POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS
CIASEG PRESTADORA DE SERVIÇOS LTDA

DEZEMBRO/2025

https://ciasegsinistros.com.br douglas.souza@ciasegsinistros.com.br

POLÍTICA DE PRIVACIDADE – CIASEG PRESTADORA DE SERVIÇOS LTDA

Versão: 1.0 – **Dez/2025**

Controladora (quando aplicável): CIASEG PRESTADORA DE SERVIÇOS LTDA – CNPJ **53.285.429/0001-39** (EPP).

Site: https://ciasegsinistros.com.br

Encarregado (DPO): Douglas Souza – douglas.souza@ciasegsinistros.com.br

Esta Política explica como a CIASEG trata dados pessoais em suas atividades de **investigação, análise e sindicância de indícios de fraude em sinistros de seguros**, inclusive com alto volume de dados e, eventualmente, **dados sensíveis e criminais/judiciais**.

1) Para quem esta Política se aplica

Aplica-se ao tratamento de dados pessoais de pessoas relacionadas a sinistros, incluindo: **segurados**, **beneficiários**, **terceiros envolvidos** (ex.: vítimas e prestadores), **testemunhas** e **suspeitos de participação em fraude**.

2) Papéis (controlador/operador) e contexto de seguros

No contexto de sindicância de sinistros, a **seguradora contratante** é, em regra, a responsável principal pela apuração e decisão sobre o sinistro, e a CIASEG atua no **apoio técnico/administrativo**, com coleta de informações e emissão de relatórios. Conforme o caso, **CIASEG e seguradora (ex.: Icatu)** podem figurar como controladores em suas respectivas responsabilidades.

3) Quais dados pessoais tratamos

De acordo com o ROPA, podemos tratar, conforme necessário e proporcional ao caso:

- **Identificação civil:** nome, RG, CPF, CNH, passaporte.
- **Contato:** endereço, telefone, e-mail.
- **Profissionais e financeiros:** vínculo empregatício, renda, extratos, notas fiscais, contratos.
- **Relacionados ao seguro:** apólices, histórico de sinistros, comunicações com a seguradora.
- **Dados sensíveis (quando aplicável):** prontuários, laudos, receitas, exames (ex.: vida/saúde/acidentes).
- **Dados visuais/biométricos:** imagens de câmeras, fotografias, assinaturas.
- **Dados criminais/judiciais:** certidões, boletins de ocorrência, inquéritos.

Em geral, esses dados chegam e ficam registrados em **documentos** (imagens e PDFs).

4) Como coletamos os dados

A CIASEG recebe e coleta dados principalmente:

- **Da seguradora**, via plataforma, com posterior armazenamento no ambiente corporativo da CIASEG (Microsoft 365 E3).
- **Do titular, terceiros e fontes necessárias à apuração**, durante a sindicância, incluindo coleta de novos documentos mediante **termo de autorização** quando aplicável.

5) Finalidades do tratamento

Tratamos dados para:

- **Prevenir, detectar e apurar indícios de fraude em seguros**.
- **Garantir a integridade econômica** da seguradora.
- **Cumprir obrigações legais e regulatórias** (incluindo SUSEP, quando aplicável).
- **Produzir relatórios de sindicância** e subsidiar medidas administrativas/judiciais.

6) Bases legais

As bases legais variam conforme o caso e a natureza do dado/documento,incluindo:

- **Execução de contrato (art. 7º, V)**.
- **Cumprimento de obrigação legal/regulatória** (ex.: exigências do setor e requisições oficiais).
- **Consentimento**, quando aplicável (ex.: certas coletas adicionais formalizadas).
- **Legítimo interesse (art. 7º, IX)**, especialmente para **prevenção à fraude e segurança do titular**.

7) Compartilhamento de dados

7.1. Compartilhamento operacional (casos de sinistro)

No fluxo de sindicância, os dados podem ser acessados/compartilhados entre **CIASEG, seguradora e sindicante**, com controle de acesso e, após o encerramento, o **sindicante deixa de ter acesso**.

7.2. Compartilhamento externo (autoridades e profissionais)

O compartilhamento externo pode ocorrer com **órgãos públicos, autoridades judiciais/policiais, advogados, peritos e reguladores**, **somente** quando necessário em demandas judiciais/administrativas ou no devido processo legal.

8) Transferência internacional e provedores de nuvem

A CIASEG utiliza **Microsoft 365 E3** como plataforma de documentos; esse serviço pode envolver **servidores no Brasil e no exterior**, conforme a política do provedor, caracterizando possibilidade de transferência internacional.

9) Segurança da informação

Adotamos medidas técnicas e administrativas compatíveis com o porte e o risco do tratamento, incluindo:

- **Autenticação multifator (MFA)** com Microsoft Authenticator e perfis de acesso.
- **Auditoria/logs de acesso** no Microsoft 365 E3.
- **Criptografia de armazenamento (cofre digital) com VeraCrypt** e **backups criptografados em discos externos**, com guarda em local diverso para resiliência.
- **Antivírus (Norton Security)** nas estações de trabalho.
- **Proteção física**: documentos em papel mantidos em armários com fechadura e ambiente com **monitoramento por câmeras** no local da sede.

10) Retenção e descarte

- Mantemos dados pelo tempo necessário à sindicância e, no mínimo, **mais 5 anos após o encerramento**, considerando normas aplicáveis e prazos prescricionais; em caso judicial, até o trânsito em julgado + 5 anos.
- Dados de **sindicantes**: enquanto durar o contrato e **2 anos após o distrato**, com backup criptografado.
- **Descarte físico**: realizado com **trituradora** antes do descarte final.
- **Descarte digital**: exclusão dos documentos na plataforma e nos computadores corporativos, conforme registro de protocolo e regras internas de encerramento.

11) Atendimento ao titular e direitos

Os titulares podem solicitar, nos termos da LGPD, informações e providências relacionadas a: confirmação/ acesso, correção, anonimização/bloqueio/eliminação (quando aplicável), informação sobre compartilhamento e revogação de consentimento (quando for a base legal).
Canal oficial: Encarregado (DPO) – douglas.souza@ciasegsinistros.com.br.

12) Sede em coworking (Company Hero) e efeitos de privacidade

A sede da CIASEG está em coworking, cuja infraestrutura de internet/segurança é gerida pelo próprio espaço.
Ao utilizar o ambiente, podem existir tratamentos de dados pelo coworking para fins de **contratação, controle de acessos e segurança**, incluindo:

- **login e senha individuais** e regras de uso de conta.
- **monitoramento por circuito interno de vigilância**, com guarda/uso de imagens quando necessário.
- compromisso de **medidas de segurança** e **comunicação de incidentes** pelo coworking, além de armazenamento após término contratual para obrigações legais.

A CIASEG reforça que **informações e documentos de sinistros** devem permanecer nos repositórios corporativos definidos (ex.: Microsoft 365 E3) e sob controles de acesso.

13) Incidentes de segurança

Em caso de incidente, a CIASEG avalia a necessidade e a profundidade de comunicação à **ANPD** e aos titulares conforme parâmetros aplicáveis, e mantém procedimento de resposta e melhoria contínua.

14) Atualizações desta Política

Esta Política pode ser atualizada para refletir mudanças operacionais, contratuais ou regulatórias, mantendo-se alinhada ao **ROPA** e aos controles de segurança/retenção descritos.

ENCARREGADO

gov.br Documento assinado digitalmente
DOUGLAS SANTANA DE SOUZA
Data: 12/12/2025 12:21:42-0300
Verifique em https://validar.iti.gov.br

DOUGLAS SOUZA

Belém, 10 de dezembro de 2025