Política de Privacidade Cesla
Cesla Privacy Policy

Versão 2.1 | 14 de Agosto de 2025
Responsável Técnico: CPO – Silvia Adriana Silvestrini
Aprovador Institucional: CEO – Cleber Candido Eduardo
Status do documento: Aprovado
Uso Interno - Documento Confidencial

Version 2.1 | Aug 14, 2025
Technical Responsible: CPO – Silvia Adriana Silvestrini
Executive Approver: CEO – Cleber Candido Eduardo
Document Status: Approved
Internal Use / Confidential Document

Sumário

Controle de versionamento – Política de Privacidade Cesla
Version Control – Cesla Privacy Policy

Emissão Inicial / Document creation – V1.0		
Data: **Creation Date:**	June, 2021	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Paulo Rodrigues - CTO	• Emissão inicial | Document creation
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Versão / Version V2.0		
Data: **Creation Date:**	May 2, 2025	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Comitê de Tecnologia Cesla | Cesla Technology Committee	• Revisão geral de lay-out e conteúdo | Layout and content review • Elaboração do Documento – Versão Bilíngue (Português/Inglês) | Bilingual Document Preparation (Portuguese/English)
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Versão / Version V2.1		
Data: **Creation Date:**	Aug 14, 2025	**Comentários / Conteúdo revisado** **Comments / Revised Content**
Criado por: **Created by:**	Comitê de Tecnologia Cesla | Cesla Technology Committee	• Inclusão do item: **10.1 - Transferência Internacional de Dados** • Inclusion of item: **10.1 – International Data Transfers**
Revisado por: **Reviewed by:**	Silvia Adriana Silvestrini – CPO	
Aprovado por: **Approved by:**	Cleber Candido Eduardo – CEO	

Local de Armazenamento do Documento

O arquivo "**Cesla Privacy Policy_Bilingual_V2.1_Aug2025.docx"** está armazenado no repositório oficial da Cesla, com controle de versão e acesso restrito às áreas autorizadas, conforme estrutura a seguir:

📁 **SharePoint > Governança > Documentos > Planos e Políticas > Privacidade > Cesla Privacy Policy_Bilingual_V2.1_Ago2025.docx**

Este diretório é gerenciado pelo Comitê de Tecnologia, e as atualizações do documento são registradas com controle de histórico e revisão. A versão atual está identificada como **V2.1 – August 2025**, com status **Aprovado**.

Document Storage Location

The file "**Cesla Privacy Policy_Bilingual_V2.1_Aug2025.docx"** is stored in Cesla's official repository, with version control and restricted access to authorized departments, according to the following structure:

📁 **SharePoint > Governança > Documentos > Planos e Políticas > Privacidade > Cesla Privacy Policy_Bilingual_V2.1_Aug2025.docx**

This directory is managed by the Technology Committee, and document updates are recorded with version history and revision control. The current version is identified as **V2.1 – August 2025**, with the status **Approved**.

1. Introdução

Em vigor a partir de 14 de Agosto de 2025.

A presente Política de Privacidade tem por finalidade demonstrar o compromisso da Cesla Tecnologia, inscrita no CNPJ nº 57.813.530/0001-76, com sede em Campinas/SP, com a privacidade, proteção e tratamento dos dados pessoais coletados por meio da plataforma Cesla e seus respectivos módulos.

Este documento foi elaborado em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), reforçando a responsabilidade da Cesla Tecnologia como controladora dos dados pessoais tratados no âmbito de seus serviços.

Ao utilizar os nossos sistemas, o titular de dados reconhece que a Cesla Tecnologia poderá realizar operações de coleta, armazenamento, uso e compartilhamento de dados, conforme descrito nesta Política.

Para dúvidas, solicitações ou reclamações relacionadas ao tratamento de dados pessoais, o titular poderá entrar em contato com o Encarregado pelo Tratamento de Dados (DPO) através do e-mail **dpo@intuix.com**.

2. Glossário

Para facilitar sua leitura e compreensão desta Política de Privacidade, segue um resumo das definições de termos usados com recorrência ao longo deste documento:

- **Titular de Dados:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No contexto da Cesla, normalmente é o cliente contratante da licença.
- **Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. A Cesla Tecnologia atua como operadora da Cesla.
- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, e-mail, endereço IP, entre outros.
- **Dado Pessoal Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, biometria, entre outros, cuja proteção é reforçada pela LGPD.
- **LGPD (Lei Geral de Proteção de Dados):** Lei nº 13.709/2018, que regula o tratamento de dados pessoais no Brasil, inclusive nos meios digitais.
- **Token de Acesso:** Código criptografado utilizado para autenticar sessões de usuários na plataforma, com validade limitada e renovação controlada.
- **SSO (Single Sign-On):** Mecanismo que permite ao usuário acessar múltiplos sistemas com uma única autenticação centralizada, utilizado via Entra ID e FusionAuth na Cesla.
- **MFA (Autenticação Multifator):** Camada extra de segurança que exige mais de um fator de verificação (como senha + código de verificação) para autenticação.
- **Logs de Auditoria:** Registros automáticos das ações realizadas pelos usuários na plataforma, contendo informações como login, horário, IP, ação executada, entre outros.
- **SIEM (Security Information and Event Management):** Sistema de monitoramento e análise de eventos de segurança, utilizado para detectar e responder a possíveis ameaças e incidentes.
- **Incident Response Plan (IRP):** Documento que define como a Cesla detecta, responde e documenta incidentes de segurança que impactam os dados ou sistemas da plataforma.
- **Business Continuity Plan (BCP):** Estrutura de governança e processos adotados para manter ou restabelecer os serviços essenciais da Cesla diante de falhas críticas ou desastres.
- **EPS (Empresa Prestadora de Serviço):** Organização contratada pelo cliente da Cesla para executar atividades operacionais. Seus dados e documentos são gerenciados em ambiente segregado e com licenciamento próprio.

3. Finalidade

Esta Política de Privacidade tem como finalidade estabelecer, de forma clara e transparente, as diretrizes adotadas pela Cesla Tecnologia para o tratamento de dados pessoais realizado por meio da plataforma Cesla.

O documento descreve como os dados são coletados, utilizados, armazenados, compartilhados e protegidos, assegurando a conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), bem como o respeito aos princípios da segurança, privacidade e autodeterminação informativa dos titulares.

Ao definir essas diretrizes, a Cesla reforça seu compromisso com:

- A transparência no uso de dados pessoais;
- A proteção da integridade, confidencialidade e disponibilidade das informações;
- A garantia dos direitos dos titulares;
- E a responsabilidade compartilhada entre os atores que interagem com a plataforma, incluindo clientes, EPSs, parceiros e colaboradores.

4. Abrangência

Esta Política de Privacidade se aplica a **todos os usuários que interagem com a plataforma Cesla**, por meio de seus módulos web ou mobile, incluindo:

- Clientes contratantes da licença de uso da plataforma;
- Colaboradores das empresas prestadoras de serviço (EPSs) cadastrados pelos clientes;
- Parceiros autorizados a operar funcionalidades específicas da solução;
- E colaboradores da Cesla Tecnologia que, no exercício de suas funções, tenham acesso a dados pessoais tratados na plataforma.

Abrange também o tratamento de dados realizado pelas equipes técnicas, administrativas, de suporte, implantação, segurança da informação e gestão de produto da Cesla Tecnologia, em conformidade com os papéis de controlador e operador definidos contratualmente.

5. Dados Coletados

A plataforma Cesla poderá coletar e tratar dados pessoais de diferentes naturezas, conforme o uso e o perfil do usuário. Os principais grupos de dados tratados incluem:

- **Dados de Identificação:** Nome completo, e-mail corporativo, CPF, telefone, empresa vinculada, cargo/função e outras informações cadastrais básicas.
- **Dados de Autenticação e Acesso:** Nome de usuário (login), tokens de sessão, autenticação via SSO (Single Sign-On), múltiplos fatores de autenticação (MFA), logs de login e registros de tempo de acesso.
- **Dados de Navegação e Uso da Plataforma:** Endereço IP, datas e horários de acesso, registros de ações realizadas dentro dos módulos, menus acessados e operações executadas.
- **Dados Operacionais:** Informações preenchidas em formulários, permissões atribuídas, uploads de documentos, interações com APIs, respostas a checklists e comentários inseridos na plataforma.
- **Dados Técnicos do Dispositivo e Conexão:** Tipo de dispositivo, navegador utilizado, sistema operacional, resolução de tela e dados de rede/internet utilizados durante a navegação.

A coleta e o tratamento desses dados visam garantir a rastreabilidade, a segurança, a prestação adequada dos serviços e a conformidade com as obrigações contratuais e legais.

6. Finalidade do Tratamento

Os dados pessoais coletados na plataforma Cesla são tratados de acordo com os princípios da necessidade, finalidade, segurança e responsabilização, com as seguintes finalidades principais:

- **Assegurar o funcionamento técnico da plataforma**, incluindo autenticação de usuários, gerenciamento de permissões, controle de sessões e integridade dos dados;
- **Garantir a segurança da informação**, com aplicação de controles de acesso, registros de atividade, rastreabilidade e resposta a incidentes;
- **Cumprir obrigações legais, contratuais e regulatórias**, relacionadas à gestão de terceiros, qualificação de prestadores de serviço, saúde e segurança do trabalho, entre outras;
- **Apoiar a continuidade operacional e os planos de recuperação de desastres**, conforme previsto no Plano de Continuidade de Negócios (BCP);
- **Monitorar e auditar o uso da plataforma**, promovendo a conformidade com normas internas e exigências de clientes;
- **Personalizar e aprimorar a experiência do usuário**, com base em seus acessos e interações dentro dos módulos Cesla.

6.1. Tratamento de Dados Pessoais Sensíveis

A depender do contexto de uso da plataforma e da natureza dos dados inseridos por clientes e EPSs, poderão ser tratados dados pessoais sensíveis, como informações de saúde, exames médicos ocupacionais (ASO), certificados de treinamentos e documentos obrigatórios para fins legais e operacionais.

Esses dados são tratados com:

- Finalidade legítima e previamente definida;
- Restrições de acesso técnico e administrativo;
- Controles de segurança e confidencialidade adequados;
- E base legal compatível, conforme os contratos firmados entre a Cesla Tecnologia, o cliente contratante e as partes envolvidas.

7. Compartilhamento de Dados

A Cesla poderá compartilhar dados pessoais tratados na plataforma com terceiros estritamente necessários à prestação dos serviços ou ao cumprimento de obrigações legais e contratuais. Os dados poderão ser compartilhados:

- Com prestadores de serviço contratados para infraestrutura (ex.: Azure, EVEO) e segurança (ex.: Cloudflare, Firebase);
- Com autoridades competentes, mediante obrigação legal;
- Com o cliente contratante da licença, quando aplicável, respeitando a finalidade contratual;
- Com sistemas parceiros indicados pelo cliente, para fins de integração com ferramentas de controle de acesso, portaria, medicina ocupacional, segurança do trabalho e afins.

A responsabilidade por documentar e justificar tais integrações é exclusiva do cliente contratante e das empresas prestadoras de serviço (EPSs), que devem firmar os contratos e aditivos apropriados com os respectivos terceiros envolvidos.

7.1. Garantia de Segurança e Privacidade no Compartilhamento de Dados

A responsabilidade por aplicar cláusulas contratuais, políticas de privacidade e demais garantias legais junto aos sistemas parceiros indicados pelo cliente — tais como ferramentas de controle de acesso, portaria, medicina ocupacional e segurança do trabalho — é exclusiva do cliente contratante da plataforma Cesla.

Cabe ao cliente assegurar que tais terceiros estejam em conformidade com a LGPD e demais normas aplicáveis, por meio de validações técnicas, contratuais e obrigações de confidencialidade firmadas entre as partes.

Por outro lado, os prestadores de serviço contratados pela Cesla Tecnologia para suporte à infraestrutura da Cesla (como Azure, EVEO, Cloudflare e Firebase) são contratualmente obrigados a garantir níveis adequados de segurança da informação e proteção à privacidade, compatíveis com os padrões internos da Cesla Tecnologia.

São exigidas dessas partes obrigações específicas, como:

- Confidencialidade das informações tratadas;
- Uso limitado à finalidade contratada;
- Implementação de controles técnicos e organizacionais que assegurem a integridade, disponibilidade e sigilo dos dados pessoais.

A Cesla realiza, sempre que necessário, validações técnicas e contratuais para assegurar que seus parceiros diretos estejam aderentes à LGPD, às normas ISO/IEC 27001/27035 e demais diretrizes aplicáveis.

8. Segurança da Informação

A Cesla Tecnologia adota medidas técnicas e organizacionais rigorosas para garantir a segurança da informação e a proteção dos dados pessoais tratados na plataforma Cesla. Entre os principais controles implementados, destacam-se:

- Autenticação via SSO com MFA obrigatório (FusionAuth e Entra ID) para colaboradores da Cesla;
- Criptografia de dados em repouso (SHA-512) e em trânsito (TLS 1.2+ com camada adicional AES-256-CBC);
- Sessões autenticadas com tokens expiráveis e rastreáveis;
- Logs de auditoria mantidos por no mínimo 5 anos;
- Monitoramento e proteção com ferramentas como SIEM, WAF, Fail2Ban, Jump Server e segregação de ambientes (produção, homologação, QA, desenvolvimento).

A autenticação de usuários na plataforma Cesla ocorre por meio de dois modelos distintos:

- Clientes com integração ao Entra ID realizam o login via autenticação federada (SSO), utilizando os controles de segurança e identidade do próprio ambiente corporativo.
- Clientes sem integração com Entra ID e usuários vinculados a Empresas Prestadoras de Serviço (EPSs) são cadastrados diretamente na plataforma Cesla pelos administradores da licença (cliente ou EPS), que também definem os perfis de acesso e permissões específicas, de acordo com a função e responsabilidade do usuário.

Independentemente do modelo de autenticação, o acesso à plataforma exige o uso de senhas fortes e autenticação multifator (MFA), garantindo rastreabilidade e controle contínuo de acessos.

9. Direitos do Usuário (Titular dos Dados)

Em conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), os usuários da plataforma Cesla, na qualidade de titulares de dados pessoais, têm garantido o direito de:

- Solicitar a confirmação da existência de tratamento de seus dados;
- Ter acesso aos dados armazenados e receber informações claras sobre sua finalidade;
- Requisitar a correção de dados incompletos, inexatos ou desatualizados;
- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos;
- Obter informações sobre compartilhamentos realizados com terceiros;
- Requerer a portabilidade dos dados, observados os segredos comercial e industrial;
- Revogar consentimentos fornecidos, quando aplicável;
- Manifestar oposição ao tratamento de dados realizado com base em interesses legítimos, quando for o caso.

Esses direitos poderão ser exercidos de forma gratuita e a qualquer momento, mediante solicitação encaminhada aos canais oficiais:

✉ **dpo@intuix.com**
📞 **0800 002 3752** (horário comercial)

As solicitações serão analisadas em conformidade com os prazos e limites legais aplicáveis, podendo exigir validação de identidade do titular para proteção contra acesso indevido.

10. Armazenamento e Retenção

Os dados pessoais coletados por meio da plataforma Cesla são armazenados em nuvem segura (Microsoft Azure e EVEO), com backups periódicos (total e incremental) e retenção mínima de 90 dias.

A Cesla Tecnologia adota diferentes políticas de retenção conforme o papel do titular e o tipo de dado tratado:

- Dados vinculados à conta do cliente contratante (ex.: administradores, operadores e responsáveis técnicos): são mantidos por até 2 anos após a rescisão contratual, ou conforme cláusula contratual.
- Dados de prestadores de serviço (EPSs) cadastrados pelo cliente, incluindo dados pessoais de colaboradores e documentos de qualificação (como exames, treinamentos, ASOs, certificados etc.):
    - Permanecem acessíveis em ambiente segregado e com licenciamento específico por até 2 anos após o encerramento do contrato da EPS.
    - Após esse prazo, a licença da EPS é inativada, mas os dados são mantidos por um período mínimo de 20 anos, exclusivamente para fins legais, regulatórios e trabalhistas, em conformidade com os contratos firmados entre a Cesla e o cliente.

Registros de login, trilhas de auditoria e logs de rastreabilidade são mantidos por, no mínimo, **5 anos**, conforme as boas práticas de segurança e os requisitos das normas ISO/IEC 27001 e 27035.

10.1. Transferência Internacional de Dados

A Cesla poderá realizar a transferência internacional de dados pessoais e corporativos quando necessário para a operação de seus serviços, observando integralmente as disposições da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais legislações aplicáveis.

Atualmente, essa transferência ocorre nos seguintes casos:

- Armazenamento de backups: parte dos backups da plataforma Cesla é armazenada em datacenters da Microsoft Azure localizados nos Estados Unidos (região Central US), com proteção conforme padrões internacionais de segurança da informação, incluindo criptografia AES-256-CBC em trânsito e SHA-512 em repouso, e certificação ISO/IEC 27001:2022.
- Armazenamento de documentos e imagens: arquivos enviados e processados pela plataforma (incluindo imagens, evidências e documentos) podem ser armazenados no Cloudflare R2, com servidores distribuídos globalmente, assegurando que a transferência e o processamento sigam as medidas técnicas e organizacionais adequadas para proteção dos dados.
- Todos os provedores utilizados adotam cláusulas contratuais padrão, certificações internacionais (como ISO/IEC 27001) e mecanismos de segurança compatíveis com os requisitos da LGPD.
- Sempre que aplicável, a Cesla adota medidas complementares, como pseudonimização e controle estrito de acesso, para reduzir riscos na transferência internacional de dados.

11. Responsabilidades do Cliente Contratante e das Empresas Prestadoras de Serviço (EPSs)

A Cesla Tecnologia, como operadora dos dados pessoais tratados por meio da plataforma Cesla, atua sob as instruções e finalidade definidas pelos clientes contratantes, que são os controladores das informações inseridas em seus respectivos ambientes.

É de responsabilidade exclusiva dos clientes contratantes e das empresas prestadoras de serviço (EPSs):

- Garantir que exista base legal válida para o tratamento dos dados pessoais inseridos na plataforma Cesla, incluindo consentimentos, quando aplicável.
- Informar seus colaboradores, prestadores ou quaisquer titulares de dados que os dados poderão ser compartilhados com a Cesla Tecnologia (Cesla) e, quando necessário, com outros parceiros indicados pelo cliente, como empresas de controle de acesso, portaria, medicina ocupacional, segurança do trabalho e afins.
- Incluir cláusulas contratuais apropriadas que reconheçam que os dados pessoais e documentos enviados poderão ser utilizados para fins de qualificação, rastreabilidade, auditoria e segurança operacional, conforme os requisitos do contrato com o cliente.

A Cesla não se responsabiliza pela ausência de formalização adequada entre o cliente, seus fornecedores (EPSs) e os colaboradores cadastrados, devendo qualquer reivindicação por parte dos titulares ser tratada inicialmente junto ao controlador responsável pelo tratamento.

12. Comunicação de Incidentes e Não Conformidades

Todos os usuários da plataforma Cesla — incluindo clientes, empresas prestadoras de serviço (EPSs) e colaboradores internos da Cesla Tecnologia — devem adotar uma postura ativa na identificação e comunicação de qualquer situação que represente risco à segurança da informação ou à conformidade com a LGPD.

Em caso de identificação ou suspeita de:

- Vazamento ou acesso indevido a dados pessoais;
- Comportamento anômalo no sistema ou falhas técnicas relevantes;
- Compartilhamento não autorizado de dados;
- Utilização indevida de credenciais ou permissões de acesso;
- Não conformidade contratual ou legal relacionada ao tratamento de dados;
- Falhas de segurança na autenticação, permissões ou integridade de informações;
- Não conformidades com a LGPD ou cláusulas contratuais vigentes;

o incidente deve ser comunicado **imediatamente à equipe Cesla**, preferencialmente por meio dos canais institucionais de suporte ao usuário ou por contato direto com o Encarregado (DPO) através do e-mail **dpo@intuix.com**, a fim de viabilizar a contenção e tratamento adequado.

Canais de suporte ao usuário Cesla (horário comercial – segunda a sexta, das 8h às 17h):

- E-mail: suporte@ws-solution.com
- WhatsApp: (19) 9 9331-2498
- Telefone: 0800 002 3752

A Cesla Tecnologia mantém um Plano de Resposta a Incidentes (PRI) alinhado às normas ISO/IEC 27035, 27001 e à legislação brasileira, garantindo procedimentos formais de detecção, contenção, análise, comunicação e correção de incidentes de segurança da informação.

É expressamente vedado o uso, compartilhamento ou armazenamento de dados acessados indevidamente. Qualquer violação dessa diretriz poderá resultar em responsabilização civil, penal e contratual, conforme a legislação vigente e os compromissos assumidos com os titulares dos dados.

13. Propriedade Intelectual

Todos os direitos de propriedade intelectual relacionados à plataforma Cesla, incluindo seus módulos, funcionalidades, interface, estrutura de dados, fluxos operacionais, marca, identidade visual, código-fonte, bancos de dados e demais componentes técnicos, são de titularidade exclusiva da **Cesla Tecnologia**.

É expressamente vedado a qualquer usuário, cliente, empresa prestadora de serviço (EPS) ou terceiro:

- Reproduzir, copiar, modificar, descompilar, fazer engenharia reversa ou criar obras derivadas com base em qualquer módulo ou funcionalidade da Cesla;
- Utilizar o sistema para fins não autorizados contratualmente, ou fora do escopo da licença concedida;
- Transferir, ceder ou sublicenciar o uso da plataforma sem autorização prévia e formal da Cesla Tecnologia.

A contratação da licença de uso da plataforma Cesla concede ao cliente **um direito de uso não exclusivo, intransferível e limitado ao período contratual**, conforme definido em contrato comercial vigente.

Qualquer uso indevido poderá gerar responsabilização civil, penal e administrativa, além de sanções previstas nos termos de uso, contrato e legislação aplicável.

14. Encarregado pelo Tratamento de Dados (DPO)

A Cesla Tecnologia designou um **Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO)**, responsável por atuar como canal de comunicação entre a Cesla, os titulares de dados, a Autoridade Nacional de Proteção de Dados (ANPD) e demais partes interessadas.

Compete ao DPO:

- Receber e responder solicitações dos titulares de dados, conforme previsto na LGPD;
- Prestar esclarecimentos sobre o tratamento de dados pessoais realizado na plataforma Cesla;
- Orientar colaboradores e parceiros quanto às práticas de proteção de dados;
- Supervisionar a conformidade da organização com as diretrizes da LGPD e demais normativas aplicáveis;
- Apoiar auditorias, investigações e iniciativas de melhoria contínua da privacidade e segurança da informação.

Para entrar em contato com o DPO da Cesla Tecnologia, utilize o canal oficial: **dpo@intuix.com**

15. Atualizações e Revisões

A presente Política de Privacidade será **revisada periodicamente**, com frequência mínima anual, ou sempre que ocorrerem:

- Alterações significativas na legislação aplicável, especialmente relacionadas à proteção de dados pessoais;
- Atualizações nos serviços, funcionalidades ou módulos da plataforma Cesla que impactem o tratamento de dados;
- Mudanças relevantes nos processos internos de segurança da informação, privacidade ou governança de dados.

Todas as atualizações serão registradas com controle de versão e, quando envolverem mudanças relevantes que impactem os titulares, serão devidamente **comunicadas pelos canais oficiais** da Cesla.

A versão mais recente da Política estará sempre disponível para consulta.

16. Confidencialidade

Todas as informações e dados pessoais tratados na plataforma Cesla são considerados confidenciais e protegidos contra acesso, uso ou divulgação não autorizada.

A Cesla Tecnologia adota medidas técnicas e administrativas rigorosas para preservar a confidencialidade dos dados inseridos por clientes, EPSs e usuários, incluindo:

- Acordos de confidencialidade com colaboradores e parceiros;
- Controles de acesso baseados em perfis e necessidades operacionais;
- Monitoramento contínuo de sessões e registros de atividades;
- Criptografia e segregação de ambientes.

É vedado a qualquer usuário, colaborador ou terceiro:

- Compartilhar ou utilizar dados acessados de forma indevida;
- Divulgar informações tratadas na plataforma sem autorização formal do controlador dos dados;
- Reutilizar informações para fins pessoais, comerciais ou não autorizados.

A violação das obrigações de confidencialidade poderá ensejar **sanções administrativas, civis ou criminais**, conforme previsto na legislação vigente e nos contratos firmados entre as partes.

17. Disposições Finais

A presente Política de Privacidade tem como objetivo garantir a transparência, a segurança e a conformidade no tratamento dos dados pessoais realizados por meio da plataforma Cesla. Seu conteúdo reflete os princípios da Lei Geral de Proteção de Dados (LGPD), as práticas de governança da Cesla Tecnologia e os compromissos firmados com nossos clientes, usuários e parceiros.

A Cesla Tecnologia compromete-se a manter esta Política atualizada, de acordo com mudanças legais, contratuais, tecnológicas ou operacionais que impactem o ciclo de vida dos dados pessoais tratados.

Qualquer atualização relevante será comunicada pelos canais institucionais da Cesla, e estará sujeita à nova validação por parte dos responsáveis legais e técnicos da empresa.

Ao utilizar os serviços da Cesla, o usuário declara estar ciente e de acordo com as diretrizes aqui estabelecidas, bem como com seus direitos e deveres relacionados ao uso dos dados pessoais.

18. Revisão e Aprovação

Revisão Técnica:

- **Silvia Adriana Silvestrini** — *Chief Product Officer (CPO)*
  - Responsável técnica principal.

Aprovação Executiva:

- **Cleber Candido Eduardo** — *Chief Executive Officer (CEO)*
  - Responsável institucional.

ENGLISH VERSION – OFFICIAL TRANSLATION

1. Introduction

Effective as of August 14, 2025.

This Privacy Policy aims to demonstrate the commitment of Cesla Tecnologia, registered under CNPJ No. 57.813.530/0001-76, headquartered in Campinas/SP, to the privacy, protection, and processing of personal data collected through the Cesla platform and its respective modules.

This document has been prepared in accordance with Law No. 13.709/2018 – General Data Protection Law (LGPD), reinforcing Cesla Tecnologia' responsibility as the controller of the personal data processed within the scope of its services.
By using our systems, the data subject acknowledges that Cesla Tecnologia may carry out operations of collection, storage, use, and sharing of data, as described in this Policy.

For questions, requests, or complaints related to the processing of personal data, the data subject may contact the Data Protection Officer (DPO) via the email dpo@intuix.com .

2. Glossary

To facilitate your reading and understanding of this Privacy Policy, below is a summary of definitions of terms frequently used throughout this document:

- **Data Owner:** A natural person to whom the personal data that is the object of processing refers.
- **Controller:** A natural or legal person, whether governed by public or private law, who is responsible for decisions regarding the processing of personal data. In the context of Cesla, this is usually the client contracting the license.
- **Data Operator:** A natural or legal person who processes personal data on behalf of the controller. Cesla Tecnologia acts as the processor of Cesla.
- **Personal Data:** Information relating to an identified or identifiable natural person, such as name, taxpayer ID (CPF), email, IP address, among others.
- **Sensitive Personal Data:** Personal data about racial or ethnic origin, religious belief, political opinion, health, sex life, biometrics, among others, whose protection is reinforced by the LGPD.
- **GDPL (General Data Protection Law):** Law No. 13.709/2018, which regulates the processing of personal data in Brazil, including in digital media.
- **Access Token:** An encrypted code used to authenticate user sessions on the platform, with limited validity and controlled renewal.
- **SSO (Single Sign-On):** A mechanism that allows the user to access multiple systems with a single centralized authentication, used via Entra ID and FusionAuth in Cesla.
- **MFA (Multi-Factor Authentication):** An additional security layer requiring more than one verification factor (such as password + verification code) for authentication.
- **Audit Logs:** Automatic records of actions performed by users on the platform, containing information such as login, timestamp, IP address, executed action, among others.
- **SIEM (Security Information and Event Management):** A system for monitoring and analyzing security events, used to detect and respond to possible threats and incidents.
- **Incident Response Plan (IRP):** A document defining how Cesla detects, responds to, and documents security incidents that impact data or platform systems.
- **Business Continuity Plan (BCP):** A governance structure and processes adopted to maintain or restore Cesla's essential services in the event of critical failures or disasters.
- **Contractor – Service Provider Company (EPS):** An organization contracted by Cesla's client to perform operational activities. Its data and documents are managed in a segregated environment under its own licensing.

3. Purpose

This Privacy Policy aims to clearly and transparently establish the guidelines adopted by WS Solutions for the processing of personal data carried out through the Cesla platform.

This document describes how data is collected, used, stored, shared, and protected, ensuring compliance with the General Data Protection Law (Law No. 13.709/2018 – LGPD), as well as respect for the principles of security, privacy, and the informational self-determination of data subjects.

By defining these guidelines, Cesla reinforces its commitment to:

- Transparency in the use of personal data;
- Protection of the integrity, confidentiality, and availability of information;
- Guaranteeing the rights of data subjects;
- And the shared responsibility among all parties interacting with the platform, including clients, service providers (EPSs), partners, and employees.

4. Scope

This Privacy Policy applies to all users who interact with the Cesla platform, through its web or mobile modules, including:

- Clients contracting the license to use the platform;
- Employees of the Contrators (Service provider companies - EPSs) registered by the clients;
- Partners authorized to operate specific functionalities of the solution;
- And Cesla employees who, in the course of their duties, have access to personal data processed on the platform.

It also covers the processing of data carried out by Cesla technical, administrative, support, implementation, information security, and product management teams, in accordance with the roles of controller and processor defined contractually.

5. Data Collected

The Cesla platform may collect and process personal data of different types, depending on the user's use and profile. The main groups of data processed include:

- **Identification Data:** Full name, corporate email, nacional ID (CPF), phone number, associated company, position/function, and other basic registration information.
- **Authentication and Access Data:** Username (login), session tokens, authentication via SSO (Single Sign-On), multi-factor authentication (MFA), login logs, and access time records.
- **Browsing and Platform Usage Data:** IP address, dates and times of access, records of actions performed within modules, menus accessed, and operations executed.
- **Operational Data:** Information entered in forms, assigned permissions, document uploads, interactions with APIs, responses to checklists, and comments added to the platform.
- **Device and Connection Technical Data:** Device type, browser used, operating system, screen resolution, and network/internet data used during navigation.

The collection and processing of this data are intended to ensure traceability, security, proper service delivery, and compliance with contractual and legal obligations.

6. Purpose of Processing

The personal data collected on the Cesla platform are processed in accordance with the principles of necessity, purpose, security, and accountability, with the following main purposes:

- Ensuring the technical operation of the platform, including user authentication, permission management, session control, and data integrity;
- Guaranteeing information security through the application of access controls, activity logs, traceability, and incident response;
- Complying with legal, contractual, and regulatory obligations related to third-party management, qualification of service providers, occupational health and safety, among others;
- Supporting operational continuity and disaster recovery plans, as set out in the Business Continuity Plan (BCP);
- Monitoring and auditing platform usage, promoting compliance with internal policies and customer requirements;
- Personalizing and improving the user experience based on their access and interactions within the Cesla modules.

6.1. Processing of Sensitive Personal Data

Depending on the context of platform use and the nature of the data entered by clients and contractors (Service providers - EPSs), sensitive personal data may be processed, such as health information, occupational hearth certificate (ASO), training certificates, and documents required for legal and operational purposes.

This data is processed with:

- A legitimate and previously defined purpose;
- Technical and administrative access restrictions;
- Appropriate security and confidentiality controls;
- And a compatible legal basis, in accordance with the agreements established between Cesla, the contracting client, and the involved parties.

7. Data Sharing

Cesla may share personal data processed on the platform with third parties strictly necessary for the provision of services or compliance with legal and contractual obligations. Data may be shared:

- With service providers contracted for infrastructure (e.g., Azure, EVEO) and security (e.g., Cloudflare, Firebase);
- With competent authorities, as required by law;
- With the client contracting the license, when applicable, respecting the contractual purpose;
- With partner systems designated by the client, for the purpose of integration with access control, reception, occupational health, occupational safety, and similar tools.

The responsibility for documenting and justifying such integrations lies exclusively with the contracting client and the contractor (Service provider companies -EPSs), who must execute the appropriate agreements and amendments with the respective third parties involved.

7.1. Guarantee of Security and Privacy in Data Sharing

The responsibility for applying contractual clauses, privacy policies, and other legal safeguards with partner systems designated by the client—such as access control tools, reception, on-boarding and EH&S (Environment, Health and Safety) is exclusively that of the client contracting the Cesla platform.

It is the client's responsibility to ensure that such third parties comply with the GDPL and other applicable regulations through technical validations, contractual agreements, and confidentiality obligations established between the parties.

On the other hand, the service providers contracted by Cesla to support Cesla's infrastructure (such as Azure, EVEO, Cloudflare, and Firebase) are contractually obligated to guarantee adequate levels of information security and privacy protection compatible with Cesla' internal standards.

These parties are required to adhere to specific obligations, such as:

- Confidentiality of the information processed;
- Use limited to the contracted purpose;
- Implementation of technical and organizational controls to ensure the integrity, availability, and confidentiality of personal data.

Cesla carries out, whenever necessary, technical and contractual validations to ensure that its direct partners comply with the GDPL, ISO/IEC 27001/27035 standards, and other applicable guidelines.

8. Information Security

Cesla adopts rigorous technical and organizational measures to ensure information security and the protection of personal data processed on the Cesla platform. Among the main controls implemented are:

- Authentication via SSO with mandatory MFA (FusionAuth and Entra ID) for Cesla employees;
- Data encryption at rest (SHA-512) and in transit (TLS 1.2+ with an additional AES-256-CBC layer);
- Authenticated sessions with expirable and traceable tokens;
- Audit logs retained for a minimum of 5 years;
- Monitoring and protection with tools such as SIEM, WAF, Fail2Ban, Jump Server, and environment segregation (production, staging, QA, development).

User authentication on the Cesla platform occurs through two distinct models:

- Clients integrated with Entra ID perform login via federated authentication (SSO), using their own corporate environment's security and identity controls.
- Clients without Entra ID integration and users linked to Contractors (Service Provider Companies - EPSs) are registered directly on the Cesla platform by the license administrators (client or EPS), who also define access profiles and specific permissions according to the user's role and responsibilities.

Regardless of the authentication model, access to the platform requires the use of strong passwords and multi-factor authentication (MFA), ensuring traceability and continuous access control.

9. User Rights (Data Subject Rights)

In accordance with the General Data Protection Law (GDPL – Law No. 13.709/2018), users of the Cesla platform, as data subjects, are guaranteed the right to:

- Request confirmation of the existence of processing of their data;
- Access the stored data and receive clear information about its purpose;
- Request the correction of incomplete, inaccurate, or outdated data;
- Request the anonymization, blocking, or deletion of unnecessary or excessive data;
- Obtain information about data sharing with third parties;
- Request data portability, subject to commercial and industrial confidentiality;
- Revoke previously provided consents, when applicable;
- Object to the processing of data carried out on the basis of legitimate interests, when applicable.

These rights may be exercised free of charge and at any time by submitting a request through the official channels:

📧 **dpo@intuix.com**
📞 **0800 002 3752 (business hours)**

Requests will be reviewed in accordance with applicable legal timeframes and limitations and may require identity verification of the data subject to protect against unauthorized access.

10. Storage and Retention

The personal data collected through the Cesla platform are stored in a secure cloud environment (Microsoft Azure and EVEO), with periodic backups (full and incremental) and a minimum retention period of 90 days.

Cesla adopts different retention policies depending on the data subject's role and the type of data processed:

- Data linked to the contracting client's account (e.g., administrators, operators, and technical managers): retained for up to 2 years after contract termination, or as established in the contract.
- Data of contractors (Service providers - EPSs) registered by the client, including personal data of employees and qualification documents (such as medical reports, training records, Health certificate, training certificates, etc.):
    - Remain accessible in a segregated environment with specific licensing for up to 2 years after the termination of the Contractor´s contract.
    - After this period, the contractor license is deactivated, but the data is retained for a minimum period of 20 years exclusively for legal, regulatory, and labor purposes, in accordance with the agreements established between Cesla and the client.

Login records, audit trails, and traceability logs are retained for a minimum of 5 years, in line with security best practices and the requirements of ISO/IEC 27001 and 27035 standards.

10.1. International Data Transfers

Cesla may carry out international transfers of personal and corporate data when necessary for the operation of its services, in full compliance with the provisions of the Brazilian General Data Protection Law (Law No. 13.709/2018) and other applicable legislation.

Currently, such transfers occur in the following cases:

- Backup storage: part of the Cesla platform backups is stored in Microsoft Azure datacenters located in the United States (Central US region), protected according to international information security standards, including AES-256-CBC encryption in transit and SHA-512 encryption at rest, and certified under ISO/IEC 27001:2022.
- Document and image storage: files uploaded and processed by the platform (including images, evidence, and documents) may be stored in Cloudflare R2, with globally distributed servers, ensuring that transfers and processing follow adequate technical and organizational measures to protect data.
- All providers used adopt standard contractual clauses, international certifications (such as ISO/IEC 27001), and security mechanisms compatible with LGPD requirements.
- Whenever applicable, Cesla applies complementary measures such as pseudonymization and strict access control to reduce risks in international data transfers.

11. Responsibilities of the Contracting Client and Contractor´s (Service Provider Companies - EPSs)

Cesla, as the processor of personal data processed through the Cesla platform, operates under the instructions and purposes defined by the contracting clients, who are the controllers of the information entered in their respective environments.

It is the exclusive responsibility of the contracting clients and the service provider companies (EPSs) to:

- Ensure that there is a valid legal basis for processing the personal data entered into the Cesla platform, including obtaining consent when applicable.
- Inform their employees, contractors, or any data subjects that their data may be shared with Cesla and, when necessary, with other partners designated by the client, such as access control companies, reception services, occupational health providers, occupational safety providers, and similar entities.
- Include appropriate contractual clauses acknowledging that the personal data and documents submitted may be used for qualification, traceability, auditing, and operational safety purposes, in accordance with the requirements of the client's agreement.

Cesla is not responsible for any lack of proper formalization between the client, their suppliers/contractor´s (EPSs), and the registered employees, and any claims by data subjects must be initially addressed with the controller responsible for the processing.

12. Incident and Non-Compliance Reporting

All users of the Cesla platform—including clients, contractors (Service provider companies - EPSs), and internal Cesla employees—must take an active role in identifying and reporting any situation that poses a risk to information security or compliance with the GDPL.

In the event of identification or suspicion of:

- Leakage or unauthorized access to personal data;
- Anomalous behavior in the system or relevant technical failures;
- Unauthorized data sharing;
- Misuse of credentials or access permissions;
- Contractual or legal non-compliance related to data processing;
- Security failures in authentication, permissions, or information integrity;
- Non-compliance with the LGPD or applicable contractual clauses.

The incident must be reported immediately to the Cesla team, preferably through the official user support channels or by direct contact with the Data Protection Officer (DPO) via the email dpo@intuix.com , in order to enable containment and appropriate handling.

Cesla user support channels (Brasilia Business hours – Monday to Friday, 8 AM to 5 PM (GMT -3)):

- **E-mail:** suporte@ws-solution.com
- **WhatsApp:** +55 (19) 9 9331-2498
- **Phone:** 0800 002 3752

Cesla maintains an Incident Response Plan (IRP) aligned with ISO/IEC 27035, ISO/IEC 27001 standards, and Brazilian legislation, ensuring formal procedures for the detection, containment, analysis, communication, and remediation of information security incidents.

The use, sharing, or storage of data that has been improperly accessed is expressly prohibited. Any violation of this guideline may result in civil, criminal, and contractual liability, in accordance with current legislation and the commitments made to data subjects.

13. Intellectual Property

All intellectual property rights related to the Cesla platform, including its modules, functionalities, interface, data structure, operational flows, brand, visual identity, source code, databases, and other technical components, are the exclusive property of Cesla.

It is expressly prohibited for any user, client, service provider company (EPS), or third party to:

- Reproduce, copy, modify, decompile, reverse engineer, or create derivative works based on any Cesla module or functionality;
- Use the system for purposes not contractually authorized or outside the scope of the granted license;
- Transfer, assign, or sublicense the use of the platform without prior formal authorization from Cesla.

The contracting of the Cesla platform license grants the client a non-exclusive, non-transferable right of use limited to the contractual period, as defined in the current commercial agreement.

Any misuse may result in civil, criminal, and administrative liability, in addition to sanctions provided for in the terms of use, the contract, and applicable law.

14. Data Protection Officer (DPO)

Cesla has appointed a Data Protection Officer (DPO), responsible for serving as the communication channel between Cesla, data subjects, the National Data Protection Authority (ANPD), and other interested parties.

The DPO is responsible for:

- Receiving and responding to data subject requests, as provided by the GDPL;
- Providing clarifications regarding the processing of personal data carried out on the Cesla platform;
- Guiding employees and partners on data protection practices;
- Overseeing the organization’s compliance with the GDPL guidelines and other applicable regulations;
- Supporting audits, investigations, and continuous improvement initiatives related to privacy and information security.

To contact the Cesla DPO, please use the official channel: dpo@intuix.com

15. Updates and Revisions

This Privacy Policy will be reviewed periodically, at least annually, or whenever the following occur:

- Significant changes in applicable legislation, especially those related to personal data protection;
- Updates to the services, features, or modules of the Cesla platform that impact data processing;
- Relevant changes in internal processes regarding information security, privacy, or data governance.

All updates will be recorded with version control, and when involving significant changes that impact data subjects, they will be duly communicated through Cesla's official channels.

The most recent version of the Policy will always be available for consultation.

16. Confidentiality

All information and personal data processed on the Cesla platform are considered confidential and protected against unauthorized access, use, or disclosure.

Cesla adopts rigorous technical and administrative measures to preserve the confidentiality of data entered by clients, EPSs, and users, including:

- Confidentiality agreements with employees and partners;
- Access controls based on roles and operational needs;
- Continuous monitoring of sessions and activity records;
- Encryption and environment segregation.
  It is prohibited for any user, employee, or third party to:

- Share or use data accessed improperly;
- Disclose information processed on the platform without formal authorization from the data controller;
- Reuse information for personal, commercial, or unauthorized purposes.

Violation of confidentiality obligations may result in administrative, civil, or criminal sanctions, as provided by applicable law and the agreements established between the parties.

17. Final Provisions

This Privacy Policy aims to ensure transparency, security, and compliance in the processing of personal data carried out through the Cesla platform. Its content reflects the principles of the General Data Protection Law (GDPL), the governance practices of Cesla, and the commitments made with our clients, users, and partners.

WS Solutions is committed to keeping this Policy up to date in accordance with legal, contractual, technological, or operational changes that impact the life cycle of the personal data processed.

Any relevant updates will be communicated through Cesla's official channels and will be subject to new validation by the company's legal and technical representatives.

By using Cesla's services, the user declares that they are aware of and agree with the guidelines established herein, as well as with their rights and responsibilities related to the use of personal data.

18. Review and Approval

Technical Review:

- Silvia Adriana Silvestrini — Chief Product Officer (CPO)
  - Principal technical responsible person.

Executive Approval:

- Cleber Candido Eduardo — Chief Executive Officer (CEO)
  - Institutional responsible person.

Campinas, 14 de Agosto de 2025.

gov.br Documento assinado digitalmente
SILVIA ADRIANA SILVESTRINI EDUARDO
Data: 14/08/2025 16:53:08-0300
Verifique em https://validar.iti.gov.br

Silvia Adriana Silvestrini
CPO – Chief Product Officer
Technical Responsible

gov.br Documento assinado digitalmente
CLEBER CANDIDO EDUARDO
Data: 14/08/2025 17:01:00-0300
Verifique em https://validar.iti.gov.br

Cleber Candido Eduardo
CEO – Chief Executive Officer
Institucional Responsible