POLÍTICA DE PRIVACIDADE

Dezembro/2024

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor	Aprovação
19/12/2024	V1.0	Primeira versão da Política de Privacidade.	Equipe Técnica de Elaboração	Deborah Montenegro e Alexandre de Abreu e Silva

SUMÁRIO

POLÍTICA DE PRIVACIDADE DO SENAC GOIÁS

1. INTRODUÇÃO

A Política de Privacidade Interna do Senac Goiás estabelece as diretrizes e práticas para o tratamento de dados pessoais no âmbito de suas atividades, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Este documento tem como objetivo orientar os colaboradores, prestadores de serviços e parceiros sobre a importância da proteção de dados pessoais, garantindo que todas as operações de tratamento sejam realizadas de maneira ética, segura e alinhada às melhores práticas de governança de privacidade.

O Senac Goiás reconhece a importância da privacidade como um direito fundamental e reafirma seu compromisso em adotar medidas que assegurem a integridade, confidencialidade e disponibilidade dos dados pessoais sob sua responsabilidade. Este compromisso reflete não apenas o cumprimento das exigências legais, mas também a busca pela confiança dos titulares de dados e a excelência em suas operações.

2. OBJETIVOS

Esta Política tem como principais objetivos:

i. **Garantir a conformidade com a legislação vigente:** Estabelecer procedimentos e diretrizes que assegurem o cumprimento integral da LGPD e de outras normas aplicáveis relacionadas à proteção de dados pessoais.

ii. **Orientar colaboradores e parceiros:** Fornecer orientações claras sobre as práticas e responsabilidades no tratamento de dados pessoais, promovendo uma cultura de privacidade e segurança no ambiente organizacional.

iii. **Proteger os direitos dos titulares de dados:** Garantir que os titulares de dados tenham seus direitos respeitados, incluindo a transparência no tratamento, o acesso às informações e a possibilidade de correção ou exclusão de seus dados quando aplicável.

iv. **Prevenir riscos e incidentes de privacidade:** Implementar controles e medidas que minimizem riscos de acessos não autorizados, vazamentos, perda ou uso inadequado de dados pessoais.

v. **Promover a conscientização:** Engajar colaboradores, parceiros e fornecedores sobre a importância da proteção de dados, criando um ambiente colaborativo e comprometido com a privacidade.

Esta Política é um instrumento essencial para guiar as operações do Senac Goiás no tratamento de dados pessoais, reforçando o compromisso da organização com a transparência, a ética e o respeito aos direitos de todas as partes envolvidas.

3. DEFINIÇÕES

- **LGPD**: Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- **Dados pessoais**: informações relacionadas à pessoa natural que possibilitem sua identificação, direta (exemplos: nome, RG e CPF) ou indiretamente (exemplos: nacionalidade, profissão, interesses específicos).
- **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 natural.
- **Titular de dados**: pessoa natural a quem se referem os dados pessoais objeto de tratamento.
- **Agentes de tratamento:** controlador e operador.
    - **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
    - **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador e nos limites por ele estabelecidos.

      A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores).
- **Encarregado**: profissional indicado para atuar como canal de comunicação com qualquer titular de Dados Pessoais e com as autoridades governamentais competentes, em especial, a Autoridade Nacional de Proteção de Dados (ANPD).
- **Autoridade Nacional de Proteção de Dados (ANPD)**: órgão da administração pública federal do Brasil responsável por implementar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar o cumprimento da LGPD e aplicar sanções em caso de tratamento irregular de dado pessoal. Fonte: https://www.gov.br/anpd/pt-br
- **Tratamento de dados**: toda operação realizada com dados pessoais, como as que se referem a:
    - **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade

de usar os ativos de informação de um órgão ou entidade, observada eventual restrição aplicável;

- **Armazenamento**: ação ou resultado de manter ou conservar um dado para consultas periódicas;
- **Arquivamento**: ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a vigência para utilização;
- **Avaliação**: analisar o dado com o objetivo de produzir outras informações;
- **Classificação**: maneira de ordenar os dados conforme algum critério estabelecido e para alguma finalidade específica;
- **Coleta**: recolhimento de dados com finalidade específica;
- **Comunicação**: transmitir informações pertinentes aos dados para que seja traçado um plano de ação;
- **Controle**: ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- **Difusão**: ato ou efeito de divulgação, propagação, multiplicação dos dados;
- **Distribuição**: ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- **Eliminação**: ato ou efeito de excluir ou destruir dado de onde ele está armazenado;
- **Extração**: ato de copiar ou retirar dados do armazenamento em que se encontrava;
- **Modificação**: ato ou efeito de alteração do dado;
- **Processamento**: ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
- **Produção**: criação de bens e de serviços a partir do tratamento de dados;
- **Recepção**: ato de receber os dados ao final da transmissão;
- **Reprodução**: cópia de dado preexistente obtido por meio de qualquer processo;
- **Transferência**: mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- **Transmissão**: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos etc.;
- **Utilização**: ato ou efeito do aproveitamento dos dados.

- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

- **Anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento para dissociar um dado pessoal de um indivíduo, **em caráter irreversível**, de modo que seu titular não possa mais ser identificado, direta ou indiretamente.
- **Criptografia:** é a conversão de dados de um formato legível para um formato codificado, conferindo segurança e confidencialidade. Uma vez criptografados, os dados só podem ser lidos ou processados após serem descriptografados, o que só pode ser feito por quem detém uma chave específica.
- **Decisão automatizada**: procedimento de classificação, avaliação, mapeamento de perfil, aprovação ou rejeição desenvolvido sem intervenção humana a partir do processamento eletrônico de dados com base em regras, instruções e algoritmos.

4. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

O Senac Goiás, na qualidade de Controlador de Dados Pessoais e em conformidade com o artigo 41 da LGPD, designou **Franklin Silva de Castro Bonfim** para atuar como Encarregado pelo Tratamento de Dados Pessoais ("*Encarregado*"), para dentre outras atribuições:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber/Realizar comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;
- Orientar os colaboradores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Assegurar que a Política de Privacidade e documentos correlatos sejam analisados e atualizados periodicamente, ou quando se fizer necessário;
- Monitorar as atividades de privacidade e proteção de dados dentro na empresa; dentre outras atribuições previstas em documentos internos.

Posto isto, para eventuais solicitações, dúvidas, sugestões ou reclamações, o titular ou profissional do Senac Goiás poderá entrar em contato direto com o Encarregado pelo seguinte canal de comunicação: dpo@go.senac.br.

5. INFORMAÇÕES SOBRE TRATAMENTO DE DADOS PESSOAIS

Considerando que **tratamento de dados** é toda operação ou atividade realizada com dados pessoais, conforme o artigo 5º, inciso X, da LGPD, no âmbito do Senac Goiás, o ciclo de vida dos dados pessoais compreende todas as etapas de tratamento realizadas, desde a coleta inicial até a eliminação final, sempre em conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018)** e suas regulamentações. As etapas do ciclo de vida são descritas abaixo, com suas respectivas responsabilidades e diretrizes de segurança:

- **Coleta:** A coleta de dados pessoais é a etapa inicial do ciclo de vida, onde as informações necessárias são obtidas para viabilizar finalidades específicas, como:
  - Contratação de serviços e atendimento aos clientes;
  - Processos seletivos e contratação de colaboradores;
  - Cumprimento de obrigações legais e regulatórias.

  Somente dados estritamente necessários devem ser coletados, respeitando o princípio da minimização de dados (*ver item 5.1*)**.**

- **Processamento:** Após a coleta, os dados são organizados e armazenados em sistemas ou servidores internos, permitindo que sejam acessados e utilizados de forma estruturada para finalidades específicas. Durante esta etapa:
  - Deve-se garantir que os dados sejam processados de forma precisa e consistente;
  - Sistemas de gestão interna devem seguir padrões de segurança e confidencialidade.

- **Análise:** A análise de dados pessoais ocorre para verificar e validar informações necessárias para atingir uma finalidade específica ou gerar novos dados com base nos já existentes. Durante esta etapa, é fundamental:
  - Garantir que apenas os dados estritamente necessários sejam utilizados;
  - Manter a conformidade com os princípios da LGPD, especialmente o de finalidade e transparência**.**

- **Compartilhamento:** O compartilhamento de dados pessoais será realizado somente nas seguintes hipóteses:
  - Exigências legais ou regulatórias;
  - Exercício regular de direitos em processos judiciais, administrativos ou arbitrais;

- Execução de contratos com os titulares de dados;
- Apoio na prestação de serviços com provedores confiáveis e contratados;
- Garantia da segurança dos dados ou de operações institucionais.

O compartilhamento de dados com terceiros deve ser devidamente documentado e estar vinculado a uma finalidade legítima e informada ao titular, conforme os princípios de necessidade e transparência.

Assim, o Senac Goiás realiza o compartilhamento de dados com os seguintes agentes de tratamento:

- Governo Federal e Receita Federal;
- Ministério do Trabalho e Emprego;
- Departamento Nacional do Senac;
- Tribunal de Contas da União;
- E-Social;
- INSS;
- Instituições Financeiras;
- Operadoras de planos de saúde;
- Sindicatos;
- Provedores de sistema de segurança interno;
- Escritórios de advocacia e contabilidade terceirizados.

➢ **Armazenamento:** Os dados pessoais coletados e processados são armazenados em sistemas internos ou externos, devendo observar rigorosas medidas de segurança, como:

- Controle de acesso;
- Autenticação de dois fatores;
- Monitoramento contínuo de vulnerabilidades.

O armazenamento será mantido somente pelo período necessário às finalidades estabelecidas, respeitando as políticas de retenção e eliminação.

➢ **Eliminação:** A eliminação é a etapa final do ciclo de vida, que consiste no descarte seguro dos dados pessoais após o término de sua finalidade ou período de retenção (ver item 6.1.2.). Os procedimentos incluem:

- Destruição de documentos físicos por picotadoras ou incineração;
- Exclusão definitiva de arquivos digitais em sistemas, dispositivos e *backups*;
- Registro das operações de eliminação como evidência.

➢ **Conformidade e Outras Formas de Tratamento**

Outras formas de tratamento de dados pessoais poderão ser realizadas, conforme as finalidades específicas previstas na LGPD. Em qualquer caso, o ciclo de vida deve ser integralmente seguido, e os responsáveis devem adotar práticas alinhadas às exigências legais para evitar sanções administrativas e danos à reputação institucional.

6. PRINCÍPIOS FUNDAMENTAIS

Os princípios previstos no artigo 6º da Lei nº 13.709/2018 (LGPD) são fundamentos essenciais para orientar o tratamento de dados pessoais, funcionando como normas obrigatórias que devem ser rigorosamente aplicadas a cada situação concreta. Para garantir a conformidade com a LGPD, é imprescindível que todos os colaboradores do Senac Goiás compreendam, respeitem e integrem esses princípios em suas atividades profissionais diárias, promovendo uma cultura de proteção de dados e privacidade.

6.1. PRINCÍPIO DA FINALIDADE DO TRATAMENTO

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Este princípio assegura que o tratamento seja realizado de forma transparente e ética, alinhado aos interesses legítimos do Senac Goiás e dos titulares de dados. Conforme o referido artigo, o princípio da finalidade estabelece que:

- **Propósitos Legítimos:** O tratamento de dados deve estar fundamentado em bases legais previstas pela LGPD, como o consentimento do titular, a execução de contratos, o cumprimento de obrigações legais ou outras hipóteses autorizadas pela legislação (item 6.1.1.). Qualquer tratamento que não tenha respaldo legal é considerado incompatível com este princípio.
- **Propósitos Específicos:** As finalidades do tratamento devem ser claramente definidas antes da coleta dos dados, garantindo que:
  - O motivo do tratamento seja compatível com o objetivo informado inicialmente;
  - Todo tratamento posterior à coleta respeite e esteja alinhado com as finalidades originais.
- **Propósitos Informados ao Titular:** O Senac Goiás deve comunicar aos titulares:
  - A finalidade da coleta e o motivo pelo qual seus dados serão tratados;
  - Como os dados serão utilizados, armazenados e protegidos;
  - O período pelo qual os dados serão mantidos;
  - A possibilidade de compartilhamento com terceiros, se aplicável.

Essas informações devem ser transmitidas de forma clara e acessível, por meio de:

i. Cláusulas contratuais;
ii. Avisos de Privacidade direcionados ao público externo;
iii. Orientações específicas para colaboradores e operadores.

A responsabilidade pela comunicação aos titulares recai sobre a alta direção, colaboradores e operadores envolvidos no processo de tratamento de dados. É essencial que os esclarecimentos sejam fornecidos de maneira proativa e consistente, demonstrando o compromisso do Senac Goiás com a transparência e o respeito aos direitos dos titulares.

6.1.1. LIMITAÇÃO DO TRATAMENTO ÀS BASES LEGAIS

O tratamento de dados pessoais no Senac Goiás deve estar estritamente fundamentado em uma ou mais das bases legais previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a legitimidade e a conformidade com a legislação aplicável.

Assim, os tratamentos de dados pessoais realizados deverão sempre estar amparados por alguma das bases legais previstas na Lei Geral de Proteção de Dados que incluem:

- **Art. 7º, LGPD:** Aplicável a dados pessoais gerais, como nome, endereço, e-mail, entre outros.
- **Art. 11, LGPD:** Aplicável a dados pessoais sensíveis 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.
- **Art. 14, LGPD, e Enunciado CD/ANPD nº 1/2023:** Aplicável ao tratamento de dados de crianças e adolescentes. Neste caso, o tratamento poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), conforme autorização da ANPD, mas desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto. Caso contrário deverá ser realizado mediante consentimento específico e em destaque por parte dos responsáveis legais, nos termos do art. 14 da Lei.

As bases legais para cada atividade de tratamento serão definidas pelo Encarregado de Dados. Contudo, todos devem observar em suas atividades diárias. As principais bases utilizadas nas atividades do Senac Goiás são:

- **Cumprimento de Obrigação Legal ou Regulatória**: utilizada quando o tratamento do dado decorre de exigências normativas. Exemplo:
    - Compartilhamento de dados com e-Social: CLT e Decreto 8.373/2014;
    - Coleta de dados para controle de jornada: art. 74, §2º da CLT e Portaria 1510/2009 do Ministério do Trabalho;
    - Coleta e registro de acidentes: NR5 do Ministério do Trabalho; Evento E-social 2210 e Normas do INSS;
    - Coleta e registro de atestados médicos dos colaboradores: NR7 do Ministério do Trabalho e CLT, arts.168 e 169.
- **Execução ou Preparação de um Contrato**: utilizada quando o tratamento do dado é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, tais como:

- Contrato com Clientes;
- Recrutamento e Seleção de novos colaboradores;
- Contrato de Trabalho;
- Contrato com fornecedores e prestadores de serviços.

- **Exercício Regular de Direitos**: utilizada quando o tratamento do dado é necessário para permitir o exercício regular de direitos em processo judicial, administrativo ou arbitral, preservando os dados pelo período prescricional necessário, a fim de garantir ao Senac Goiás meios hábeis à sua defesa.
- **Legítimo Interesse**: A base legal do legítimo interesse poderá ser utilizada para proteger ou promover interesses próprios do Senac Goiás, contudo só será utilizada quando houver expressa motivação da finalidade e necessidade do tratamento, como ocorre, por exemplo, na captura de imagens internas por câmeras de vídeo segurança. Neste caso cumpre ressaltar que: (i) os dados pessoais utilizados serão apenas os estritamente necessários para a finalidade pretendida; (ii) o tratamento deve observar e garantir o princípio da transparência; e (iii) deve respeitar as legítimas expectativas do titular quanto ao uso e tratamento de seus dados no instante em que foram coletados.
- **Consentimento**: Alguns tratamentos de dados pessoais exigem o consentimento expresso dos titulares dos dados autorizando o tratamento para finalidades específicas. Neste caso, o consentimento deverá ser dado de forma livre, informada, inequívoca e específica, devendo observar que:
  - O consentimento deverá ser fornecido por escrito em documento apartado (Termo de Consentimento);
  - As informações devem ser dadas de forma clara, objetiva e transparente, de modo a não deixar dúvidas para o titular;
  - O consentimento deve ser coletado para finalidades específicas de tratamento;
  - Deve constar a forma e duração do tratamento;
  - Deve constar identificação e contato do Encarregado pelo tratamento de dados;
  - Informar as responsabilidades dos agentes que realizarão o tratamento;
  - Informar os direitos do titular quanto à confirmação do tratamento, acesso, atualização, retificação, dentre outros que se fizerem necessários;
  - Caso ocorra mudança da finalidade do tratamento, deixando de ser compatível com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade;

- Caso o titular opte por revogar o consentimento em qualquer momento, o Senac Goiás ficará impedido de tratar os dados pessoais e, consequentemente, será obrigado a interromper o serviço decorrente do consentimento.

Em decorrência de todo o exposto, para garantir a conformidade e minimizar riscos, recomenda-se que todos os formulários utilizados para coleta de dados pessoais sejam previamente submetidos à aprovação do Encarregado de Dados. Essa etapa de aprovação visa assegurar que os dados coletados sejam restritos ao mínimo necessário e que estejam devidamente alinhados às finalidades legítimas e específicas.

6.1.2. RETENÇÃO E DESCARTE DE DADOS

Os dados pessoais coletados serão mantidos exclusivamente:

i. pelo período necessário para cumprir as finalidades informadas ao titular;
ii. para atender a obrigações legais; ou
iii. para possibilitar o exercício regular de direitos.

O prazo de retenção aplicável a cada categoria de dados está detalhado na Tabela de Temporalidade desta Política de Privacidade (Anexo I).

Ao término do prazo de retenção, os dados pessoais deverão ser descartados de forma segura e irreversível, conforme descrito abaixo:

- Dados Físicos: Devem ser destruídos por métodos seguros, como trituração ou incineração, garantindo a irreversibilidade do descarte.
- Dados Digitais: Devem ser excluídos de sistemas, dispositivos e backups por meio de processos que assegurem a exclusão definitiva e irreversível.
- Equipamentos eletrônicos: o descarte deverá ser realizado em conformidade com a Política Nacional de Resíduos Sólidos e outras regulamentações vigentes. Nas hipóteses em que o equipamento estiver em estado de funcionamento e for possível o acesso ao mesmo, o departamento de tecnologia da informação realizará os seguintes procedimentos antes do descarte:
  - Celulares: Desvincular a conta de seu usuário, apagar todos os dados através de restauração do sistema e retirar o chip.
  - Computadores: Proceder com a formatação completa do HD, todos os dados devem ser apagados de forma segura e efetiva, utilizando-se de meios que não permita a conversão dos dados apagados.
  - O mesmo se aplica aos dados e softwares licenciados armazenados em mídias de

armazenamento móvel (por exemplo, em papel, em CD, DVD, pen drive USB, cartão de memória, token de certificado digital etc.), todos devem ser apagados de forma segura, a mídia deve ser destruída antes de ser descartada.

Todas as ações de descarte devem ser realizadas imediatamente após o fim do prazo estabelecido, garantindo a devida documentação e rastreabilidade dessas operações para fins de auditoria e conformidade com a legislação aplicável.

Adicionalmente, caso haja operadores envolvidos no tratamento do conjunto de dados a ser descartado, eles deverão ser notificados para que realizem a exclusão em suas respectivas estruturas, assegurando a integridade do processo de descarte.

6.2. PRINCÍPIO DA MINIMIZAÇÃO NO TRATAMENTO DE DADOS PESSOAIS

Necessidade: limitação do tratamento 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.

O princípio da minimização no tratamento de dados pessoais visa restringir o tratamento de dados ao estritamente necessário para o cumprimento da finalidade pretendida, evitando a coleta, retenção ou uso excessivo de informações. Nesse sentido, para a aplicação eficaz do princípio deve-se observar:

- **Coleta Restritiva:** A coleta de dados pessoais deve ser conduzida de forma criteriosa, buscando exclusivamente as informações essenciais para atender a finalidade da operação ou atividade. Qualquer dado que não seja diretamente necessário para a execução da finalidade deve ser evitado.
- **Proporcionalidade e Pertinência:** Os dados tratados devem ser proporcionais e adequados ao objetivo para o qual foram coletados. Isso significa que não é permitido tratar dados irrelevantes ou desnecessários, mesmo que estejam disponíveis.
- **Uso e Retenção Controlados:** Os dados pessoais não devem ser retidos ou reutilizados para finalidades distintas daquelas previamente informadas ao titular, a menos que:
  - O novo uso seja essencial e esteja dentro dos limites legais;
  - Haja consentimento expresso ou outro fundamento legal que permita tal tratamento.

Em resumo, o princípio da minimização exige que o Senac Goiás adote práticas de coleta e tratamento que priorizem o uso responsável e restrito dos dados pessoais, garantindo que cada operação respeite os limites estabelecidos pela LGPD e as expectativas de privacidade dos titulares.

6.3. PRINCÍPIO DA ADEQUAÇÃO

Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

De acordo o princípio da adequação, é indispensável que:

- O tratamento de dados seja realizado exclusivamente para os fins declarados no momento da coleta.
- Qualquer nova finalidade, não prevista originalmente, seja informada ao titular e, quando necessário, autorizada mediante consentimento prévio.
- As práticas de tratamento respeitem os limites do que é razoavelmente esperado pelo titular, evitando usos que possam surpreendê-lo ou violar sua confiança.

Exemplo Prático: Se dados pessoais forem coletados para fins de cadastro, como nome e e-mail, essas informações não podem ser utilizadas para enviar publicidade sem o consentimento explícito do titular. Qualquer desvio de finalidade configura uma violação do princípio da adequação.

6.4. PRINCÍPIO DO LIVRE ACESSO

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

Esse princípio estabelece que os titulares devem ter acesso às seguintes informações de maneira objetiva e de fácil entendimento:

I. Os dados pessoais que estão sendo tratados: Detalhamento sobre quais informações estão em posse do Senac Goiás e sob que contexto foram coletadas.

II. A finalidade e o fundamento jurídico do tratamento: Explicação sobre os motivos que justificam o uso dos dados, alinhados às bases legais previstas na LGPD.

III. O período de retenção dos dados: Clareza sobre o tempo em que os dados serão armazenados, considerando a necessidade e a finalidade do tratamento.

IV. Os agentes de tratamento envolvidos: Identificação de quais agentes, sejam internos ou externos, têm acesso aos dados e de que maneira eles os utilizam.

Ao garantir o livre acesso, o titular pode exercer maior controle sobre seus dados, assegurando que o tratamento seja realizado de forma adequada e em conformidade com a legislação vigente. Além disso, essa transparência reforça a confiança nas operações conduzidas pelo Senac Goiás.

.

6.5. PRICÍPIO DA QUALIDADE DOS DADOS

Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Esse princípio enfatiza a responsabilidade do Senac Goiás em conduzir o tratamento de dados pessoais de maneira eficiente e em estrito respeito aos direitos dos titulares. Para isso, o Senac Goiás, por meio de seus colaboradores, deve adotar as seguintes práticas:

- Garantir a correção e consistência dos dados pessoais: É imprescindível assegurar que os dados tratados estejam corretos, livres de erros e devidamente validados no momento da coleta. Práticas rigorosas devem ser implementadas para evitar a inclusão de informações incorretas.
- Promover a atualização periódica das informações: Dados desatualizados podem comprometer a eficácia do tratamento e causar prejuízos ao titular. Assim, é necessário adotar processos regulares de revisão e atualização das informações armazenadas.
- Assegurar a clareza das informações: O tratamento dos dados deve ser realizado de forma transparente e compreensível, garantindo que todas as partes envolvidas possam interpretar as informações de maneira objetiva.
- Disponibilizar mecanismos acessíveis para atualização de dados pelos titulares: O Senac Goiás deve oferecer canais simples e eficientes para que os titulares possam corrigir ou atualizar suas informações diretamente ou por meio de solicitação formal.

Exemplo Prático: Caso um aluno do Senac Goiás altere seu endereço ou telefone, é essencial que essa atualização seja refletida nos sistemas institucionais. Dados desatualizados podem levar a erros operacionais, como falhas na comunicação ou envio de documentos para o local errado.

6.6. PRINCÍPIO DA TRANSPARÊNCIA

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

De acordo com esse princípio, as informações fornecidas aos titulares devem ser objetivas, detalhadas e compreensíveis, evitando o uso de linguagem técnica ou ambígua. Essas informações devem estar disponíveis por meio de canais acessíveis e variados, tais como, Avisos de Privacidade, Contratos, Termos de Consentimento e ferramentas online para consulta e atualização de dados pessoais. É fundamental que o titular tenha a possibilidade de consultar essas informações de forma simples e ágil.

Embora a transparência reforce a necessidade de detalhamento, é essencial equilibrar essa exigência com a proteção de informações sensíveis relacionadas aos processos internos das organizações. Esse cuidado assegura a confidencialidade necessária, ao mesmo tempo em que atende às obrigações de transparência previstas na legislação.

6.7. PRINCÍPIO DA SEGURANÇA

Segurança: utilização de medidas 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 difusão.

Para cumprir o princípio da segurança, é essencial a adoção de práticas e controles robustos, incluindo:

- Medidas Técnicas: Implementação de tecnologias como criptografia, *firewalls*, controle de acesso baseado em funções, *backups* regulares e sistemas de monitoramento para prevenir e detectar violações de segurança.
- Medidas Administrativas: Desenvolvimento de políticas e procedimentos internos claros, treinamento regular das equipes envolvidas no tratamento de dados, auditorias de conformidade e definição de responsabilidades no manejo das informações.
- Gerenciamento de Riscos: Realização de análises regulares de riscos para identificar vulnerabilidades e implementar soluções proativas.

Além disso, a segurança dos dados deve ser contínua e adaptável, acompanhando as evoluções tecnológicas e as mudanças nos padrões de ameaças.

É responsabilidade de todos zelar pela proteção e privacidade dos dados pessoais, com especial atenção aos dados pessoais sensíveis. Para garantir a aplicação correta das normas no dia a dia, todos os colaboradores deverão participar dos treinamentos sobre privacidade e proteção de dados oferecidos pelo Senac Goiás, adquirindo o conhecimento necessário para atuar em conformidade com as diretrizes estabelecidas.

6.8. PRINCÍPIO DA PREVENÇÃO

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Pelo princípio da prevenção cada colaborador precisa adotar medidas proativas para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais, seja para os titulares dos dados ou para a instituição que é responsável pelo tratamento.

Esse princípio reforça a necessidade de implementar práticas e controles que minimizem os riscos associados ao uso inadequado, à exposição ou ao mau gerenciamento de dados pessoais. As principais ações incluem:

- Identificação de riscos: Caso o colaborador identifique potenciais vulnerabilidades nos processos de tratamento de dados, deve comunicar imediatamente a Gerência de tecnologia e o Encarregado de Dados.
- Políticas e procedimentos: Observar diretrizes internas que orientem o tratamento de dados, garantindo que todas as etapas sejam realizadas de maneira segura e responsável.
- Treinamento e conscientização: Participar de todos os treinamentos sobre práticas seguras, riscos e a importância de prevenir danos.

Cabe ainda ao Senac Goiás:

- Monitoramento contínuo: Implementar sistemas de controle e auditoria para identificar e corrigir eventuais falhas antes que possam causar prejuízos.
- Resposta a incidentes: Planejar e testar protocolos para resposta imediata em caso de incidentes, visando mitigar danos e evitar recorrências.

Exemplo Prático: No Senac Goiás, ao coletar dados de candidatos para cursos, a organização pode prevenir danos adotando práticas como a validação de formulários para evitar o recebimento de informações

incorretas ou sensíveis. Além disso, o armazenamento em ambientes seguros e a limitação de acesso apenas a pessoal autorizado contribuem para evitar vazamentos ou acessos indevidos.

6.9. PRINCÍPIO DA NÃO DISCRIMINAÇÃO

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

O princípio da não discriminação assegura que o tratamento de dados pessoais jamais seja utilizado para fins discriminatórios, ilícitos ou abusivos, garantindo a igualdade e o respeito aos direitos fundamentais dos titulares.

Este princípio exige que o Senac Goiás, por meio de seus colaboradores, trate os dados pessoais com neutralidade, sem causar prejuízos ou favorecimentos indevidos com base em características pessoais, como origem racial ou étnica, religião, opinião política, gênero, orientação sexual, ou qualquer outro atributo protegido pela lei.

Exemplo Prático: Durante o processo de seleção para bolsas de estudo, o Senac Goiás adota rigorosos padrões de transparência e imparcialidade. A coleta e o tratamento de dados pessoais dos candidatos são conduzidos exclusivamente com base nos critérios previamente estabelecidos, como renda familiar e desempenho acadêmico, conforme diretrizes do Programa Senac de Gratuidade (PSG). Essas práticas asseguram que as decisões sejam livres de qualquer forma de discriminação, seja por raça, religião, gênero, orientação sexual ou qualquer outro fator que não esteja diretamente relacionado aos critérios objetivos definidos para o programa.

6.10. PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Este princípio exige que o Senac Goiás esteja preparado para comprovar, a qualquer momento, a observância e o cumprimento das normas de proteção de dados pessoais e que tais medidas eficazes. Esse princípio enfatiza a transparência e a proatividade no tratamento de dados, por meio de:

- Documentação detalhada: Registro de todas as práticas e processos relacionados ao tratamento de dados pessoais, incluindo políticas, procedimentos e auditorias internas.

- Implementação de controles eficazes: Adoção de medidas técnicas e organizacionais que assegurem a proteção de dados, como políticas de segurança, avaliação de impacto à proteção de dados (AIPD) e governança de dados.
- Relatórios e auditorias regulares: Monitoramento contínuo das atividades de tratamento, com auditorias periódicas que comprovem a conformidade e a eficácia das medidas adotadas.
- Treinamento e conscientização: Capacitação das equipes envolvidas no tratamento de dados para assegurar a compreensão e o cumprimento das obrigações legais.
- Disponibilidade para fiscalização: Manutenção de registros organizados e acessíveis para demonstração de conformidade perante órgãos fiscalizadores, como a ANPD (Autoridade Nacional de Proteção de Dados).

Esse princípio, mais uma vez reforça a importância e necessidade de cada colaborador observar as regras institucionais sobre proteção e privacidade de dados.

7. DIRETRIZES GERAIS

Esta Política de Privacidade é de cumprimento obrigatório para a alta direção e todos os colaboradores do Senac Goiás. Para garantir a sua efetividade, é essencial que:

i. Todos leiam de forma atenciosa a presente Política de Privacidade a fim de compreender como os dados pessoais devem ser tratados, os princípios a serem observados durante o tratamento e quais bases legais autorizam o tratamento.

ii. Todos participem dos treinamentos realizados no que tange a proteção e privacidade dos dados. Os treinamentos visam garantir que todos conheçam os seus direitos como titulares de dados, bem como, que estejam aptos à aplicação das normas internas e proteção dos dados de terceiros. Ademais, será um momento oportuno para sanar dúvidas.

iii. Todos atuem com as diligências necessárias a fim de garantir que os dados pessoais estão sendo tratados de forma segura e protegidos contra sua perda, eliminação ou dano acidental, sendo organizados adequadamente para manter a integridade e confidencialidade.

iv. Informar imediatamente o departamento de tecnologia da informação (TI) e o Encarregado de dados em caso de perda, eliminação ou dano acidental envolvendo dados pessoais para que todas as medidas de remediação cabíveis sejam tomadas.

v. Informar imediatamente o Encarregado de dados conhecimento ou razoável suspeita de violação ou inobservância desta Política de Privacidade para que este possa realizar as ações de

conformidade necessárias.

8. PAPÉIS E RESPONSABILIDADES

8.1. ALTA DIREÇÃO

- Aprovar esta Política e outros documentos correlatos;
- Cumprir e fazer cumprir a Política de Privacidade;
- Assegurar recursos adequados para implementar as diretrizes;
- Tomar medidas corretivas em casos de desconformidades;
- Promover a cultura em segurança da informação e privacidade;
- Conhecer e tomar as medidas necessárias nos casos de incidentes de segurança, que porventura vierem a ocorrer.

8.2. CONFORMIDADE

- Debater os temas relativos à segurança, proteção e privacidade dos dados;
- Cumprir e fazer cumprir a Política de Privacidade;
- Facilitar a identificação das obrigações legais de proteção e privacidade de dados pessoais;
- Documentar a avaliação dos riscos de privacidade;
- Acompanhar a implantação das ações corretivas oriundas de não conformidades identificadas;
- Assegurar que a Política de Privacidade e demais políticas correlatas se mantenham sempre atualizadas;
- Prover aconselhamento sobre assuntos relacionados a conformidade.

8.3. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

- Cumprir e fazer cumprir a Política de Privacidade;
- Garantir a publicidade dos documentos de privacidade de dados pessoais;
- Elaborar um Plano Anual de Capacitação e Conscientização;
- Sugerir à alta direção a contratação de especialistas para ministrar treinamentos sobre privacidade e proteção aos dados pessoais, bem como, segurança da informação;
- Realizar e documentar avaliações de riscos de privacidade;
- Realizar avaliações de impacto à privacidade, quando necessário;

- Elaborar Relatório de Impacto à Privacidade (RIPD), quando necessário;
- Manter o Registro das Operações de Tratamento de Dados Pessoais (ROPA) atualizado;
- Definir e manter atualizadas as bases legais das atividades desenvolvidas pelo Senac Goiás;
- Manter a alta direção informada quanto aos riscos de proteção de dados e de segurança da informação e eventuais incidentes de segurança;
- Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;
- Orientar os colaboradores e agentes de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Receber, analisar, tratar e responder às notificações e atividades relacionadas aos eventos e incidentes de segurança da informação e privacidade;
- Apresentar medidas preventivas/corretivas dos eventos e incidentes analisados visando mitigar o risco;
- Comunicar a ANPD e titulares quando da ocorrência de incidentes de segurança, nas hipóteses em que a comunicação for necessária;
- Manifestar-se, quando solicitado, sobre questões de sua competência.

8.4. COLABORADORES

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT, estagiário, menor ou jovem aprendiz, terceirizado, prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do Senac Goiás.

É dever dos colaboradores:

- Observar e cumprir a Política de Privacidade e demais documentos correlatos;
- Atuar em conformidade com as normas e regulamentos internos no que tange ao tratamento de dados pessoais no exercício de suas funções;
- Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações e dados pessoais acessados e manipulados, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia;
- Zelar pela qualidade dos dados pessoais, exatidão e atualização, sobre sua responsabilidade;
- Não revelar qualquer informação ou dado pessoal de propriedade ou sob a responsabilidade do Senac Goiás sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico;

- Participar dos treinamentos;
- Reportar formalmente ao Encarregado pelo tratamento de dados quaisquer eventos relativos à violação ou suspeita de violação das normas internas acerca de segurança da informação e privacidade dos dados, bem como de leis vigentes;
- Não compartilhar com terceiros, senhas de acesso ou informações pessoais que possam comprometer a privacidade de seus dados e de terceiros, sua segurança e a segurança do Senac Goiás.

9. RESPONSABILIZAÇÃO

O descumprimento desta e de outras Políticas do Senac Goiás relacionadas à segurança, proteção e privacidade de dados pessoais pode resultar em medidas disciplinares, que variam de uma advertência verbal até a rescisão contratual por justa causa, dependendo da gravidade da infração.

Incidentes serão avaliados pelo Encarregado de Dados e pela Gerência de Tecnologia. Caso seja constatada uma violação, será elaborado e encaminhado um relatório para a alta direção, que, após análise, poderá instaurar procedimento administrativo disciplinar para apurar responsabilidades e aplicar as sanções cabíveis, previstas em contratos, documentos normativos do Senac Goiás e na legislação vigente, considerando também os danos causados.

10. POLÍTICAS COMPLEMENTARES

Serão criadas, aprovadas e implementadas as seguintes políticas complementares, para apoiar no Programa de Privacidade do Senac Goiás:

1. Política de Segurança da Informação;
2. Plano de Respostas a Incidentes;
3. Política de Classificação da Informação;
4. Política de Atendimento aos Titulares.

11. INFORMAÇÕES E DÚVIDAS

Se precisar de esclarecimentos sobre suas informações ou desejar exercer seus direitos como Titular de Dados Pessoais, entre em contato com o Encarregado de Dados pelo e-mail dpo@go.senac.br. Todas as solicitações serão atendidas de forma gratuita, mediante a confirmação da sua identidade e a análise da viabilidade de atendimento, em conformidade com as exigências legais e regulatórias aplicáveis.

Atualizações do Aviso de Privacidade

Esta Política de Privacidade é mantida atualizada para refletir a preocupação do Senac Goiás com a privacidade e proteção de dados. Modificações serão realizadas para adequação à legislação, em novos riscos identificados que possam prejudicar a segurança da informação ou para trazer melhorias.

ANEXO I

ATIVIDADE	PERÍODO DE RETENÇÃO	LEI / REGULAMENTO / NORMA
Registro de acesso aos Sistemas	6 meses após o último acesso	Marco Civil da Internet (Lei 12.965/2014, Art. 15)
Serviços de contato	5 anos após o último atendimento	Código de Defesa do Consumidor (Lei 8.078/1990, Art. 27)
Dados de Currículo	6 meses a 1 ano caso não contratado; 5 anos durante contrato e 2 anos após	Legítimo Interesse (LGPD, Art. 7º, IX)
Ficha de Recrutamento e Seleção	Imediatamente caso não contratado; 5 anos durante contrato e 2 anos após	Legítimo Interesse (LGPD, Art. 7º, IX)
Contrato de Trabalho (Gestão de RH)	5 anos durante o contrato; 2 anos após. FGTS: 30 anos. Registro de ponto: 10 anos	CLT (Decreto-Lei 5.452/1943); Lei do FGTS (Lei 8.036/1990, Art. 23)
Administração do RH – Vale transporte, adiantamentos etc.	5 anos durante o contrato; 2 anos após	CLT (Decreto-Lei 5.452/1943)
Documentos de registro de regularidade trabalhista	5 anos durante o contrato; 2 anos após	CLT (Decreto-Lei 5.452/1943)
Folha de pagamento e registro de ponto	10 anos	CLT (Decreto-Lei 5.452/1943); Lei do FGTS (Lei 8.036/1990, Art. 23); Código Tributário Nacional (Lei 5.172/1966, Art. 173)
FGTS	30 anos	Lei do FGTS (Lei 8.036/1990, Art. 23)
Contribuição Sindical	5 anos	CLT (Decreto-Lei 5.452/1943)
Atestado de Saúde Ocupacional (ASO)	Mínimo de 20 anos após desligamento	NR-7 (Norma Regulamentadora 7, Item 7.4.5.1)

Atestado de Saúde (comum)	5 anos durante o contrato; 2 anos após	NR-7 (Norma Regulamentadora 7)
CAT – Comunicação de Acidente de Trabalho	5 anos	Lei 8.213/1991, Art. 22
Treinamento de funcionários	Imediatamente caso não contratado; 5 anos durante contrato e 2 anos após	NR-1 (Norma Regulamentadora 1)
Acesso aos Sistemas - Senhas e Logins	Logins e senhas durante o contrato; registro de acesso por 6 meses	Marco Civil da Internet (Lei 12.965/2014, Art. 15)
Monitoramento de e-mails	2 a 5 anos após o término do contrato	Legítimo Interesse (LGPD, Art. 7º, IX); CLT (Art. 7º, XXIX)
Dados de Navegação no site	6 meses após a última atividade ou revogação do consentimento	Marco Civil da Internet (Lei 12.965/2014, Art. 15)
Atas de Reuniões e Assembleias	10 anos	Código Civil (Lei 10.406/2002, Art. 1.091)
Documentos Tributários	5 anos a partir da emissão	Código Tributário Nacional (Lei 5.172/1966, Art. 173)
Imagens para Publicidade e Divulgação (redes sociais, marketing, eventos)	Até revogação do consentimento	Consentimento do titular (LGPD, Art. 7º, I)
Cumprimento de obrigação fiscal e tributária	5 anos a partir do final do exercício fiscal	Código Tributário Nacional (Lei 5.172/1966, Art. 173)
Contratos de Prestação de Serviços	10 anos	Código Civil (Lei 10.406/2002, Art. 205)
Contratos com Titulares/Clientes	10 anos	Código Civil (Lei 10.406/2002, Art. 205)
Contratos Gerais	10 anos	Código Civil (Lei 10.406/2002, Art. 205)
Contatos Comerciais	1 ano sem contato ou revogação do consentimento	Código Civil (Art. 206, § 5º, I); Consentimento do titular (LGPD, Art. 7º, I)
Campanhas Publicitárias, ações e pesquisas	Até revogação do consentimento	Código de Defesa do Consumidor (Art. 27); LGPD (Art. 7º, I)
Imagens Internas	30 dias a 1 ano (se não houver investigação em andamento)	Legítimo Interesse (LGPD, Art. 7º, IX); Código Civil (Lei 10.406/2002, Art. 206, § 3º, IV)