

LAUDO PERICIAL

Processo: 00000000-07.2020.8.13.0000

Autor: Ministério Público do Estado de Algum Estado (MPAE)

Réu: Fulano de Tal (Presidente da Câmara Municipal de Cidade De Algum Lugar – MG)

LAUDO PERICIAL

No dia 08 de Dezembro de 2025, este Perito realizou a coleta da evidência digital, com metodologia e resultados apresentados nos Autos. Na sequência do trabalho pericial, no período de 08 de Dezembro de 2025 a 08 de Dezembro de 2025, em ambiente **laboratorial (CyberOne – Laboratório de Computação Forense, Perícia Computacional e Inteligência Cibernética)**, este Perito examinou o conjunto completo das evidências digitais pertinentes ao processo.

No dia 08 de Dezembro de 2025, este Perito elaborou o presente Laudo Pericial, descrevendo com verdade e com todas as circunstâncias o conjunto completo de informações que possa interessar ao Tribunal de Justiça de Algum Estado, no âmbito do processo em epígrafe. Todas as tarefas periciais foram realizadas em conformidade com o que preconiza a **Lei No. 13.105, de 16 de março de 2015, em seu Artigo 473, do Código de Processo Civil**, que, em suma, estabelece os parâmetros para elaboração de laudos periciais e pareceres técnicos periciais, que servem como diretrizes para o trabalho do Perito. A Computação Forense e a Perícia Forense Computacional consistem, basicamente, no uso de métodos técnicos e científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo. Este Perito observou o que preconiza a **Norma ABNT ISO/IEC 27037:2013**, que apresenta as diretrizes para identificação, coleta, aquisição, extração e preservação de evidências digitais em todas as etapas de um processo judicial e/ou de investigação, preservando, assim, a **cadeia de custódia**.

OBJETIVOS DA PERÍCIA

O trabalho pericial realizado por este Perito tem como objetivo geral a **Investigação, Perícia e Resposta a Incidentes em Documentos Eletrônicos e Assinaturas Digitais**, centrado na análise baseada em evidências digitais.

1. De um modo geral, os objetivos pretendem garantir a **autenticidade** (quem assinou?) e a **integridade** (houve alterações no documento após a assinatura?) do objeto pericial.
2. Para tal, os seguintes objetivos específicos foram definidos e alcançados:
3. **Verificação de Integridade:** Determinar o código HASH SHA-256 do arquivo documento.pdf , confirmando sua integridade.
4. **Análise de Metadados:** Apresentar os metadados internos e extrair o histórico de criação e edição.
5. **Análise Temporal:** Extrair o Carimbo do Tempo (Timestamp) da assinatura digital para determinar o momento exato da aposição da assinatura.
6. **Validação da Assinatura:** Verificar a autenticidade e a validade jurídica da assinatura contida no documento.
7. **Deteção de Adulteração:** Analisar a ocorrência de edição no arquivo após a inserção da assinatura digital.
8. **Elaboração do Laudo:** Responder tecnicamente aos quesitos formulados pela parte Autora.

OBJETOS PARA PERÍCIA

O material examinado por este Perito é composto pelo seguinte objeto digital, que constitui a evidência central da presente perícia:

1. Um arquivo, em formato PDF e denominado **documento.pdf**, que contém o cronograma de um ciclo de treinamentos em Inteligência Cibernética, e cuja autenticidade e integridade foram questionadas pela parte Autora.
2. A integridade do arquivo foi verificada pelo Perito, sendo o **HASH SHA-256** de Cadeia de Custódia: 0d6adc9d0863c9dfe8ca16accbb31312ef8d657205edb739a156c38df62cb973.

QUESITOS

A parte Ré, através de seus patronos, não apresentou quesitos nos autos do processo.

Os quesitos periciais (**num total de 7 – sete**), que deveriam ser analisados e respondidos por este Perito, foram apresentados pela parte autora – o **Sr. Fulano de Tal** – no documento que instrui o processo.

METODOLOGIA

O presente trabalho pericial foi conduzido em ambiente laboratorial controlado (CyberOne), seguindo o **Método Científico** de exame e preservação de evidência digital, conforme a **Norma ABNT-ISO/IEC 27037:2013**, que estabelece as diretrizes para identificação, coleta, aquisição e preservação de evidência digital.

A aplicação desta metodologia garante que o processo seja:

REPETÍVEL: Os mesmos resultados são produzidos utilizando os mesmos procedimentos, métodos e ferramentas.

AUDITÁVEL: O método científico e a técnica foram rigorosamente seguidos e documentados.

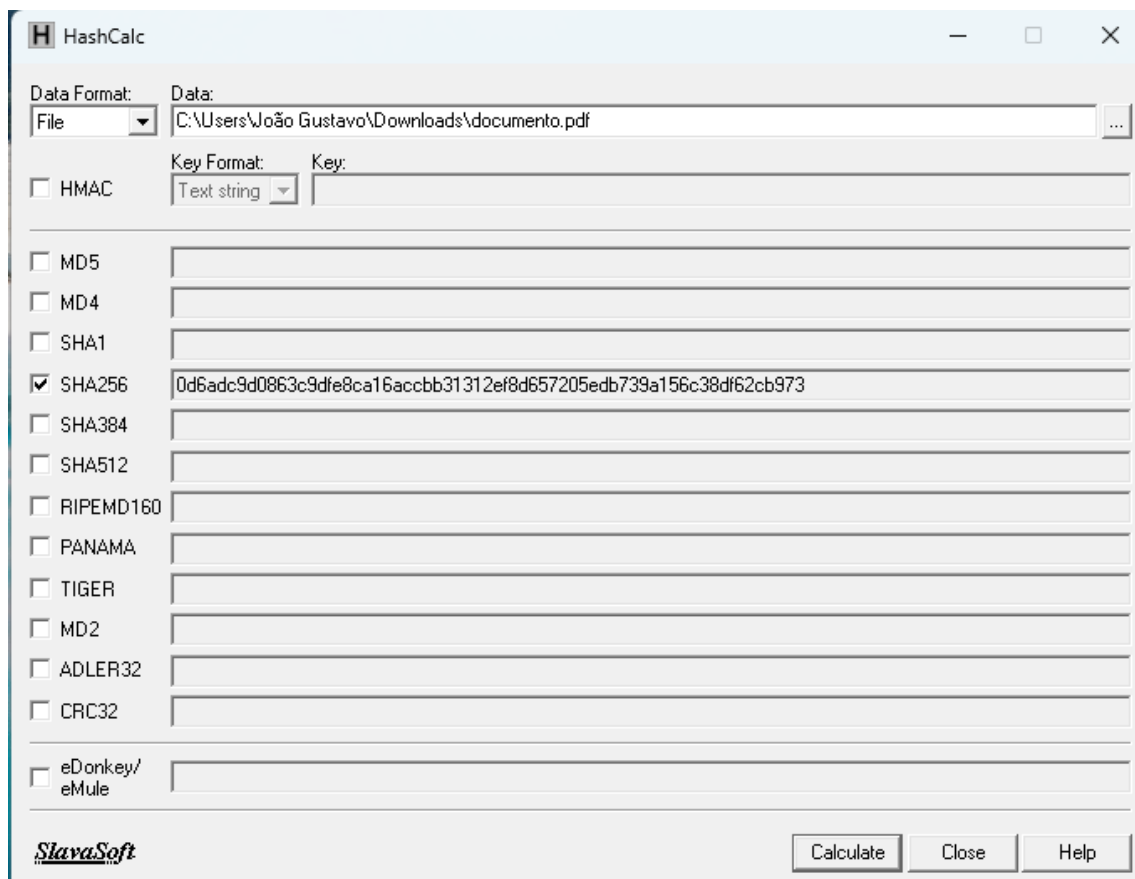
JUSTIFICÁVEL: Todas as ações e métodos utilizados são comprovados e documentados (Figura 01 a Figura 04).

As etapas da **Cadeia de Custódia** e o **Processamento Forense** do arquivo **documento.pdf** foram as seguintes:

1. Preservação da Evidência Digital

O arquivo digital foi recebido pelo Perito e imediatamente submetido ao cálculo do **código de integridade (HASH SHA-256)**, utilizando a ferramenta **HashCalc**.

O **hash** calculado (0d6adc9d0863c9dfe8ca16accbb31312ef8d657205edb739a156c38df62cb973) atesta a integridade do arquivo em custódia e serve como prova de imutabilidade.



2. Análise Técnica e Extração

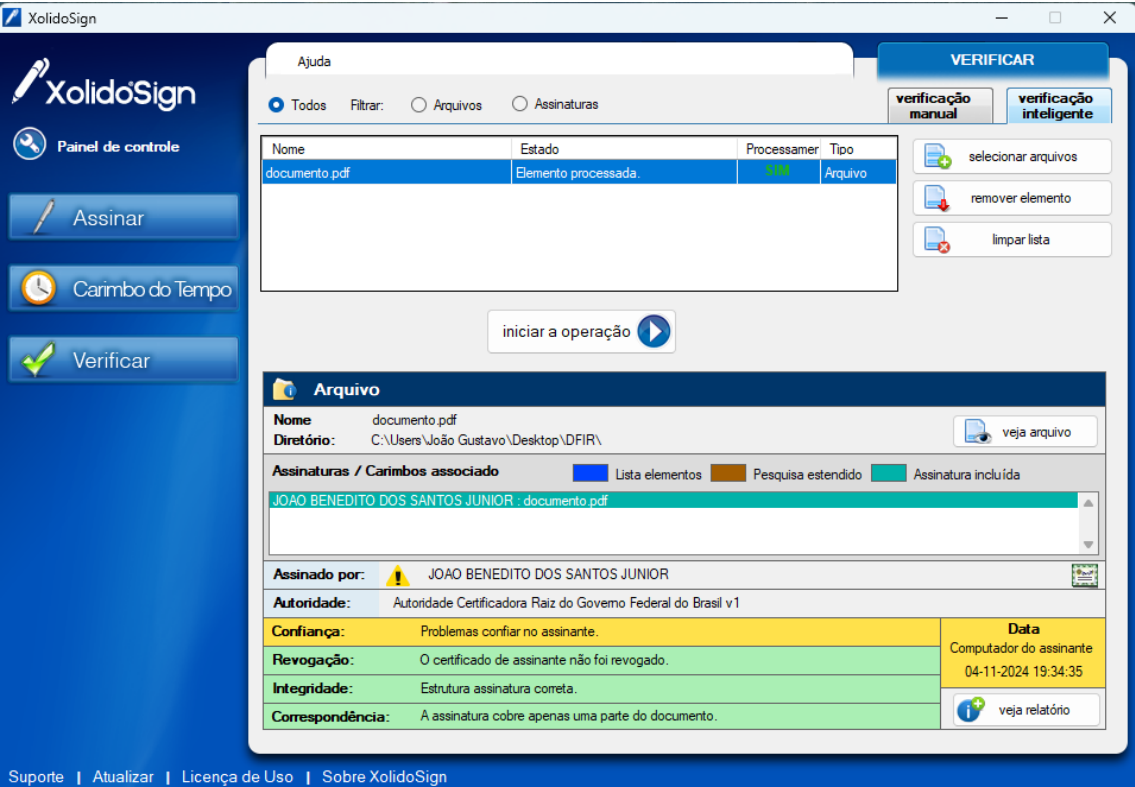
Análise de Metadados: Utilização da ferramenta **ExifTool** para extrair metadados ocultos, como software de criação, autor e timestamps de modificação e criação.

```

C:\Users\João Gustavo\Desktop\PERICIA2> exiftool documento.pdf

File Name           : documento.pdf
Directory           : .
File Size           : 340 kB
Zone Identifier      : Exists
File Modification Date/Time : 2025:12:08 14:00:44-03:00
File Access Date/Time   : 2025:12:08 16:11:27-03:00
File Creation Date/Time  : 2025:12:08 16:05:28-03:00
File Permissions      : -rw-rw-rw-
File Type           : PDF
File Type Extension   : pdf
MIME Type            : application/pdf
PDF Version          : 1.7
Linearized           : No
Has XFA              : No
Language             : pt-BR
Tagged PDF           : Yes
XMP Toolkit           : Adobe XMP Core 9.1-c001 79.675d0f7, 2023/06/11-19:21:16
Producer             : Microsoft® Word para Microsoft 365
Format               : application/pdf
Creator              : Joao Benedito dos Santos Junior
Creator Tool         : Microsoft® Word para Microsoft 365
Create Date          : 2024:11:03 23:12:02-03:00
Modify Date          : 2024:11:10 21:29:17-03:00
Metadata Date        : 2024:11:10 21:29:17-03:00
Document ID          : uuid:1C83B1EC-A104-4D24-8E20-FBDE8B0E1DF0
Instance ID          : uuid:5f996ba1-5ff7-44e2-b169-a73e167831a5
Page Count           : 5
Author               : Joao Benedito dos Santos Junior
  
```

Análise de Assinatura e Carimbo do Tempo: Utilização da ferramenta **XolidoSign** para extrair o Carimbo do Tempo e confirmar o titular da assinatura .



3. Validação Oficial

Validação de Integridade: O arquivo com a assinatura digital foi submetido ao validador oficial do Governo Federal, o validar.iti.gov.br, para verificar sua validade jurídica e integridade perante a ICP-Brasil .

Informações gerais do arquivo:

Nome do arquivo:

documento.pdf

Hash:

od6adc9do863c9dfe8ca16acbb31312ef8d657205edb739a156c38df62cb973

Data da validação:

08/12/2025 16:16:36 BRT

Informações da Assinatura:

Assinado por:

JOAO BENEDITO DOS SANTOS JUNIOR

CPF:

***.032.686-**

Nº de série de certificado emitente:

0x35bd387936e77da

Data da assinatura:

04/11/2024 19:34:35 BRT

Assinatura reprovada.

Documento modificado após a assinatura

Foram encontrados certificados expirados

ASSINATURA ELETRÔNICA

AVANÇADA

ITI

Instituto Nacional de Tecnologia da Informação

Conforme

Lei 14.063/20

gov.br

Ver Relatório de Conformidade

▼ Relatório de Conformidade

Nome: Validar

Data de validação: 08/12/2025 16:16:36 BRT

Versão do software(Verificador de Conformidade): 2.21.1.2

Versão do software(Validador de Documentos): 3.0.5.2

Fonte de verificação: Offline

▼ Informações do arquivo

Nome do arquivo: documento.pdf

Resumo da SHA256 do arquivo: 0d6adc9d0863c9dfe8ca16accbb31312ef8d657205edb739a156c38df62cb973

Tipo do arquivo: PDF

Quantidade de assinaturas: 1

Quantidade de assinaturas ancoradas: 1

> CN=JOAO BENEDITO DOS SANTOS JUNIOR

Download PDF

Expandir Elementos

RESPOSTAS AOS QUESITOS

Realizadas todas as etapas do trabalho técnico, este Perito apresenta as respostas conclusivas aos quesitos formulados e apresentados pela parte Autora..

1. Qual o formato do arquivo que contém o documento ?

O arquivo que contém o documento possui o formato **Portable Document Format (PDF)**.

2. Qual é o código de integridade HASH SHA-256 referente ao arquivo PDF que contém o documento ?

O código de integridade HASH SHA-256 é :

0d6adc9d0863c9dfe8ca16accbb31312ef8d657205edb739a156c38df62cb973

3. É possível apresentar os metadados contidos no arquivo PDF do documento ?

SIM. Os metadados extraídos indicam que o documento foi criado com **Microsoft Word para Microsoft 365** pelo Autor **Joao Benedito dos Santos Junior**.

4. É possível apresentar os carimbos do tempo contidos no arquivo PDF do documento ?

SIM. O Carimbo do Tempo (Timestamp) extraído pela ferramenta XolidoSign é:

04/11/2024 19:34:35-0300

5. Há sinais de edição do arquivo do documento, após a inserção da assinatura digital ?

SIM. A validação pelo ITI **reprovou** a assinatura e indicou que o **"Documento [foi] modificado após a assinatura"**.

6. A assinatura contida no documento é válida ?

NÃO. Devido à violação da integridade (modificação pós-assinatura), a assinatura é considerada **inválida** perante a ICP-Brasil.

7. Qual o método utilizado para assinar eletronicamente o documento ?

O método utilizado foi a **Assinatura Digital** (Baseada em Certificado Digital no padrão ICP-Brasil).

CONCLUSÃO

Em cumprimento ao que determina o Artigo 473 do Código de Processo Civil e com base nos exames técnicos e análises periciais detalhadas nos capítulos anteriores, o Perito conclui:

1. Identificação do Signatário e Tempo: A assinatura digital no documento **documento.pdf** foi aposta pelo titular **JOAO BENEDITO DOS SANTOS JUNIOR** no dia **04/11/2024**, às **19:34:35-030**.

2. Quebra de Integridade: O documento foi submetido à validação oficial no portal do Instituto Nacional de Tecnologia da Informação (ITI), o qual **REPROVOU** a assinatura digital.

3. Adulteração Comprovada: A razão formal da reprovação é a comprovação de que o **"Documento foi modificado após a assinatura"** .

Portanto, a perícia técnica atesta que, embora a assinatura digital tenha sido realizada por um certificado válido, a posterior adulteração ou modificação do conteúdo do arquivo **invalidou formalmente a assinatura** perante as normas de segurança e integridade da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

O presente Laudo Pericial segue para os Autos, contendo as informações e subsídios técnicos necessários para os devidos fins de direito.

Caconde – SP, 08 de Dezembro de 2025.

João Gustavo Pires Da Costa

Aluno da disciplina de Investigação, Perícia, Inteligência Cibernética e Resposta a Incidentes.

Sobre o Perito (conforme preconiza o inciso II, § 2º do artigo 465 do CPC)

João Gustavo Pires Da Costa, Computer Science 4º Período

Aluno do curso de Ciência da Computação da Pontifícia Universidade Católica de Minas Gerais – PUC Minas.

O executor técnico deste relatório é membro ativo da disciplina de **Investigação, Perícia, Inteligência Cibernética e Resposta a Incidentes**, sendo este Laudo uma atividade prática desenvolvida para demonstrar as competências adquiridas na aplicação de técnicas rigorosas de análise de segurança e forense digital.

A metodologia de análise foi aplicada em ambiente técnico, seguindo o rigor científico e o padrão de preservação de evidência da Norma **ABNT-ISO/IEC 27037:2013**.