ou divulgadas fora do ambiente da NSE.

As classificações acima devem utilizadas a nível organizacional por todos os setores em todos os documentos gerados ou tratados pelo proprietário da informação.

3. TRATAMENTO E PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO

3.1 GUARDA DE INFORMAÇÕES

Todas as informações devem ser mantidas pelos colaboradores em unidades de armazenamento fornecidas pela empresa NSE, seja em sua rede corporativa ou em serviços de armazenamento contratados. O acesso a informações confidenciais deve ser restrito conforme apropriado para que o menor número possível de pessoas possa acessá-las.

A empresa não se responsabiliza por informações armazenadas localmente (na estação de trabalho do usuário) caso ocorra perda dos dados. Torna-se de total responsabilidade do usuário o armazenamento dos dados em local seguro disponibilizado pela TI/Administrativo (**sharepoint/onedrive**).

Documentos físicos deverão ser armazenados em locais com acesso controlado e organizado. Documentos cujo conteúdo seja restrito não devem permanecer sobre as mesas de trabalho ou em locais de fácil acesso.

3.2ACESSO FÍSICO E LÓGICO

Todo acesso deve passar por processo de autorização e registro, seja para a concessão, alteração ou para a restrição. Os acessos são pessoais e intransferíveis. É vedado o compartilhamento de

acessos entre os colaboradores, bem como com pessoas que não pertençam ao quadro de funcionários ativos da empresa.

3.3 ACESSO LÓGICO

O acesso aos sistemas e unidades de armazenamento deve ser organizado de maneira a restringir os usuários para acessarem somente as informações necessárias para o exercício pleno de sua função.

Cada usuário terá seu acesso pessoal, com login e senha, para o uso das estações de trabalho, bem como para o acesso às redes e sistemas específicos de sua função e de acordo com perfis definidos.

Exceções aos acessos delimitados serão tratados da seguinte forma:

- ✓ Rede e pastas diversas: deverão ser previamente aprovados pelos gestores primários proprietários da informação, considerando a necessidade do conhecimento dessas informações pelo solicitante para execução de suas atividades; e
- ✓ Sistemas e Internet: serão analisados caso a caso mediante necessidade e perfis pré-definidos.

3.4 ACESSO FÍSICO

O acesso físico aos dispositivos de armazenamento de dados, em especial aqueles que contenham informações restritas, deve ser monitorado e restrito apenas aos usuários que possuam função e autorização adequadas para acessá-los. Da mesma forma, o acesso às áreas em que haja arquivamento físico de informações sensíveis deve ser restrito apenas às pessoas autorizadas.

3.4.1 ACESSO DE TERCEIROS

Nos casos de visitas de terceiros e/ou prestadores de serviços às instalações da empresa, estes deverão sempre ter o acompanhamento por um colaborador responsável.

Os acessos lógicos necessários a terceiros serão eventualmente liberados mediante solicitação dos gestores responsáveis estabelecendo data de início e fim do acesso, nunca ultrapassando o prazo inicial de **6 (seis) meses**.

3.5 SENHAS E CÓDIGOS DE ACESSO

As senhas são parte importante das medidas de segurança. Por conta disso, é de suma importância a utilização de senhas que sigam padrões de segurança estabelecidos pela TI.

A senha é de uso pessoal e intransferível, não podendo ser compartilhada, portanto, na ocorrência de prejuízo causado pelo fornecimento da senha pessoal, independente do motivo, o usuário será responsabilizado e sujeito às sanções e penalidades cabíveis ao caso.

3.6 MÍDIAS E RECURSOS PORTÁTEIS

Mídias pessoais e não pertencentes a empresa podem representar riscos à segurança dos nossos sistemas e informações. Dispositivos que contenham memória interna podem carregar consigo softwares mal-intencionados que, ao terem contato por meio da conexão de um dispositivo pessoal à rede corporativa, podem causar grandes prejuízos.

É responsabilidade de todos os colaboradores, principalmente dos gestores, o zelo pela integridade dos dados armazenados pela empresa. Com o objetivo de evitar equívocos, deve-se seguir algumas regras:

- ✓ Todas as mídias fornecidas pela NSE devem ser identificadas, para o fácil reconhecimento e distinção de mídias não oficiais;
- ✓ É vedado o uso de todo e qualquer tipo de mídia ou recursos portáteis (dispositivos como pen-drive, HD externo, cartão de memória, CD/DVD, software, etc.) que não sejam de propriedade da NSE ou autorizados por TI; e
- ✓ Caso ocorra a necessidade de utilização de mídias ou recursos portáteis será necessária a prévia autorização de TI.

3.7 TELEFONIA E E-MAIL

É responsabilidade de todos os colaboradores o bom senso na utilização dos serviços de telefonia.

Não é garantida a confidencialidade das ligações, podendo a empresa ter acesso as mesmas quando julgar necessário.

No entanto, é permitido o uso eventual do e-mail corporativo para fins pessoais, desde que:

- ✓ não cause risco à integridade dos sistemas da empresa;
- ✓ não contrarie a moral e bons costumes;
- ✓ não viole as leis aplicáveis;

- ✓ não comprometa a nossa imagem, dos colaboradores ou de terceiros;
- ✓ não prejudique as atividades profissionais; e
- ✓ não prejudique a segurança das informações e dos recursos corporativos.

A empresa poderá, a qualquer tempo, acessar e-mail e informações recebidas ou enviadas pelos colaboradores, uma vez que todo o conteúdo dos e-mails ou de outras ferramentas concedidas pela empresa está sujeito a monitoramento, que poderá ser acionado em casos de investigação de denúncias ou necessidades operacionais a critério das deliberações da diretoria.

Caso o e-mail seja utilizado de forma inadequada colocando em risco o domínio da empresa (@nsemt.com.br), o usuário poderá ser igualmente acionado em casos de investigação de denúncias ou necessidades operacionais.

O sistema de e-mail deverá possuir mecanismo de proteção contra arquivos anexos suspeitos de contaminação por vírus (“antivírus”) e contra a disseminação de e- mails em massa enviados sem o consentimento dos usuários (spam).

O sistema de e-mail corporativo não deverá ser utilizado para criação ou distribuição de mensagens ofensivas ou impróprias, incluindo conteúdo ou comentários sobre raça, gênero, aspectos físicos, orientação sexual, pornografia, religião, política, dentre outras.

3.8 DESCARTE DE INFORMAÇÕES OU MÍDIAS

No descarte devem ser utilizados métodos de remoção segura, com o uso de ferramentas específicas e o apoio de TI, devendo ser assegurado que a informação tenha sido completamente apagada da memória do dispositivo.

O descarte de documentos físicos confidenciais ou restritos deve ser feito mediante o uso de fragmentadora, ou qualquer outro meio similar.

Caso encontre algum documento que não lhe pertença, o colaborador deve imediatamente notificar a diretoria e entregar aos seus cuidados o referido documento para adoção das medidas necessárias.

O descarte de informações e/ou mídias, nos casos aplicáveis, só poderá ser efetivamente realizado, transcorrido o prazo estipulado em Política específica que aborde o tema.

3.9 USO DE EQUIPAMENTO COMPUTACIONAL

Os colaboradores que tiverem direito ao uso de equipamento computacional, de propriedade da NSE, devem estar cientes que:

- ✓ Os recursos de tecnologia da informação, disponibilizados para os colaboradores, têm como objetivo a realização de atividades profissionais.
- ✓ A proteção do recurso computacional de uso individual é de responsabilidade do próprio colaborador.
- ✓ É de responsabilidade de cada colaborador assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- ✓ O colaborador não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:

3.9.1 FORA DAS DEPENDÊNCIAS:

- ✓ Mantenha o equipamento sempre com você;
- ✓ Atenção redobrada em hall de hotéis, aeroportos, aviões, táxi e etc;
- ✓ Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível.

3.9.2 EM CASO DE FURTO

- ✓ Registre a ocorrência em uma delegacia de polícia;
- ✓ Comunique ao seu superior imediato e ao Setor de TI e administrativo; e
- ✓ Envie uma cópia da ocorrência para o Setor de TI e administrativo da empresa.

3.10 COMUNICAÇÃO VERBAL

Toda comunicação verbal deve ser pautada no princípio de *"dever saber"* (*need to know)*. Informações consideradas internas não deverão ser compartilhadas com amigos, familiares, ou qualquer outra pessoa que não se encontre no quadro de colaboradores da empresa.

Da mesma forma, informações restritas e confidenciais devem ser compartilhadas apenas entre aqueles que possuam autorização para ter ciência destas. Toda informação restrita ou confidencial deve ser tratada sempre em local restrito, como as salas de reunião. Deve-se evitar ao máximo conversas em locais públicos que contenham as informações acima mencionadas.

4. PENALIDADES

Em caso de violação a esta política poderão ocorrer os seguintes níveis de sanções disciplinares, de acordo com o disposto em nosso **Código de Ética**:

- ✓ **Notificação** – caso seja necessária apenas a correção de alguma conduta;
- ✓ **Advertência** – caso seja alguma infração de média gravidade ou reincidência; e
- ✓ **Suspensão ou Demissão** - nos casos de alta gravidade.

Portanto, ao apurar o descumprimento das regras, serão realizados procedimentos disciplinares resultando na aplicação de medidas administrativas, com caráter educativo e/ou punitivo, podendo o profissional ser advertido, afastado preventivamente de suas funções ou, em casos mais graves, suspenso ou desligado de suas funções institucionais, bem como a comunicação, pela empresa, das eventuais violações às autoridades competentes para a responsabilização cível e criminal, quando aplicável.

5. CONSIDERAÇÕES FINAIS

Todos os colaboradores, sem qualquer distinção, devem atestar a leitura e perfeita compreensão deste documento e suas posteriores alterações.

A presente política será revisada quando demandado ou, no mínimo, a cada 2 (dois) anos. A revisão não necessariamente resultará em uma nova versão do documento.

Em situações que não se encaixem ou estejam em desacordo de qualquer maneira com esta Política, deverão ser submetidas a Diretoria, que analisará as circunstâncias e fundamentos.