www.nescred.com.br

POLÍTICA DE GOVERNANÇA DE DADOS PESSOAIS

NESCRED
presente na sua conquista

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/do-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

1. OBJETIVO

Apresentar aos colaboradores da Nescred as diretrizes da proteção aos dados pessoais, além de estabelecer as suas responsabilidades e os limites de atuação em relação aos dados pessoais.

A Diretoria Executiva da Nescred está comprometida e apoia as diretrizes estabelecidas nesta Política, bem como na legislação aplicável, fortalecendo os negócios, as parcerias e as relações com os Titulares dos dados pessoais.

2. ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores da Nescred.

3. DEFINIÇÕES

Agente de Tratamento: O controlador e o operador.

ANPD ou Agência Nacional de Proteção de Dados: Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável.

Ciclo de Vida de Dados Pessoais: Atividades de tratamento compreendidas desde a coleta dos dados pessoais até sua final destinação com expurgo/eliminação segura.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente com a organização.

Compartilhamento de dados pessoais: Comunicação, difusão, transferência nacional ou internacional, interconexão de dados pessoais ou tratamento

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoais, e para uma ou mais modalidades de tratamento.

Comunicação de incidente de segurança: Ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Consentimento: Manifestação livre, informada e inequívoca pela qual o Titular dos dados pessoais concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Controladoria Conjunta: Determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD.

Dado anonimizado: Dado que não identifica de forma direta ou indireta um titular dos dados pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal: Informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os dados pessoais são classificados como Informação Confidencial.

Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.

Encarregado pelo tratamento de dados pessoais: Pessoa física ou jurídica indicada pela Nescred e que atua como canal de comunicação entre Nescred com os Titulares dos dados pessoais ou a ANPD.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

Incidente de segurança: Qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Infração: Descumprimento de obrigação estabelecida na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), e nos regulamentos expedidos pela ANPD.

Legítima expectativa: É a expectativa razoável do titular, que deve ser demonstrada pelo controlador, de que o tratamento de dados pessoais, para a finalidade pretendida, é o esperado em determinada situação concreta.

Medidas de segurança: Medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Operador: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Política de boas práticas e de governança: Normas e processos internos que assegurem o cumprimento abrangente da legislação de proteção de dados pessoais, estabelecidos e implementados pelo agente de tratamento mediante a adoção de regras de boas práticas e de governança.

Suboperador: Contratado pelo Operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do Controlador.

Teste de Balanceamento: Avaliação de proporcionalidade realizada pelo Controlador com base no contexto e nas circunstâncias específicas do tratamento de dados, levando em consideração os impactos e os riscos aos direitos e liberdades dos titulares.

Titular dos dados pessoais: Pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento de Dados Pessoais: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação,

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Transferência Internacional de Dados: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

Violação de Dados Pessoais: Destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

4. PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais da Nescred deve ser regido pelos seguintes princípios:

a) **Finalidade:** Tratar os dados pessoais apenas para as finalidades determinadas, explícitas, legítimas e informadas antes do tratamento, não podendo ser tratados posteriormente para finalidades incompatíveis com essas finalidades.

b) **Adequação:** Tratar os dados pessoais de modo adequado e pertinente às finalidades informadas ao titular, de acordo com o contexto do tratamento.

c) **Necessidade:** Tratar somente os dados pessoais necessários e proporcionais ao alcance de suas finalidades e buscar formas alternativas de se atingir as mesmas finalidades por meios menos invasivos à privacidade do titular dos dados pessoais.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

d) **Livre acesso:** Viabilizar aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

e) **Qualidade dos dados:** Manter a exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

f) **Transparência:** Prestar informações claras, precisas e facilmente acessíveis aos titulares de dados sobre o tratamento de seus dados pessoais e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

g) **Segurança:** Proteger dados pessoais contra o acesso não autorizado ou ilícito, perda, destruição ou dano acidental, com a adoção de medidas técnicas e organizacionais para salvaguardar a integridade, confidencialidade e disponibilidade dos dados pessoais e atender as diretrizes de segurança existentes na Nescred durante todo o ciclo de vida do dado pessoal.

h) **Prevenção:** Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

i) **Não discriminação:** Não tratar os dados pessoais para fins discriminatórios ilícitos ou abusivos.

j) **Responsabilização e prestação de contas:** Demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais e a eficácia dessas medidas.

5. BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS

O tratamento dos dados pessoais, de acordo com a legislação vigente, somente pode ser realizado em caso de:

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

a) Consentimento do titular dos dados pessoais, sendo vedado o tratamento de dados pessoais mediante vício de consentimento;

b) Cumprimento de uma obrigação legal ou regulatória;

c) Formalização de contrato, em que o titular seja parte, ou os seus dados pessoais são necessários para execução de procedimentos preliminares para se firmar o contrato;

d) Exercício regular de direitos em processo judicial, administrativo ou arbitral;

e) Proteção da vida ou da segurança física da pessoa a quem os dados pessoais se referem;

f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) Interesse legítimo da Nescred ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, sendo obrigatória a confecção de Relatório de Impacto à Proteção de Dados Pessoais;

h) Execução de políticas públicas pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

i) Estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

j) Proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento de dados pessoais sensíveis somente pode ser realizado em caso de:

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

i. Consentimento pelo titular ou seu responsável legal, de forma específica e destacada, para finalidades específicas;

ii. Cumprimento de obrigação legal ou regulatória pela Nescred**;**

iii. Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

iv. Proteção da vida ou da incolumidade física do titular ou de terceiro;

v. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

vi. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

6. TRATAMENTO DE DADOS PESSOAIS

Informações da Nescred: A Nescred deverá informar o titular de dados pessoais, com relação ao(a):

a) Qualificação da Nescred e os dados para contato;

b) Finalidade específica do tratamento;

c) Forma e duração do tratamento, observados os segredos comercial e industrial;

d) Informações acerca do uso compartilhado de dados e a finalidade;

e) Responsabilidades dos agentes que realizarão o tratamento;

f) Informação sobre a transferência de dados pessoais para outro país;

g) Direitos do titular; e

h) Identificação do canal de contato do Encarregado pelo Tratamento de Dados Pessoais da Nescred.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

Coleta: A coleta do dado pessoal poderá ser feita por meio de sistemas da informação ligados a sites, aplicativos, recebimento de arquivos, aquisição de base de dados, bem como no ambiente físico como pelo preenchimento de formulários, listas ou pelo registro de uma conversa presencial.

A coleta deve atender ao princípio da necessidade, ou seja, ser limitado ao mínimo de dados necessários para atendimento da finalidade pretendida, de modo proporcional e não excessivo.

Direitos dos titulares de dados: Devem ser recepcionadas e avaliadas as solicitações de direitos do titular com relação aos dados pessoais tratados, como a confirmação da existência do tratamento, acesso aos dados pessoais, correção, revogação de consentimento, portabilidade, anominização, bloqueio e eliminação de dados pessoais.

Respostas às requisições dos titulares: As tratativas e providências quanto às requisições dos titulares dos dados pessoais deverão ser feitas pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio das áreas de negócio da Nescred e serão regidas pelo Procedimento de Resposta às Requisições dos Titulares.

Consentimento: Sempre que o Tratamento tiver como base o consentimento, este consentimento deve ser obtido por meio de uma manifestação livre, informada e inequívoca do titular de dados, de acordo com as finalidades determinadas para o tratamento, podendo ser revogado a qualquer momento pelo titular. Não é permitido o tratamento de dados pessoais mediante vício de consentimento.

Legítimo Interesse: O Tratamento de dados que tiver como base legal o legítimo interesse deverá ser previamente analisado pelo Avaliador e validado junto ao Encarregado da Proteção de Dados Pessoais da Nescred conforme Procedimento para Análise do Legítimo Interesse, sendo recomendada a

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

elaboração do Relatório de Impacto à Proteção de Dados pessoais, nos termos do Procedimento para Elaboração do Relatório de Impacto à Proteção de Dados Pessoais..

Contratos: O Gerente da Área deve assegurar que todas as contratações em que ocorra o tratamento de dados pessoais sejam precedidas de contratos que regulem a privacidade e proteção de dados pessoais.

Avaliação da Proteção de Dados em Terceiros: Nas contratações, renovações ou manutenções de contratos com parceiros ou fornecedores, a Nescred deve aplicar o formulário de avaliação de proteção de dados pessoais para terceiros nos termos do Procedimento de Autoavaliação da Proteção de Dados para Terceiros.

Mapeamento de Dados: Tanto o Controlador como o Operador deverão manter o registro das operações de tratamento de dados pessoais que realizarem, com apoio e orientação do Encarregado pelo Tratamento de Dados Pessoais. .

Armazenamento: O armazenamento dos dados pessoais pode ser feito de modo físico (guarda de crachás, cartões, fichas, papeis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (somente em nuvem ou servidor da Nestlé. Hardwares externos não são permitidos) ou em serviço contratado para esta finalidade), sendo que deve ser assegurada a segurança e a qualidade dos dados, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de tratamento.

Uso: O uso dos dados pessoais deve ser realizado dentro dos limites das finalidades legitimadas na coleta, de acordo com a base legal definida. Caso haja a necessidade de realizar o tratamento do dado pessoal para outra finalidade diversa da informada no momento da coleta, é necessário verificar:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram coletados e a finalidade do novo tratamento;

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

b) O contexto em que os dados pessoais foram tratados (a relação entre o titular dos dados pessoais e a Nescred);

c) Se o dado coletado está sendo compartilhado com demais Agentes de Tratamento;

d) As consequências do novo tratamento para o titular dos dados pessoais, e

e) A existência de medidas de proteção adequada, como criptografia ou pseudonimização.

Essas informações devem ser encaminhadas ao Encarregado pelo Tratamento de Dados Pessoais para que defina se o novo tratamento já está ou não legitimado, e, caso não esteja, ele deve propor as estratégias de como este tratamento pode ser legitimado antes de ser realizado.

Decisões Automatizadas: O tratamento de dados pessoais realizado com base em decisões automatizadas, deve contar com informações claras e adequadas sobre os critérios utilizados para estes tratamentos, e serem disponibilizados aos titulares dos dados pessoais, somente quando solicitado, observando o segredo comercial e industrial.

O titular dos dados pessoais tem o direito de solicitar a revisão de decisão baseada em tratamento automatizado que afetem seus interesses..

Compartilhamento: O compartilhamento de dados pessoais ou de documentos/arquivos que contenham dados pessoais, somente poderá ser feito para Agentes de Tratamento autorizados, observando as medidas de segurança indicadas pelo TI na Política de Segurança da Informação e somente para as finalidades de uso ou tratamento prévia e devidamente informadas e legitimadas junto ao titular dos dados pessoais.

Transferência Internacional: A Nescred deve garantir que todas as transferências internacionais de dados pessoais realizadas estejam em

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

conformidade com as leis e regulamentos aplicáveis, protegendo os direitos e a privacidade dos titulares dos dados.

A Nescred deve aplicar mecanismos de transferência internacional de dados conforme as hipóteses previstas nos incisos I a IX do art. 33 da Lei nº 13.709, de 14 de agosto de 2018 e da Resolução CD/ANPD nº 19/2024.

Manutenção dos dados: Os dados pessoais deverão ser eliminados pela Nescred após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) Cumprimento de obrigação legal ou regulatória pela Nescred;

b) Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

c) Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

d) Uso exclusivo pela Nescred, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Eliminação segura: Após cumprida a finalidade do tratamento e findo o prazo de armazenamento determinado pela Tabela De Temporalidade, os dados devem ser eliminados de modo seguro, independentemente se em meios físicos ou digitais, observando as diretrizes previstas no Procedimento de Descarte Seguro de Informações

Classificação da Informação: Todos os dados pessoais tratados pela Nescred são tratados de acordo com a Norma de Classificação da Informação.

Segurança da Informação: A Nescred deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

As diretrizes de segurança existentes na Política de Segurança da Informação da Nescred, devem ser observadas durante todo o ciclo de vida do dado pessoal.

Incidente de segurança de dados pessoais: Todos os colaboradores têm o dever de notificar a Nescred imediatamente, sem demora injustificada, acerca de qualquer incidente ou tentativa de violação de dados pessoais, confirmado ou sob suspeita, da qual tenham conhecimento, além de cooperar para a investigação e mitigação de incidentes de violação de dados pessoais.

Registro: Todos os procedimentos realizados devem ser documentados pelas partes envolvidas, sob a supervisão do Encarregado pelo Tratamento de Dados Pessoais.

Privacidade desde a Concepção: A Nescred deve incorporar proativamente a privacidade em práticas de negócios, infraestrutura, produtos, serviços, processos ou qualquer outra iniciativa que envolva tratamento de dados pessoais de modo a antecipar e prevenir situações que possam afetar a privacidade do titular.

Relatório de Impacto à Proteção de Dados Pessoais: A Nescred deve manter a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco nos termos do Procedimento de Elaboração do Relatório de Impacto à Proteção de Dados Pessoais.

Treinamento e Conscientização: A Nescred deve estabelecer em nível estratégico, tático e operacional, medidas para treinamento e conscientização em proteção de dados pessoais e segurança da informação para seus colaboradores, terceiros e parceiros de negócio.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

7. RESPONSABILIDADES

7.1. Encarregado pelo Tratamento de Dados Pessoais

a) Apoiar a organização e/ou ministrar treinamentos em proteção de dados pessoais aos colaboradores ou prestadores de serviço, promovendo a cultura de proteção de dados pessoais na Nescred;

b) Elaborar e/ou revisar os procedimentos internos relativos à proteção de dados pessoais e auxiliar na definição de controles para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais;

c) Auxiliar na definição de controles para garantir a existência de registros auditáveis de todo o ciclo de vida dos dados pessoais;

d) Apoiar na resposta aos incidentes de segurança que envolvam dados pessoais e no processo de apuração;

e) Realizar acompanhamento legislativo/regulatório sobre o tema;

f) Orientar as áreas de negócio em caso de mudanças de finalidades de tratamento;

g) Apoiar na manutenção atualizada do mapeamento dos fluxos de dados pessoais;

h) Recomendar os requisitos adequados no caso de transferência de dados entre Agentes de Tratamento, especialmente transferências internacionais;

i) Responder as consultas e apresentar recomendações sobre a aplicação das regras de privacidade junto às áreas de negócios e demais Agentes de Tratamento;

j) Participar no processo de avaliação dos demais Agentes de Tratamento de dados pessoais (aderência e maturidade do tema), quando necessário;

k) Realizar o reporte do Programa de Proteção de Dados à Diretoria;

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

l) Zelar para que os titulares dos dados sejam informados sobre seus direitos, obrigações e responsabilidades sobre a proteção de dados;

m) Avaliar Relatórios de Impacto à Proteção de Dados Pessoais e os Testes de Balanceamento realizados pelas áreas de negócio;

n) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

o) Receber comunicações da Autoridade Nacional e adotar providências;

p) Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outros documentos internos para proteção de dados pessoais na Nescred.

7.2. Comitê de Privacidade

a) Analisar e tomar decisões em relação aos reportes e orientações realizados pelo Encarregado pelo Tratamento de Dados Pessoais;

b) Aprovar e rever periodicamente as políticas, normas e procedimentos de privacidade e segurança da informação da Nescred, sugerindo possíveis alterações, aperfeiçoamentos, esclarecendo dúvidas e deliberando sobre questões não contempladas em normativos relacionados.

7.3. Gerência Administrativa (TI, RH, MKT e Áreas de Negócio)

a) Assegurar que todos os sistemas, serviços e equipamentos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança;

b) Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que a Nescred esteja considerando contratar para processar ou armazenar dados pessoais (exemplos: nuvem, hardware, equipamentos de rede);

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

c) Auxiliar a implementação de procedimentos, controles e rotinas necessárias para o tratamento de dados pessoais;

d) Implementar medidas necessárias e apropriadas para manutenção da confidencialidade, integridade e disponibilidade dos dados pessoais;

e) Promover, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a cultura de proteção de dados pessoais na Nescred , realizando campanhas de capacitação e divulgação da proteção dos dados pessoais;

f) Assegurar a divulgação dos documentos que compõem esta Política e outros documentos internos para proteção de dados pessoais na Nescred;

g) Assegurar que os colaboradores estejam cientes do tratamento realizado aos seus dados pessoais;

h) Definir controles de proteção de dados pessoais especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões);

i) Elaborar, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, campanhas de conscientização e materiais de divulgação e alerta relacionados a proteção de dados pessoais;

j) Analisar e aprovar a forma das comunicações relacionadas à proteção de dados pessoais;

k) Responder, seguindo as orientações do Encarregado pelo Tratamento de Dados Pessoais, eventuais questionamentos de veículos de imprensa.

7.4. Jurídico

a) Auxiliar nos processos de contratação e aquisição de produtos e serviços da Nescred;

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

b) Apoiar o Encarregado pelo Tratamento de Dados Pessoais quanto a possibilidades de tratamento de dados pessoais no exterior, auxiliando no entendimento de validação do nível de proteção de dados pessoais do país destino;

c) Aplicar os mecanismos de transferência internacional em contratos;

d) Fornecer orientação legal na ocorrência de incidentes de violação de dados pessoais.

7.5. Coordenadores

a) Cumprir, fazer cumprir e gerenciar o cumprimento das diretrizes desta Política e seus documentos complementares por parte de seus colaboradores;

b) Assegurar que qualquer dado pessoal só poderá ser recebido, tratado, excluído ou compartilhado por sua Gerência de acordo com as atividades profissionais autorizadas pela Nescred e nos termos desta Política e de seus documentos internos;

c) Identificar e avaliar riscos relacionados à proteção de dados pessoais em suas atividades e propor melhorias;

d) Submeter à análise do Encarregado pelo Tratamento de Dados Pessoais todo novo processo, incluindo novas aplicações, contratações, serviços, produtos, dentre outros, onde houver tratamento de dados pessoais;

e) Assegurar a observação desta Política e da legislação competente pelos parceiros de negócio que recebam dados pessoais enviados por sua Gerência;

f) Ao identificar violações ou incidentes de dados pessoais ou qualquer ação duvidosa, comunicar o Encarregado pelo Tratamento de Dados Pessoais imediatamente.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

7.6. Colaboradores

a) Cumprir as diretrizes desta Política e seus documentos complementares;

b) Tratar os dados pessoais sob responsabilidade da Nescred somente para fins autorizados, de forma ética e legal, respeitando os direitos do titular dos dados pessoais e de acordo com as orientações desta Política, demais instrumentos regulamentares relacionados à proteção de dados pessoais e da legislação aplicável;

c) Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;

d) Reportar formalmente ao Encarregado pelo Tratamento de Dados Pessoais quaisquer eventos relativos à violação ou possibilidade de violação de dados pessoais ou atividades suspeitas de que tiver conhecimento.

8. PENALIDADES

Violações: Qualquer atividade que desrespeite as disposições estabelecidas nesta Política ou em quaisquer dos documentos complementares da Nescred deve ser considerada como uma violação e tratada pela Nescred a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da Nescred visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

9. DISPOSIÇÕES FINAIS

Esta Política deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da Nescred .

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela Nescred **.**

Este documento bem como os demais documentos que a complementam encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Encarregado pelo Tratamento de Dados Pessoais da Nescred

Qualquer dúvida relativa a esta Política deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da Nescred por meio do e-mail protecaodedados11@br.nestle.com

Esta Política entra em vigor na data de sua publicação.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

PROTOCOLO DE AÇÕES

Este é um documento assinado eletronicamente pelas partes, utilizando métodos de autenticações eletrônicas que comprovam a autoria e garantem a integridade do documento em forma eletrônica. Esta forma de assinatura foi admitida pelas partes como válida e deve ser aceito pela pessoa a quem o documento for apresentado. Todo documento assinado eletronicamente possui admissibilidade e validade legal garantida pela Medida Provisória nº 2.200-2 de 24/08/2001.

Data de emissão do Protocolo: 04/12/2025

Dados do Documento

Tipo de Documento	POLÍTICAS_Normativos Internos
Referência Contrato	Nescred_Política de Governança de Dados Pessoais_a
Situação	Vigente / Ativo
Data da Criação	27/11/2025
Validade	27/11/2025 até Indeterminado
Hash Code do Documento	C0272956AFD07C4A0F3AB69DC8A757D83F273D629DB740AA711D90A9CA3CF234

Assinaturas / Aprovações

Papel (parte) Diretoria (Outorgantes Procuração NÃO Eletrônica)
Relacionamento 62.562.012/0001-67 - Nescred

Representante			CPF
Francisco Gonçalves Neto			144.039.528-44
Ação:	Assinado em 01/12/2025 10:49:08 - Forma de assinatura: Usuário + Senha	**IP:**	130.41.103.2
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 Edg/142.0.0.0		
Localização	Latitude: -23.640848/ Longitude: -46.722496		
Tipo de Acesso	Normal		

Representante			CPF
TIAGO CASTILLO E SOUSA			094.209.376-31
Ação:	Assinado em 04/12/2025 08:51:45 - Forma de assinatura: Usuário + Senha	**IP:**	130.41.103.246
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 Edg/142.0.0.0		
Localização	Latitude: -23.628376/ Longitude: -46.743519		
Tipo de Acesso	Normal		

A autenticidade, validade e detalhes de cada assinatura deste documento poderá ser verificada através do endereço http://portal.qualisign.com.br/login/dc-validar, utilizando o código de acesso (passcode) abaixo:

Código de Acesso (Passcode): **56JFV-HDHFD-ODHBQ-WWUVM**

No caso de assinatura com certificado digital também pode ser verificado no site https://validar.iti.gov.br/, utilizando-se o documento original e o documento com extensão .p7s.

Os serviços de assinatura digital deste portal contam com a garantia e confiabilidade da **AR-QualiSign**, Autoridade de Registro vinculada à ICP-Brasil.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM

Validação de documento não armazenado no Portal QualiSign

Caso o documento já tenha sido excluído do Portal QualiSign, a verificação poderá ser feita conforme a seguir;

a.) Documentos assinados exclusivamente com Certificado Digital (CADES)

A verificação poderá ser realizada em http://portal.qualisign.com.br/login/dc-validar, desde que você esteja de posse do documento original e do arquivo que contém as assinaturas (.P7S). Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

b.) Documentos assinados exclusivamente com Certificado Digital (PADES)

Para documentos no formato PDF, cuja opção de assinatura tenha sido assinaturas autocontidas (PADES), a verificação poderá ser feita a partir do documento original (assinado), utilizando o Adobe Reader. Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

c.) Documentos assinados exclusivamente SEM Certificado Digital ou de forma híbrida (Assinaturas COM Certificado Digital e SEM Certificado Digital, no mesmo documento)

Para documento híbrido, as assinaturas realizadas COM Certificado Digital poderão ser verificadas conforme descrito em (a) ou (b), conforme o tipo de assinatura do documento (CADES ou PADES).

A validade das assinaturas SEM Certificado Digital é garantida por este documento, assinado e certificado pela QualiSign.

Validade das Assinaturas Digitais e Eletrônicas

No âmbito legal brasileiro e em também em alguns países do Mercosul que já assinaram os acordos bilaterais, as assinaturas contidas neste documento cumprem, plenamente, os requisitos exigidos na Medida Provisória 2.200-2 de 24/08/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e transformou o ITI – Instituto Nacional de Tecnologia da Informação em autarquia garantidora da autenticidade, integridade, não-repúdio e irretroatividade, em relação aos signatários, nas declarações constantes nos documentos eletrônicos assinados, como segue:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º. As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2º. O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Pelo exposto, o presente documento encontra-se devidamente assinado pelas Partes, mantendo plena validade legal e eficácia jurídica perante terceiros, em juízo ou fora dele.

Documento assinado eletronicamente. Verificação em http://portal.qualisign.com.br/login/dc-validar através do código 56JFV-HDHFD-ODHBQ-WWUVM