

PROVVI

Tecnologia de Autenticidade de Imagens

Autenticidade como Infraestrutura de Compliance:

C2PA e ICP-Brasil como resposta ao PL 3507/2025

Vistoria Veicular e a Prova Criptográfica que a Lei vai Exigir

Produzido pelo Comitê de Tecnologia e Compliance da Provvi · Março de 2026

PROBLEMA CENTRAL

Laudos de vistoria veicular são documentos digitais sem prova criptográfica de autenticidade. O PL 3507/2025 exigirá rastreabilidade e integridade — mas a regulamentação técnica ainda não foi definida.

SOLUÇÃO PROPOSTA

O padrão C2PA (Coalition for Content Authenticity and Provenance), com assinatura ICP-Brasil, oferece uma cadeia de custódia criptograficamente verificável — desde a captura da imagem até a emissão do laudo.

provvi.com.br · contato@provvi.com.br

Sumário Executivo

O setor de vistoria veicular brasileiro opera sobre uma premissa silenciosa e perigosa: que as imagens registradas durante uma inspeção são autênticas. Essa premissa nunca foi tecnicamente garantida.

Com o avanço do PL 3507/2025 — aprovado na Comissão de Viação e Transportes da Câmara e em tramitação na CCJ — o Brasil caminha para um regime de vistoria periódica obrigatória que transformará o volume de laudos emitidos por Empresas Credenciadas de Vistoria (ECVs) de milhões para dezenas de milhões por ano. Cada laudo será um documento jurídico. Cada imagem que o compõe precisará ser defensável.

Este whitepaper apresenta três argumentos centrais:

- O PL 3507/2025 cria uma demanda regulatória implícita por rastreabilidade digital de laudos que as soluções atuais não atendem.
- O padrão C2PA (Coalition for Content Authenticity and Provenance), com assinatura via ICP-Brasil, é a infraestrutura técnica que responde a essa demanda — e já é adotada globalmente por Adobe, Microsoft, Google, Reuters e BBC.
- A implementação via SDK nativo é viável sem substituição de sistemas existentes, com integração na camada de captura de imagem.

Para ECVs, o argumento é de diferenciação competitiva e redução de risco jurídico. Para seguradoras de automóvel, é de qualidade probatória da evidência que fundamenta decisões de sinistro. Para o Detran e reguladores, é de infraestrutura de auditoria digital que o novo marco legislativo vai exigir.

1. O Contexto Regulatório: O Que o PL 3507/2025 Realmente Muda

1.1 O Estado Atual da Vistoria Veicular no Brasil

A vistoria veicular no Brasil é hoje uma atividade regulada pelo Conselho Nacional de Trânsito (Contran), executada por Empresas Credenciadas de Vistoria (ECVs) credenciadas pelos DETRANs estaduais. Na prática, a vistoria ocorre principalmente em momentos pontuais: transferência de propriedade, recuperação de veículo roubado e casos de suspeita de clonagem.

O fluxo operacional típico envolve um vistoriador que fotografa o veículo com um dispositivo móvel, insere os dados em um sistema de gestão da ECV, e gera um laudo digital que é transmitido ao DETRAN. A questão técnica que nenhum regulamento atual responde: como provar que a imagem registrada no laudo é a mesma imagem capturada no momento da vistoria, no local declarado, pelo dispositivo credenciado?

Ponto crítico: O laudo digital atual é tão defensável quanto um documento Word. A imagem pode ser substituída entre a captura e o upload. Os metadados podem ser alterados. O sistema de gestão da ECV pode ser comprometido. Não há prova criptográfica de autenticidade em nenhuma dessas etapas.

1.2 O Que o PL 3507/2025 Propõe

O Projeto de Lei 3507/2025, de autoria do deputado Fausto Pinato (PP-SP), altera o Código de Trânsito Brasileiro para consolidar e ampliar as regras de vistoria veicular. O substitutivo aprovado na Comissão de Viação e Transportes foi relatado pelo deputado Cezinha de Madureira (PSD-SP), que em dezembro de 2025 foi também designado relator do projeto na Comissão de Constituição e Justiça e de Cidadania (CCJ) — sinal de continuidade política e de apoio consistente ao texto ao longo de sua tramitação. O substitutivo introduz mudanças significativas:

1. Vistoria periódica obrigatória para veículos com mais de cinco anos de fabricação, com periodicidade a ser definida pelo Contran (anual ou bienal).
2. Obrigatoriedade ampliada nas situações de transferência de propriedade, recuperação de veículo roubado e suspeita de clonagem.
3. Criação de infração grave específica para condução de veículo sem vistoria em dia, com multa de R\$ 195,23, cinco pontos na CNH e retenção do veículo.
4. Integração da verificação de segurança com controle de emissão de poluentes e ruído — fiscalização que hoje ocorre de forma esporádica.
5. Proteção do comprador de veículo usado, com possibilidade de vistoria prévia e ressarcimento do custo pelo vendedor em caso de reprovação.

O projeto tramita em caráter conclusivo e, com a designação do mesmo relator tanto na CVT quanto na CCJ, mantém continuidade técnica e política em sua análise. A expectativa do setor é que a tramitação se consolide ao longo de 2026, com vigência plena em 2027.

1.3 O Problema que o PL Não Resolve — e que Vai Criar

O PL 3507/2025 estabelece o quê: quais veículos, quando, por quem, com quais consequências. Ele não estabelece o como técnico da emissão e verificação de laudos. Essa lacuna será preenchida por regulamentação do Contran — e é exatamente nessa regulamentação que o debate sobre rastreabilidade digital de imagens vai acontecer.

Mas há um problema de escala que aparece antes da regulamentação técnica. Se hoje o Brasil emite alguns milhões de laudos por ano nas situações pontuais existentes, a vistoria periódica obrigatória de veículos com mais de cinco anos — estimados em mais de 40 milhões de unidades —

multiplicará esse volume por uma ordem de grandeza. Um número muito maior de laudos significa um alvo muito maior para fraude.

Projeção de escala: Se o Brasil tem aproximadamente 50 milhões de veículos em circulação e estima-se que cerca de 70% têm mais de 5 anos, a vistoria bienal obrigatória representaria em torno de 17 milhões de laudos por ano — contra um volume atual de poucos milhões. Cada laudo fraudado é uma externalidade que o sistema de seguros e o poder público pagam.

2. A Fraude que Escala com o Volume

2.1 Os Vetores de Fraude em Laudos de Vistoria

Antes de apresentar a solução, é necessário ser preciso sobre o problema. Fraude em vistoria veicular não é um fenômeno hipotético — é uma realidade operacional com padrões conhecidos:

Substituição de imagem pós-captura

O vistoriador captura a imagem de um veículo legítimo. Antes do upload ao sistema da ECV, a imagem é substituída por uma de outro veículo — um com menos danos, placa diferente, ou características distintas. Sem prova criptográfica de que a imagem não foi alterada após a captura, essa substituição é indetectável pelo sistema.

Reutilização de imagem legítima

Uma imagem autêntica de uma vistoria anterior, de outro veículo, ou de um banco de imagens é inserida em um novo laudo. O arquivo tem aparência legítima, os metadados básicos são consistentes, mas a imagem não corresponde ao veículo vistoriado naquele momento.

Captura de tela ou re-fotografia

Uma imagem exibida em tela — de um veículo diferente, sem os danos que deveriam ser documentados — é fotografada como se fosse a captura original. Técnicas de detecção de re-fotografia (análise de padrão Moiré, reflexo especular, aberração cromática) existem, mas precisam estar integradas no momento da captura.

Manipulação de localização

O laudo declara que a vistoria ocorreu em um endereço específico, mas a imagem foi capturada em outro local. Sem verificação de GPS no momento da captura — integrada de forma imutável ao arquivo —, a localização declarada não tem sustentação técnica.

2.2 Por Que as Soluções Atuais São Insuficientes

As ECVs operam hoje com sistemas de gestão que implementam controles básicos: login do vistoriador, registro de timestamp do sistema, campos obrigatórios. Esses controles têm uma característica em comum: são todos passíveis de contorno por um agente interno malicioso ou por comprometimento do sistema de gestão.

Controle Atual	O Que Protege	O Que Não Protege
Login do vistoriador	Identifica quem fez o upload	Não prova que a imagem é do dispositivo credenciado
Timestamp do sistema	Registra quando o upload ocorreu	Não prova quando a imagem foi capturada
GPS declarado	Registra localização informada	Não vincula criptograficamente local à imagem
Hash do arquivo	Detecta alteração após o upload	Não detecta substituição antes do upload

A lacuna crítica é a seguinte: todos os controles atuais protegem o arquivo após ele entrar no sistema. Nenhum deles protege o momento entre a captura da câmera e a entrada no sistema — que é exatamente onde a fraude acontece.

Vale distinguir esse ponto de uma confusão frequente no mercado: soluções baseadas em IA de visão computacional — reconhecimento de placa, análise de cor, detecção de inconsistências de

iluminação — operam de forma reativa. Elas tentam inferir, a partir do conteúdo da imagem, se ela é provavelmente autêntica. É uma análise probabilística: a IA estima a chance de fraude, mas não pode provar que a foto é real. C2PA opera de forma proativa e determinística: não tenta adivinhar — prova matematicamente, por meio de criptografia assimétrica, que aquela imagem foi capturada por aquele dispositivo, naquele local, naquele instante, sem alterações posteriores. Uma imagem com manifesto C2PA válido não é "provavelmente autêntica". É verificavelmente autêntica. As duas abordagens não são mutuamente exclusivas — mas apenas a segunda oferece garantia jurídica robusta.

IA de imagem vs. C2PA: Sistemas de visão computacional respondem à pergunta "essa imagem parece autêntica?". C2PA responde à pergunta "essa imagem é provadamente autêntica?". A diferença não é de grau — é de natureza. Em um contexto regulatório e jurídico, apenas a segunda resposta tem validade como prova.

3. C2PA: O Padrão Global de Proveniência de Conteúdo

3.1 O Que é C2PA

C2PA (Coalition for Content Authenticity and Provenance) é um padrão aberto de especificação técnica desenvolvido pela Coalition for Content Authenticity and Provenance — um consórcio que reúne Adobe, Microsoft, Google, Intel, Arm, Sony, BBC, Reuters, Associated Press e mais de 300 organizações. Não é um produto proprietário: é uma especificação pública que define como metadados de proveniência devem ser estruturados, assinados e verificados.

O que diferencia C2PA de uma assinatura digital simples é que ele registra a história do conteúdo — não apenas o estado final. Um manifesto C2PA contém:

- Identidade do dispositivo de captura (hardware e software)
- Timestamp criptograficamente vinculado ao momento da captura
- Localização GPS integrada ao arquivo, não ao sistema de gestão
- Hash SHA-256 do frame original, calculado antes de qualquer compressão
- Asserções de negócio customizáveis — incluindo dados do vistoriador, placa do veículo, tipo de inspeção
- Cadeia de assinaturas: local (dispositivo) e backend (autoridade certificadora)

Qualquer alteração no arquivo — desde a substituição de um pixel até a modificação de um metadado — invalida a assinatura e quebra a cadeia de custódia. Isso é detectável por qualquer verificador compatível com o padrão, sem necessidade de acesso ao sistema de origem.

Analogia jurídica: Um manifesto C2PA equivale a uma ata notarial contínua que começa no momento em que o obturador da câmera é acionado e acompanha o arquivo por toda a sua vida útil. Qualquer intervenção posterior deixa rastro verificável.

3.2 C2PA + ICP-Brasil: A Combinação com Validade Jurídica

Para o contexto brasileiro, C2PA resolve a integridade técnica. A validade jurídica plena exige a integração com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), o sistema de certificação digital reconhecido pela legislação nacional para documentos eletrônicos com validade jurídica equivalente ao documento físico assinado.

A arquitetura de assinatura em dois estágios funciona da seguinte forma:

Etapa	Onde ocorre	O que produz
1	Dispositivo móvel (momento da captura)	Hash SHA-256 do frame RAW, GPS, timestamp, manifesto C2PA assinado localmente — prova de integridade do dispositivo
2	Backend seguro (AWS KMS + certificado ICP-Brasil)	Re-assinatura com certificado ICP-Brasil via ECDSA P-256 — validade jurídica plena reconhecida pela legislação brasileira
Resultado	Manifesto duplamente assinado	Imagem com cadeia de custódia completa: integridade + proveniência + validade jurídica

3.3 Verificação Independente

Um diferencial crítico do padrão C2PA é que a verificação é independente do sistema que gerou o documento. Qualquer verificador compatível — incluindo uma ferramenta pública disponível online

— pode confirmar a autenticidade de uma imagem sem precisar acessar o banco de dados da ECV ou do DETRAN.

Isso tem uma implicação direta para o contexto de auditoria regulatória: um fiscal do Detran, um perito judicial, ou uma seguradora podem verificar a autenticidade de um laudo a partir do arquivo, sem depender de cooperação do sistema de origem. A evidência é autossuficiente.

4. Aplicação ao PL 3507/2025: Uma Resposta Técnica à Demanda Regulatória

4.1 O que a Regulamentação do Contran vai Precisar Definir

O PL 3507/2025, se aprovado, delega ao Contran a definição dos critérios técnicos da vistoria periódica. Com base nos precedentes regulatórios de inspeção veicular em outros países e na tendência de digitalização de laudos já observada no estado de São Paulo, é possível antecipar as exigências que virão:

- Rastreabilidade do laudo: capacidade de provar que as imagens no laudo correspondem à vistoria declarada.
- Integridade do documento: garantia de que o laudo não foi alterado após a emissão.
- Vinculação entre imagem e localização: evidência de que a captura ocorreu no endereço declarado.
- Cadeia de responsabilidade: registro auditável de quem capturou, quem emitiu e quando.
- Verificação de autenticidade por terceiros: capacidade de auditar o laudo sem acesso ao sistema da ECV.

C2PA com ICP-Brasil atende a todos esses critérios com uma única camada de infraestrutura adicionada ao processo de captura. Não requer substituição do sistema de gestão da ECV — apenas a integração de um SDK nativo no dispositivo de captura.

4.2 O Fluxo Operacional com C2PA

O processo de vistoria com autenticidade C2PA preserva o fluxo existente da ECV, adicionando a camada de proveniência de forma transparente para o vistoriador:

#	Ação do Vistoriador	O que ocorre na camada C2PA
1	Abre o app de vistoria e autentica	SDK verifica integridade do dispositivo e do aplicativo
2	Posiciona câmera no veículo	GPS é capturado e vinculado à sessão de captura
3	Aciona a câmera	Hash SHA-256 calculado do frame RAW antes da compressão JPEG
4	Imagem é processada	Manifesto C2PA gerado com hash, GPS, timestamp e identidade do dispositivo
5	App envia laudo ao sistema	Upload do arquivo + manifesto para backend; re-assinatura KMS com certificado ICP-Brasil
6	Laudo emitido	Arquivo final com cadeia de custódia completa e verificação pública disponível

4.3 Benefícios por Stakeholder

Para Empresas Credenciadas de Vistoria (ECVs)

- Diferenciação competitiva: laudo com validade jurídica superior aos concorrentes sem a camada de autenticidade.
- Redução de risco de responsabilidade: em caso de contestação de laudo, a ECV tem evidência forense de que a imagem não foi alterada.
- Preparação antecipada para regulamentação do Contran: implementar agora evita custo de adequação forçada.

- Argumento comercial para seguradoras parceiras: laudo mais confiável reduz sinistros fraudulentos, o que pode se traduzir em vantagens contratuais.

Para Seguradoras de Automóvel

- Qualidade probatória da evidência: laudos de vistoria com C2PA são defensáveis em processo administrativo e judicial.
- Redução de fraude em sinistro: correlação entre estado do veículo na vistoria e estado no momento do sinistro é verificável.
- Subsídio para precificação de risco: histórico de vistorias autenticadas enriquece o perfil de risco do veículo.
- Conformidade proativa: preparação para futuras exigências regulatórias de qualidade de evidência digital.

Para DETRANs e Reguladores

- Auditoria independente de laudos: verificação sem necessidade de acesso aos sistemas das ECVs.
- Infraestrutura de fiscalização escalável: a verificação automática de autenticidade pode ser integrada ao sistema de licenciamento.
- Rastreabilidade em investigações: em casos de fraude documentada, a cadeia de custódia C2PA fornece evidência forense admissível.

5. Implementação Técnica: O que é Necessário

5.1 Arquitetura de Integração

A implementação de C2PA em um fluxo de vistoria veicular não requer substituição de infraestrutura existente. A integração ocorre em uma camada específica: o momento de captura da imagem no dispositivo móvel do vistoriador.

Os componentes técnicos necessários são:

- SDK nativo Android e iOS — integrado ao aplicativo da ECV, substitui a câmera nativa pelo pipeline de captura autenticada.
- Backend de assinatura — serviço na nuvem que recebe o manifesto C2PA gerado pelo dispositivo e aplica a segunda assinatura com certificado ICP-Brasil via AWS KMS.
- Armazenamento de manifesto — registro imutável do manifesto assinado, associado ao laudo no sistema de gestão da ECV.
- Verificador público — endpoint que permite a qualquer parte verificar a autenticidade de um laudo a partir do `session_id` ou do hash da imagem, sem necessidade de credenciais.

5.2 Pré-requisitos para a ECV

Do lado da ECV, a integração requer:

- Aplicativo Android ou iOS existente (ou a desenvolver) para captura de imagens de vistoria.
- Conectividade de rede no momento da captura para transmissão ao backend de assinatura. O SDK opera com suporte a fila local em modo offline — a assinatura backend ocorre quando a conectividade é restaurada, com o hash local garantindo integridade durante o período offline.
- Certificado ICP-Brasil da ECV ou integração com certificado da autoridade certificadora Provvi — para assinaturas em nome da ECV credenciada.

Nota sobre offline: Em locais com conectividade limitada — garagens, pátios cobertos, áreas rurais — o SDK realiza a assinatura local completa no dispositivo, garantindo a integridade da captura. O timestamp é derivado do relógio seguro do hardware do dispositivo e vinculado criptograficamente ao hash da imagem no momento da captura — não no momento do upload. Isso impede uma forma de fraude específica ao ambiente de vistoria: a adulteração manual do relógio do celular para forjar a data ou hora do registro. Uma imagem capturada com o SDK Provvi tem sua prova de tempo selada no dispositivo, independentemente de qualquer configuração de horário feita depois. A assinatura com certificado ICP-Brasil é aplicada quando a conectividade é restaurada, sem comprometer a rastreabilidade do momento de captura.

5.3 Compatibilidade com o Padrão C2PA

O Provvi implementa o padrão C2PA usando a biblioteca de referência `c2pa-rs` (Rust, open-source, mantida pela Coalition for Content Authenticity and Provenance), garantindo interoperabilidade com qualquer verificador compatível com o padrão — incluindo o verificador público da CAI disponível em verify.contentcredentials.org.

Isso significa que um laudo gerado pelo Provvi pode ser verificado por:

- O verificador público da Provvi (provvi.com.br).

- O verificador da CAI (verify.contentcredentials.org).
- Qualquer sistema de terceiros que implemente o padrão C2PA — incluindo futuros sistemas de fiscalização do Detran.

6. Considerações sobre o Cenário Regulatório

6.1 Timing de Adoção

O PL 3507/2025 ainda tramita no Congresso. A regulamentação técnica do Contran viria após a aprovação da lei. A implementação plena de um novo padrão técnico para emissão de laudos levaria tempo adicional após a regulamentação. O ciclo completo pode ser de 2 a 3 anos.

Esse timing, à primeira vista, pode sugerir que a urgência de adoção é baixa. A leitura contrária é mais precisa: ECVs que implementarem a infraestrutura de autenticidade agora estarão operacionalmente prontas quando a regulamentação se consolidar — sem o custo e o risco de uma adequação forçada sob pressão de prazo. Mais importante: estarão posicionadas para oferecer laudos com qualidade técnica superior durante o período de transição, o que é um diferencial comercial relevante com seguradoras.

6.2 Precedentes Internacionais

A exigência de autenticidade criptográfica em documentos de inspeção veicular não é uma demanda sem precedente. Países com sistemas de inspeção veicular obrigatória consolidada — como Reino Unido (MOT), Alemanha (TÜV) e Portugal (IPO) — caminham para requisitos de integridade digital de laudos que vão além de assinatura eletrônica simples.

O padrão C2PA, originalmente desenvolvido para combate a deepfakes em contexto jornalístico, tem aplicação direta em qualquer contexto onde imagens digitais têm valor probatório — o que inclui inspeção veicular, sinistro de seguros, perícia técnica e registro regulatório.

6.3 Relação com LGPD e Proteção de Dados

O manifesto C2PA registra dados do dispositivo e localização GPS — dados que se enquadram nas categorias protegidas pela LGPD. A implementação deve observar:

- Minimização de dados e anonimização granular: o C2PA, por ser um padrão de metadados estruturados, permite controle preciso sobre quais campos do manifesto são expostos em cada contexto. É possível, por exemplo, compartilhar com um verificador externo apenas a prova de integridade e o timestamp — sem expor a identidade do vistoriador, o número do dispositivo ou as coordenadas GPS exatas. Essa capacidade de anonimização seletiva implementa o princípio de Privacidade por Design: a autenticidade da foto pode ser verificada publicamente sem que dados sensíveis do profissional responsável sejam revelados. O manifesto registra apenas os dados necessários para proveniência — hash do frame, timestamp, GPS, identidade do dispositivo — e não registra biometria do vistoriador nem dados do proprietário do veículo.
- Base legal: o tratamento ocorre no contexto de obrigação legal (vistoria regulamentada pelo Contran) e interesse legítimo da ECV (rastreadabilidade operacional).
- Retenção: os manifestos são dados de auditoria — sua retenção deve seguir os prazos definidos pela regulamentação aplicável ao setor de vistoria veicular.

7. Conclusão: A Infraestrutura que o Mercado Vai Precisar

O PL 3507/2025 é um marcador de uma tendência, não um evento isolado. O Brasil está construindo, com mais de duas décadas de atraso em relação a países europeus, um sistema de inspeção veicular com ambições de rigor técnico e consequências jurídicas reais. Esse sistema precisará, inevitavelmente, de uma infraestrutura de autenticidade digital que as soluções atuais não oferecem.

C2PA com ICP-Brasil não é uma resposta especulativa a uma regulamentação futura. É um padrão técnico maduro, adotado globalmente, que responde a uma necessidade que já existe hoje — e que o novo marco legislativo tornará urgente.

Para ECVs, a janela de adoção antecipada é uma oportunidade de diferenciação. Para seguradoras, é uma oportunidade de elevar a qualidade probatória dos laudos que fundamentam decisões de sinistro. Para reguladores, é uma infraestrutura de fiscalização que pode ser exigida sem desenvolvimento de sistema proprietário.

Próximo passo: O Provvi oferece uma demonstração técnica do pipeline completo — da captura autenticada à verificação pública — para ECVs e seguradoras interessadas em avaliar a integração. Acesse provvi.com.br ou entre em contato em contato@provvi.com.br para agendar uma demonstração.

Sobre o Provvi

O Provvi é um SDK Android e iOS de captura autenticada de imagens com validade jurídica via C2PA e ICP-Brasil. Desenvolvido para setores que precisam de evidência digital defensável — seguros, vistorias, registros regulatórios e educação —, o Provvi implementa o padrão internacional de proveniência de conteúdo com assinatura via infraestrutura de chaves públicas brasileira.

Site: provvi.com.br · Contato: contato@provvi.com.br

Sobre a Autoria

Este whitepaper foi desenvolvido pelo Comitê de Tecnologia da Provvi, composto por especialistas em criptografia, infraestrutura de chaves públicas (ICP-Brasil) e direito digital. A Provvi dedica-se ao desenvolvimento de padrões de proveniência de conteúdo para setores de alta criticidade, assegurando que a inovação tecnológica em IA e automação esteja sempre amparada por evidências digitais defensáveis e conformidade regulatória plena.

Produzido por: Comitê de Tecnologia e Compliance da Provvi · Data de Publicação: Março de 2026

Referências Regulatórias

- PL 3507/2025 — Câmara dos Deputados. Altera o Código de Trânsito Brasileiro para dispor sobre vistoria veicular.
- Resolução CONTRAN nº 716/2017 — Vistoria veicular obrigatória (histórico regulatório).
- ICP-Brasil — Infraestrutura de Chaves Públicas Brasileira, ITI/Casa Civil da Presidência da República.
- C2PA Specification v2.1 — Coalition for Content Authenticity and Provenance (contentauthenticity.org).
- CNseg — 22º Ciclo SQF: Seminário de Quantificação da Fraude em Seguros, 2024.
- LGPD — Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais.