

# Política de Proteção de Dados Pessoais

**Versão 1.**

**Julho/2023**

## SUMÁRIO

INTRODUÇÃO .....	4
ABRANGÊNCIA.....	4
OBJETIVO.....	4
PRINCIPAIS REFERÊNCIAS REGULATÓRIAS E INTERNAS .....	4
1. PRINCIPAIS DEFINIÇÕES .....	5
1.1 PRIVACIDADE .....	5
1.2 PROTEÇÃO DE DADOS.....	5
2. COLETA DE DADOS E CONSENTIMENTO .....	8
3. DIREITOS DOS TITULARES DE DADOS .....	8
4. DAS DIRETRIZES DE TRATAMENTO DE DADOS .....	9
4.1 CONFIDENCIALIDADE .....	9
4.2 FINALIDADE E ADEQUAÇÃO .....	10
4.3 NECESSIDADE .....	10
4.4 QUALIDADE DOS DADOS.....	10
4.5 QUALIDADE DOS DADOS.....	10
4.6 NÃO DISCRIMINAÇÃO .....	10
4.7 MEDIDAS DE SEGURANÇA.....	10
4.8 ENCERRAMENTO .....	11
5. HIPÓTESES DE COMPARTILHAMENTO OU DIVULGAÇÃO DE DADOS .....	11
6. ARMAZENAMENTO E ELIMINAÇÃO .....	12
7. SUBCONTRATAÇÃO .....	13
8. REGISTRO DE ATIVIDADES E AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS.....	13
9. FUNÇÕES E RESPONSABILIDADES .....	14
9.1 COMERCIAL .....	14
9.2 DIRETORIA .....	14
9.3 ENCARREGADO DE DADOS PESSOAIS – DPO .....	14
9.4 RECURSOS HUMANOS (“RH”) .....	15
9.5 TECNOLOGIA (“TI”).....	15

9.6 COLABORADORES EM GERAL.....	16
10. CANAIS DE ATENDIMENTO .....	16
11. RESPOSTAS A INCIDENTES .....	16
12. AUDITORIA .....	18
13. PROCEDIMENTOS DISCIPLINARES.....	18
14. PENALIDADES .....	19
15. CONSIDERAÇÕES FINAIS .....	19

## **INTRODUÇÃO**

Esta Política foi elaborada para estabelecer regras relativas à Proteção de Dados Pessoais na empresa Norte Soluções Elétricas

Em atendimento à Lei nº 13.709/2018, Lei Geral de Proteção de Dados (“LGPD”), bem como em aderência às melhores práticas de mercado, a NSE, por meio desta Política define as diretrizes de proteção dos dados pessoais nos nossos processos internos, visando explicar e reafirmar nosso compromisso com a privacidade, a proteção de dados, as melhores práticas de segurança da informação e a transparência no acesso e tratamento dos dados pessoais coletados, acessados ou manuseados.

Recomendamos que esta Política seja periodicamente consultada de forma a garantir que qualquer decisão esteja baseada na versão atualizada.

## **ABRANGÊNCIA**

Esta Política é aplicável a todas as empresas que integram a empresa NSE, seus colaboradores (sócios, colaboradores, estagiários), partes relacionadas e quaisquer terceiros que possuam alguma relação laboral conosco.

## **OBJETIVO**

Estabelecer as regras, parâmetros, conceitos, critérios e diretrizes relacionadas à proteção de dados pessoais de todos os indivíduos, incluindo, mas não limitados aos atuais, futuros ou potenciais candidatos a vagas de emprego ou estágio, colaboradores, clientes, fornecedores, parceiros comerciais ou prestadores de serviços.

## **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;**
- ✓ **Política de Segurança da Informação.**

## 1. PRINCIPAIS DEFINIÇÕES

Proteção de dados e privacidade têm abordagens bastante diferentes para alcançar o objetivo principal.

Abaixo, conceituamos estes termos para os fins de escopo desta Política:

### 1.1 PRIVACIDADE

Entende-se como privacidade o direito à reserva de informações pessoais e da própria vida pessoal. É o controle que um indivíduo exerce sobre a entrada e saída de informações sobre si mesmo.

### 1.2 PROTEÇÃO DE DADOS

Sabendo que a Privacidade é o direito de ser protegido de uma interferência em assuntos pessoais, a **Proteção de Dados** representa o modo para implementar essa proteção.

Para que a NSE assegure a proteção dos dados pessoais e sensíveis que possuímos, adotamos um conjunto de processos e ferramentas que visam garantir a proteção dessas informações contra ameaças externas e internas.

Além disso, a NSE atende os direitos dos titulares de dados estabelecidos armazenando os registros que comprovam todas as ações que envolvam dados pessoais para uma eventual auditoria, fiscalização da ANPD (Autoridade Nacional de Proteção de Dados) ou até mesmo em processos judiciais.

Para os fins desta Política, considera-se:

- ✓ **Autoridade Nacional de Proteção de Dados (“ANPD”):** órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD);
- ✓ **Controlador:** pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais;
- ✓ **Operador:** pessoa natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador;
- ✓ **Titular:** a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Indivíduo que pode ser identificado direta ou indiretamente, a partir de um nome, um número de identificação ou de matrícula, dados de localização ou por um ou mais fatores físicos, psicológicos, genéticos, mentais, econômicos, culturais específicos ou identidade social;
- ✓ **Informação:** Consiste em qualquer dado pessoal em qualquer meio, incluindo mas não se limitando à base de dados, documentos (físicos, eletrônicos, magnéticos ou digitais) finalizados ou em desenvolvimento, recursos de informática, segurança de tecnologia da informação (domínios, mídias, processos, políticas, procedimentos, medidas, recursos de segurança), informações comerciais, financeiras, estatísticas, jurídicas e/ou técnicas, relacionadas aos negócios ou aos empregados da empresa e, em geral, qualquer conhecimento ou comunicação transmitida por qualquer forma (verbal, escrita, audiovisual etc.);
- ✓ **Dado Pessoal:** qualquer informação relacionada a um titular identificado ou identificável. Tais dados podem incluir, entre muitos outros, nome, endereço, número de telefone, CPF, número da carteira de habilitação e detalhes de transações comerciais pessoais;
- ✓ **Dado Pessoal Sensível:** informação sobre origem racial ou étnica, convicção religiosa, posicionamento político, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando

vinculado a uma pessoa natural, bem como aquelas Informações que, ainda que sejam difundidas na empresa, sejam classificadas como sendo de uso interno;

- ✓ **Encarregado de Proteção de Dados (*Data Protection Officer* – “DPO”)**: pessoa natural, indicada pela NSE, com base em sua expertise e conhecimento do tema, responsável por supervisionar a estratégia e coordenar a implementação da proteção de dados pessoais, bem como atuar como canal de comunicação entre a NSE, titulares e a autoridade nacional, assegurando a conformidade com a LGPD;
- ✓ **Tratamento**: toda operação realizada com dados pessoais, como as que se referem à visualização, acesso, coleta, gravação, organização, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outro modo disponibilização, alinhamento ou combinação, bloqueio, exclusão, descarte ou destruição;
- ✓ **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- ✓ **Anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- ✓ **Incidente**: violação da segurança que provoque, de modo acidental, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;
- ✓ **Vazamento de dados**: trata de exposição intencional de dados pessoais e/ou dados sensíveis a pessoas não autorizadas. Destacando que, a utilização deliberada dos dados para finalidade diversa à da coletada também pode ser enquadrada como vazamento dos dados;
- ✓ **Transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

## **2. COLETA DE DADOS E CONSENTIMENTO**

Utilizamos os dados pessoais coletados principalmente para prestar o serviço, realizar uma transação ou comercializar o produto requisitado, de acordo com os nossos procedimentos internos.

A NSE informará aos titulares sobre eventuais demandas legais que resultem na divulgação de dados pessoais, a menos que tal informação seja vedada por lei ou proibida por mandado judicial ou, ainda, se a requisição for emergencial. A NSE contestará essas demandas se julgar que as solicitações são excessivas, infundadas ou realizadas por autoridades incompetentes.

Quanto ao consentimento do titular, este será realizado mediante o aceite da Política, bem como por meio de cláusulas contratuais junto a terceiros relacionados e colaboradores.

As regras previstas nessa Política não se aplicam a dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado.

## **3. DIREITOS DOS TITULARES DE DADOS**

O titular dos dados pessoais tem direito a obter da empresa controladora da empresa, em relação aos seus próprios dados por ela tratados, a qualquer momento e mediante requisição:

- Confirmação da existência de tratamento;
- Acesso aos dados de forma facilitada, gratuita e transparente sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais, observados os segredos comercial e industrial;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto em Lei;

- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses legais;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento, nos termos da Lei.

Os direitos acima poderão ser exercidos pelo usuário mediante requerimento realizado via e-mail direcionado ao Encarregado de Dados (DPO), desde que comprovada sua identidade, ou outro meio idôneo disponibilizado pela empresa para a mesma finalidade. Alterações dependerão do envio de solicitação para posterior avaliação e adoção de demais providências.

#### **4. DAS DIRETRIZES DE TRATAMENTO DE DADOS**

A seguir, trataremos das diretrizes básicas que regularão o tratamento de dados pela empresa e demais partes envolvidas no tratamento de dados relacionados aos seus negócios.

##### **4.1 CONFIDENCIALIDADE**

Toda informação, sensível ou não, tratada pela empresa, deve ser mantida no mais absoluto e estrito sigilo, mesmo após o término da relação entre as partes na hipótese em que seja necessário o armazenamento dos dados, por prazo não inferior a 5 (cinco) anos contados a partir do término da relação contratual, salvo caso de eliminação dos dados antes desse prazo.

Nenhuma informação, sensível ou não, poderá ser extraída ou transmitida de qualquer forma ou meio (eletrônico, mecânico, fotocópia, gravação ou outro meio) das instalações da empresa, salvo se houver autorização expressa para praticá-los, de modo que se reconhece o dever de confidencialidade das informações e as obrigações relacionadas ao tratamento das informações.

## **4.2 FINALIDADE E ADEQUAÇÃO**

Toda informação, sensível ou não, deverá ser tratada exclusivamente para a finalidade informada e consentida pelo titular de dados, os quais devem ser legítimos, específicos, explícitos, informados ao titular e compatíveis com as finalidades informadas ao titular, de acordo com o contexto do tratamento, sem possibilidade de tratamento posterior, salvo exceção legal ou novo consentimento

## **4.3 NECESSIDADE**

Toda informação, sensível ou não, deverá ser limitada ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

## **4.4 QUALIDADE DOS DADOS**

Toda informação, sensível ou não, deverá ser exata, clara, relevante e atual, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

## **4.5 QUALIDADE DOS DADOS**

Toda informação, sensível ou não, deverá ser exata tratada de forma segura, com a adoção de medidas, técnicas e administrativas, preventivas e repressivas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

## **4.6 NÃO DISCRIMINAÇÃO**

Toda informação, sensível ou não, não deverá ser utilizada para fins discriminatórios ilícitos ou abusivos.

## **4.7 MEDIDAS DE SEGURANÇA**

Deverão ser cumpridos todos os padrões e procedimentos de segurança técnicos e organizacionais relacionados abaixo para o tratamento das informações, sensíveis ou não:

- a) Pseudonimização, entendida como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

- b) Criptografia;
- c) Garantia da confidencialidade permanente, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento;
- d) Capacidade de restaurar a disponibilidade e o acesso às informações, sensíveis ou não, rapidamente, em caso de incidente físico ou técnico;
- e) Procedimento de verificação, avaliações regulares da eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento;
- f) Garantir que todas as ferramentas tecnológicas (hardware, software e comunicação) utilizadas sejam licenciadas;
- g) Proteger todas as ferramentas tecnológicas (hardware, software e comunicação) com antivírus;
- h) Não conectar seus recursos à rede de comunicações pertencente a empresa, a menos que expressamente autorizado;
- i) Não realizar a instalação de quaisquer softwares, a não ser que haja a prévia e expressa autorização para fazê-lo pela área de TI.

#### **4.8 ENCERRAMENTO**

No encerramento dos serviços e/ou nas hipóteses previstas na legislação, as informações, sensíveis ou não, deverão ser destruídas imediatamente e de forma irreversível, salvo para o atendimento das hipóteses previstas na legislação.

Na hipótese de descarte de qualquer suporte tecnológico, este deverá ser destruído ou apagado usando todas as medidas cabíveis para impedir a recuperação subsequente das informações.

#### **5. HIPÓTESES DE COMPARTILHAMENTO OU DIVULGAÇÃO DE DADOS**

Em regra, o compartilhamento e/ ou divulgação de dados somente poderá ser realizado mediante consentimento específico do titular. Todavia, em alguns casos, a NSE poderá divulgar os

dados pessoais coletados com o objetivo de cumprir a legislação vigente ou por força de ordem ou intimação judicial ou administrativa, nos seguintes cenários:

- ✓ Investigar, impedir ou tomar medidas relacionadas a cooperação com órgãos públicos ou para proteger a segurança nacional;
- ✓ Execução de contratos;
- ✓ Investigação e defesa de alegações de terceiros;
- ✓ Proteção da segurança ou integridade dos serviços;
- ✓ Cumprimento de obrigação legal ou regulatória pelo controlador;
- ✓ Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- ✓ Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei;
- ✓ Quando do uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados;
- ✓ Quando os dados forem tornados manifestamente públicos pelo titular, resguardados os direitos do titular.

As hipóteses acima descritas não excluem outras porventura existentes ou que venham a ser criadas pelas autoridades públicas.

## **6. ARMAZENAMENTO E ELIMINAÇÃO**

Conservamos os dados pessoais estritamente pelo tempo necessário para as finalidades para as quais forem processados para execução de nossos negócios e/ou para cumprimento de obrigação legal ou regulatória.

Os Dados Pessoais serão excluídos após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

- ✓ Cumprimento de obrigação legal ou regulatória pelo Controlador dos dados;
- ✓ Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados; ou

- ✓ Uso exclusivo do Controlador, vedado seu acesso por terceiro, e, em caso de necessidade eventual, desde que estes sejam anonimizados.

## **7. SUBCONTRATAÇÃO**

Sempre que houver a contratação ou subcontratação de serviços que envolvam o tratamento de dados, deverá haver expressa previsão de que a empresa, seus empregados, prepostos, representantes ou terceiros designados para o tratamento dos dados deverão se comprometer, expressamente e por escrito, a respeitar a confidencialidade e a cumprir as medidas de segurança contidas neste instrumento, responsabilizando-se pelo repasse de toda a informação e treinamento sobre as obrigações estabelecidas neste documento, sujeitando-se às mesmas condições (instruções, obrigações, medidas de segurança etc.) e aos mesmos requisitos formais submetidos ao contratado em relação ao tratamento adequado dos dados e garantia dos direitos dos titulares de dados.

No caso de descumprimento pelo subcontratado, o contratado permanecerá totalmente responsável perante a empresa em relação ao cumprimento das obrigações estabelecidas neste instrumento.

A contratada e a subcontratada devem manter à disposição da empresa a documentação que comprove o cumprimento das obrigações estabelecidas neste documento, e deverão comunicar imediatamente a partir do conhecimento ou da suspeita de incidentes ocorridos/a ocorrer que afetem a segurança dos dados relacionadas ao empresa, de acordo com as normas e procedimentos que estabelecerão para esse fim.

## **8. REGISTRO DE ATIVIDADES E AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**

Deverá ser providenciado pelo **DPO** o **Relatório de Impacto à Proteção de Dados Pessoais**, entendido como a documentação que contenha a descrição dos processos de tratamento de dados

personais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Também deverá ocorrer a colaboração de uma parte à outra quando a elaboração do relatório de impacto seja necessária, assim como a colaboração mútua em eventual consulta que possa ocorrer à Autoridade Nacional, quando apropriado.

## **9. FUNÇÕES E RESPONSABILIDADES**

### **9.1 COMERCIAL**

- ✓ Estabelecer procedimentos adequados de identificação dos clientes;
- ✓ Dar o tratamento adequado às informações recebidas e enviadas para clientes, bem como observar o estrito cumprimento das regras de proteção de dados pessoais e outras atribuições que forem pertinentes;
- ✓ Reportar casos suspeitos ou atípicos de solicitações de acessos a dados pessoais por terceiros que não sejam titulares ou de solicitação destes acerca do envio para terceiros não cadastrados/autorizados;
- ✓ Validar, previamente, qualquer solicitação nova de dados pessoais que pretenda solicitar que eventualmente não esteja prevista em políticas internas ou na Lei; e
- ✓ Zelar pela guarda adequada de arquivos físicos e mídias que contenham dados pessoais.

### **9.2 DIRETORIA**

- ✓ Analisar processos internos e identificar riscos ou oportunidades de melhorias em controles internos relacionados à proteção de dados pessoais;
- ✓ Registrar ocorrências ou apontamentos identificados referentes a falhas ou incidentes específicos; e
- ✓ Realizar a revisão periódica desta Política.

### **9.3 ENCARGADO DE DADOS PESSOAIS – DPO**

- ✓ Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- ✓ Receber comunicações da ANPD e adotar providências;
- ✓ Deverá comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
- ✓ Orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- ✓ Executar as demais atribuições determinadas internamente para a empresa na função de controladoras ou operadoras.

#### **9.4 RECURSOS HUMANOS (“RH”)**

- ✓ Realizar o tratamento dos dados pessoais de colaboradores, bem como eventuais candidatos ou banco de talentos;
- ✓ Inserir no cronograma anual e coordenar a realização de treinamentos/campanhas de conscientização acerca de proteção de dados pessoais; e
- ✓ Zelar pela guarda adequada de arquivos físicos e mídias que contenham dados pessoais dos colaboradores.

#### **9.5 TECNOLOGIA (“TI”)**

- ✓ Tomar ações emergenciais preventivas e/ou corretivas em casos de ameaças da integridade dos dados pessoais;
- ✓ Manter eficientes controles de segurança cibernética atualizados;
- ✓ Sugerir melhorias nos procedimentos relacionados ao armazenamento e tratamento de dados pessoais;
- ✓ Auxiliar o DPO na condução das eventuais respostas a incidentes, juntamente com o auxílio das demais áreas necessárias para a resolução do problema;
- ✓ Corrigir e mitigar vulnerabilidades detectadas;
- ✓ Providenciar, quando necessário, a anonimização de dados pessoais e sensíveis; e

- ✓ Zelar pela guarda adequada de arquivos digitais e mídias que contenham dados pessoais.

## **9.6 COLABORADORES EM GERAL**

- ✓ Obedecer fielmente às regras estabelecidas pela presente política, bem como notificar eventuais incidentes de segurança para o DPO;
- ✓ Respeitar os controles e mecanismos de proteção de dados pessoais existentes;
- ✓ Não utilizar, copiar, armazenar ou compartilhar dados pessoais a que tenham acesso sem a devida autorização prévia do DPO; e
- ✓ Zelar pela guarda adequada de arquivos físicos e mídias que contenham dados pessoais.

## **10. CANAIS DE ATENDIMENTO**

A empresa deverá indicar o nome e os detalhes de contato do Encarregado de Proteção de Dados (DPO) e, se aplicável, o representante da empresa.

Este encarregado ou seu representante/ procurador deverá auxiliar a empresa no atendimento aos direitos dos titulares de dados na forma descrita pela legislação.

Os titulares poderão realizar comunicações, solicitações, reclamações e tirar dúvidas enviando um e-mail para o Encarregado de Dados Pessoais – DPO por meio do endereço “[dpo@nsemt.com.br](mailto:dpo@nsemt.com.br)”, ou outro meio idôneo disponibilizado pela empresa para a mesma finalidade, desde que comprovada sua identidade. Alterações dependerão do envio de solicitação para posterior avaliação e adoção de demais providências pela empresa

A empresa deverá ser comunicado imediatamente ou em até 24 (vinte e quatro horas), pelo endereço eletrônico “[dpo@nsemt.com.br](mailto:dpo@nsemt.com.br)” as informações que possam ser relevantes para resolver a solicitação.

## **11. RESPOSTAS A INCIDENTES**

Um processo deverá ser implementado para a notificação e gerenciamento de incidentes que afetem as informações, sensíveis ou não, o qual possa identificar e registrar o tipo de incidente,

data, detecção, quem o notifica, os efeitos dele derivados, data da solução, descrição da solução etc.

Este sistema deverá incluir as recuperações das informações feitas, indicando a pessoa que as executou, os dados restaurados e, quando apropriado, quais dados foram necessários para registrar manualmente no processo de recuperação.

Na eventual ocorrência de um incidente, a pessoa que tomar conhecimento desta situação deverá comunicar o DPO imediatamente, que tomará as providências cabíveis junto à ANPD e da tratativa de solução do caso.

Os incidentes de segurança referentes a dados pessoais, nos termos de sua definição, deverão ser classificados conforme sua relevância e de acordo com (i) a classificação dos dados pessoais e informações envolvidas; e (ii) o impacto na continuidade dos nossos negócios.

O **DPO** deverá comunicar, à ANPD e ao titular, a eventual identificação de ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares e todas as medidas que serão devidamente tomadas, de forma tempestiva pela empresa.

A comunicação será feita em prazo razoável, conforme definido pela Autoridade Nacional, e deverá mencionar, no mínimo<sup>1</sup>:

- ✓ a descrição da natureza dos dados pessoais afetados;
- ✓ as informações sobre os titulares envolvidos;
- ✓ a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- ✓ os riscos relacionados ao incidente;
- ✓ os motivos da demora, no caso de a comunicação não ter sido imediata; e
- ✓ as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Se não for possível fornecer as informações descritas acima simultaneamente, as informações deverão ser fornecidas gradualmente, sem demora injustificada.

---

<sup>1</sup> Referência regulatória: Art. 48 da Lei nº 13.709/2018 (LGPD).

A empresa também dispõe de um linha Fale Conosco, acessível por meio de endereço eletrônico e gerido por empresa terceira especializada para os casos em que o titular não se sinta confortável em se identificar para a realização de denúncias de fatos ou suspeitas relacionadas a qualquer prática ilegal, imprópria ou inadequada. Todas as eventuais denúncias serão tratadas com a devida confidencialidade e há a garantia da faculdade do anonimato ao denunciante.

## **12. AUDITORIA**

A empresa se reserva ao direito de verificar, a qualquer momento, a conformidade com os procedimentos, medidas e controles de segurança exigidos neste instrumento, inclusive por meio de auditorias e testes de segurança em relação a sistemas de informação, comunicações, arquivos, regulamentos legais de proteção de dados pessoais, etc., bem como os procedimentos que suportam a execução dessa política, mediante prévia solicitação por escrito com pelo menos 48 (quarenta e oito) horas de antecedência.

Será disponibilizado a NSE todas as informações necessárias para demonstrar o cumprimento de suas obrigações, bem como para permitir a adequada realização de auditorias ou inspeções empresa ou outro auditor autorizado por ela e apoiar em eventuais consultas à Autoridade supervisora, quando apropriado.

## **13. PROCEDIMENTOS DISCIPLINARES**

Diante da eventual ocorrência de desvios ou eventos de não conformidade com as diretrizes aqui dispostas, penalidades administrativas poderão ser impostas, conforme

No âmbito da responsabilização, a Lei Geral de Proteção de Dados e o Marco Civil da Internet preveem sanções e penalidades graves. Abaixo estão algumas exemplificadas:

- a) Advertência;
- b) Multa de até 10% (dez por cento) do faturamento anual da empresa;
- c) Publicização da infração;
- d) Bloqueio dos dados pessoais a que se refere a infração;

- e) eliminação dos dados pessoais a que se refere a infração;
- f) Suspensão temporária ou proibição do tratamento de dados pessoais;

## 14. 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, demitido de suas funções institucionais, bem como a comunicação, pela empresa, das eventuais violações às autoridades competentes para a responsabilização cível e criminal, quando aplicável.

## 15. 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 ao DPO, que analisará as circunstâncias e fundamentos e submeterá para deliberação da Diretoria.