Aurellius

Análise Técnica Auxiliar de Documento Eletrônico

Número do contrato: 432524352435	**Objeto do contrato:** EMPRÉSTIMO	**Nome do emitente/contratante:** JOÃO AVELINO
Nome do credor: BANCO LOREN IPSUM	**Origem do contrato** (Download do processo judicial nº): 02398403-294	**Usuário que requisitou o laudo:** MARCOS OLIVEIRA

Sobre esse laudo técnico

Este laudo técnico apresenta uma análise detalhada da autenticidade de documentos eletrônicos, utilizando uma ferramenta de Inteligência Artificial (A.I.) **DAVE - Digital Agreement Verification Engine**, alimentada com critérios periciais avançados para verificar a integridade, a validade jurídica e a confiabilidade dos elementos que compõem o contrato analisado. Estruturado de forma a facilitar a compreensão e a rastreabilidade dos dados, o relatório está dividido em seções que contemplam:

- **Introdução:** Apresentação do objetivo e da metodologia empregada.
- **Fundamentação Científica:** Base teórica que sustenta as análises realizadas, com ênfase nos padrões legais e técnicos aplicáveis.
- **Análises Detalhadas:** Avaliação de elementos específicos, como consistência do hash, validade da assinatura digital, cronologia das datas, geolocalização, IP, e verificação técnica dos padrões de imagens/selfies utilizados para biometria facial.
- **Conclusão:** Síntese dos resultados obtidos e observações relevantes sobre a autenticidade do documento analisado.
- **Recomendações:** Orientações finais para o uso e a validação do relatório em contextos legais ou contratuais. Cada análise foi conduzida com o objetivo de identificar eventuais inconsistências, fornecendo uma visão clara e objetiva do estudo da autenticidade do documento avaliado.

Fundamentação científica

A análise de autenticidade documental está fundamentada em princípios científicos reconhecidos nas áreas de criptografia, biometria, análise de metadados e certificação digital, ABNT NBR ISO/IEC 27037:2013. Essas metodologias são essenciais para garantir a validade, a integridade e a confiabilidade de documentos eletrônicos em contextos jurídicos e administrativos.

Entre os elementos avaliados, destacam-se:

- **Hash Criptográfico:** Fundamental para assegurar a integridade dos dados e detectar alterações. Conforme Schneier (2015), funções hash criptográficas, como SHA-256, são ferramentas indispensáveis para preservar a segurança e rastreabilidade de informações digitais.
- **Certificação Digital:** Sustenta a autenticidade e a validade jurídica de documentos. Segundo Menezes, van Oorschot e Vanstone (2001), a certificação digital, baseada em infraestruturas de chave pública (ICP), desempenha papel central na autenticação de transações e na garantia de não-repudiação.
- **Metadados:** Proporcionam informações cruciais sobre a origem, o histórico e as possíveis manipulações de um documento. De acordo com Garfinkel (2013), a análise de metadados é essencial para auditorias digitais e investigações forenses, permitindo rastrear ações associadas aos documentos.
- **Geolocalização e Endereço IP:** Garantem a coerência das localizações relacionadas às transações digitais. Bellovin (2011) argumenta que a análise de IP e geolocalização é uma ferramenta poderosa para assegurar a autenticidade em sistemas conectados.
- **Verificação Biométrica:** Combate fraudes por meio da confirmação da identidade dos signatários. Jain, Ross e Nandakumar (2011) destacam a biometria como um dos métodos mais confiáveis para a identificação de indivíduos em sistemas digitais, devido à sua precisão e singularidade.

A relevância desse diagnóstico de autenticidade vai além do cumprimento de requisitos técnicos e legais, impactando diretamente na segurança das transações digitais. Ele reduz os riscos de fraudes, protege os direitos das partes envolvidas e atende a padrões normativos globais, como o **Regulamento Geral de Proteção de Dados (GDPR)** na União Europeia e a **Lei Geral de Proteção de Dados (LGPD)** no Brasil.

A base científica dessas metodologias reforça sua credibilidade e eficácia, proporcionando ferramentas robustas para a análise e validação de contratos e documentos digitais, indispensáveis em um cenário onde a digitalização de processos cresce exponencialmente.

Análise 1: Consistência do HASH

Resultado: A hash apresentada é INCOMPATÍVEL com a hash calculada

Dado de referência
HASH Calculado
8833ac8fd3a2cde232f14cc4b003d8f9a1c815e94b6269ba39af69c7014ede39
Origem: Metadados

Hash incompatível
HASH Declarado
af4946548aace05f7c3fbe8ea347120514dced56122d43cf9857338e73359ed
Origem: Corpo do contrato

Detalhes da análise

O Hash se refere a uma função criptográfica que transforma um conjunto de dados em uma sequência alfanumérica única, denominada "resumo criptográfico". Este mecanismo é utilizado para verificar a autenticidade e integridade dos dados.

A relevância do hash se manifesta na sua capacidade de assegurar a integridade dos dados, constituindo um meio eficaz para detectar quaisquer alterações nos dados originais. Sua utilização é de suma importância em contextos legais, visando garantir a autenticidade e integridade de documentos digitais, bem como fortalecer a validade probatória desses documentos em processos jurídicos.

HASH CALCULADO:
MD5: 2afa465f5f46fdf18d9b263a55c9f3b1
SHA-1: 8b0c3759bbbb72d1bc3cc0860011beedc4a72fb7
SHA-256: 8833ac8fd3a2cde232f14cc4b003d8f9a1c815e94b6269ba39af69c7014ede39
SHA-512: c611ebf52a23352558ccd96ca3a01c287c76897b910caf66874aedacdc01bc442d8a49bfdc18ecfff7316ce561943c99d5e2856b5c22da466770253ad9032368

Resultado da análise: A hash apresentada é INCOMPATÍVEL com a hash calculada

No presente caso, observa-se que o documento contém um hash. Contudo, em confronto com o hash gravado na estrutura digital do documento, verifica-se inconsistências, o que demonstra que houve modificação dos dados após a formalização da operação, comprometendo a autenticidade e a integridade das informações.

Análise 2: Assinatura Digital e Certificação Eletrônica

Resultado: A assinatura digital está AUSENTE na documentação

Dado ausente
Data da assinatura
Dado ausente
Origem: Assinatura digital

Assinatura ausente
Assinatura Digital
Assinatura ausente
Origem: Assinatura digital

Detalhes da análise

Utilizou-se o autenticador padrão VALIDAR que é um serviço de validação de assinaturas eletrônicas provido pelo Instituto Nacional de Tecnologia da Informação - ITI, conforme MP 2.200-2/01 e Lei nº 14.063/20. Fonte para validação: https://validar.iti.gov.br/

Este serviço visa validar assinaturas eletrônicas qualificadas quanto à integridade e autoria, em documentos assinados digitalmente por certificado emitido no âmbito da ICP-Brasil e por outras infra estruturas reconhecidas de formas oficial no Brasil, como a assinatura avançada produzida no âmbito do portal Gov.br. Este serviço também inclui a validação de infra estruturas de chaves públicas nacionais de outros países.

Resultado da análise: A assinatura digital está AUSENTE na documentação

O sistema reportou a **AUSÊNCIA** de assinatura eletrônica conforme os padrões estabelecidos pelo ICP-BRASIL, comprometendo, assim, a validade jurídica do referido instrumento contratual.

Análise 3: Cronologia de datas

Resultado: As datas analisadas são INCOMPATÍVEIS

Dado de referência
Assinatura do contrato
17/05/2025
Origem: Corpo do contrato

Data incompatível
Data de criação do arquivo
19/05/2025
Origem: Metadados

Data incompatível
Última alteração do arquivo
19/05/2025
Origem: Metadados

Detalhes da análise

A consistência das datas em um contrato eletrônico é essencial para garantir sua autenticidade e validade jurídica. Incoerências entre as datas registradas nos metadados do arquivo e as datas de assinatura presentes no texto do contrato e no certificado eletrônico comprometem a integridade do documento. Tais discrepâncias indicam alterações não autorizadas e manipulação de conteúdo, o que se consubstancia em evidência de fraude.

Quando as datas mencionadas não são as mesmas, isso sugere irregularidades no processo de elaboração ou operação fraudulenta do contrato, comprometendo sua confiabilidade e podendo afetar sua eficácia legal. A congruência das datas assegura que o contrato reflete fielmente o acordo estabelecido entre as partes no momento apropriado, sem adulterações posteriores. Portanto, é crucial que todas as datas estejam alinhadas para preservar a integridade do contrato e garantir sua plena eficácia jurídica.

Resultado da análise: As datas analisadas são INCOMPATÍVEIS

Analisando os metadados do documento e seu conteúdo, verificou-se que as datas de assinatura do contrato, assinatura digital, última alteração não coincidem e a data de criação do arquivo não têm consistência entre si. Essa discrepância indica que o contrato pode ter sofrido modificações posteriores ou que as datas de assinatura e criação não refletem o mesmo período. Em contratos, essa divergência é inadmissível, pois compromete a integridade do processo de formalização e a autenticidade do documento. A existência de múltiplas datas em momentos distintos sem justificativa plausível revela falta de conformidade com práticas documentais de governança e segurança. A incongruência entre as datas sugere uma possível manipulação do conteúdo contratual, o que caracteriza uma irregularidade grave e coloca em dúvida a validade do contrato.

Análise 4: Geolocalização

Resultado: Os locais analisados são INCOMPATÍVEIS

Dado de referência
Endereço no contrato
B. Jardim, 123 - Vila Leonina, Belo Horizonte - MG, 30440, Brazil
Origem: Corpo do contrato

Coordenadas incompatíveis
Coordenadas geográficas
Local: -19.9167, -43.9345
Endereço: Av. dos Andradas, 134 - Centro, Belo Horizonte - MG, 30110-002, Brasil
Origem: Corpo do contrato

Detalhes da análise

A geolocalização nos contratos e documentos eletrônicos tem como objetivo identificar a localização geográfica de um dispositivo ou usuário em tempo real ou em um momento específico.

Quando uma geolocalização inconsistente é detectada em um contrato eletrônico, isso levanta indícios sobre a validade ou autenticidade do contrato, sobre a identidade e intenção da parte envolvida.

A ausência de tal informação pode dificultar ou mesmo impossibilitar a confirmação de que a pessoa que realizou a ação é realmente quem diz ser, tornando o contrato mais vulnerável a fraudes.

Resultado da análise: Os locais analisados são INCOMPATÍVEIS

Ao proceder com a análise técnica do contrato fornecido, observa-se uma discrepância significativa entre o endereço indicado como pertencente ao cliente e as coordenadas geográficas inseridas no documento pela instituição financeira. A comparação detalhada revela que as coordenadas geográficas apontam para uma localização divergente do endereço residencial do cliente conforme consta nos registros oficiais e nas informações presentes no contrato.

Análise 5: Imagem Facial

Resultado: A análise é INCONCLUSIVA

Imagem inadequada
Resolução da imagem
Baixa
Origem: Corpo do contrato

Imagem adequada
Ausência de obstrução da face
Sim
Origem: Corpo do contrato

Imagem adequada
Olhos abertos
Sim
Origem: Corpo do contrato

Imagem adequada
Ausência de óculos escuros
Sim
Origem: Corpo do contrato

Detalhes da análise

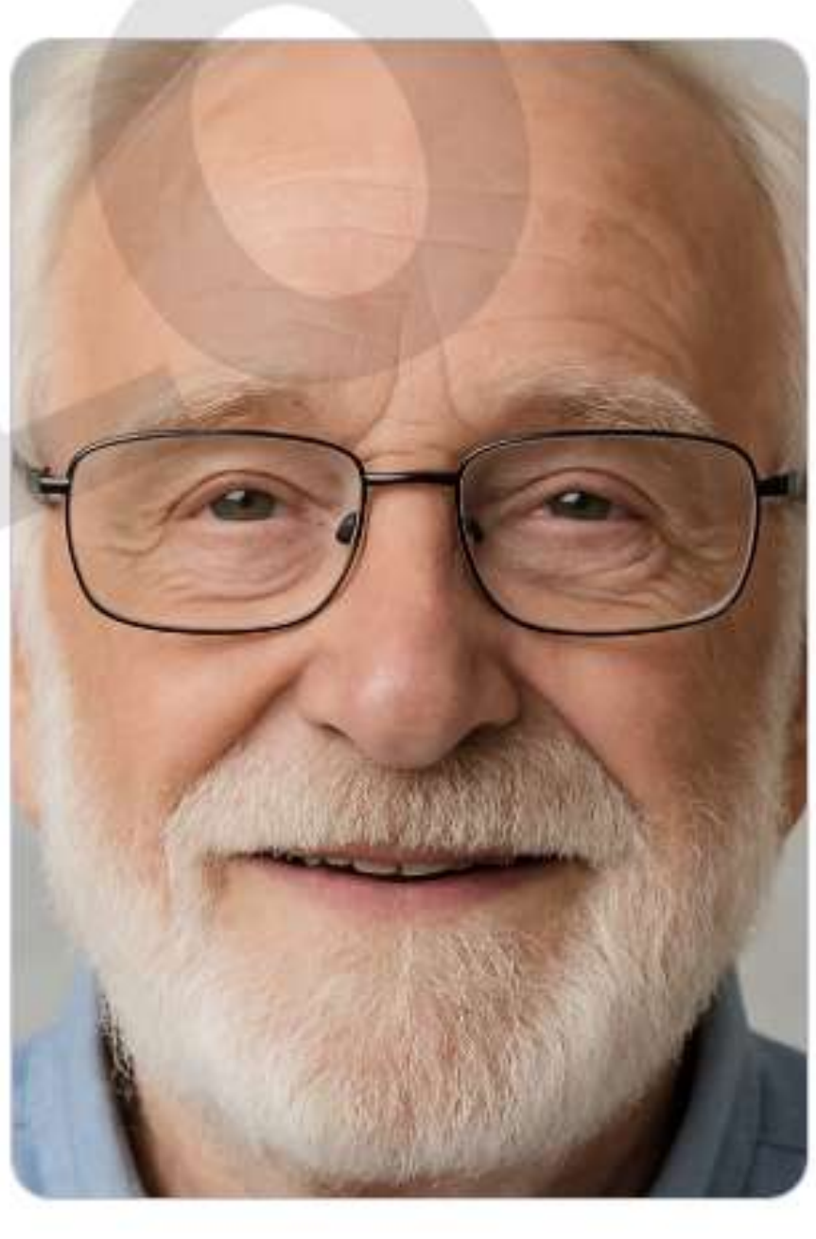
Uma selfie/imagem facial em um contrato/documento eletrônico é uma das várias medidas de verificação de identidade, ajudando a confirmar que determinada pessoa está assinando ou aceitando os termos do contrato é, de fato, quem ela diz ser.

Indispensável destacar que **a presente análise não verifica se a imagem da fotografia é do titular do documento**, mas sim se a mesma preenche os requisitos técnicos mínimos para ser utilizada para a identificação biométrica.

Requisitos de biometria

Resultado da análise: A análise é INCONCLUSIVA

Devido à impossibilidade de aferição da rastreabilidade da imagem facial (foto/selfie), bem como da integridade e autenticidade de seus metadados essenciais – incluindo informações de criação, modificação, data, horário e geolocalização da captura –, em razão do método adotado pela instituição para a incorporação da referida imagem ao contrato, restam comprometidos os pressupostos técnicos necessários à sua validação pericial.



Análise 6: Endereço IP

Resultado: Endereço IP inconclusivo

Dado de referência
Endereço no contrato
B. Jardim, 123 - Vila Leonina, Belo Horizonte - MG, 30440, Brazil
Origem: Corpo do contrato

Inconclusivo
Endereço IP
IP: 192.168.0.101
Origem: Corpo do contrato

Detalhes da análise

A rastreabilidade de endereços IP em contratos eletrônicos é essencial para garantir segurança, validade jurídica e prevenção de fraudes. O endereço IP é um identificador único que permite rastrear o dispositivo utilizado e a localização aproximada do usuário no momento da formalização do contrato. Quando combinado com dados como carimbos de data e hora, ele fornece informações cruciais para a verificação de autoria e autenticidade das partes envolvidas.

A capacidade de identificar o dispositivo e o local de origem de uma assinatura eletrônica fortalece a integridade do contrato, servindo como um elemento-chave em processos de auditoria e em casos de litígio. Esses dados são amplamente utilizados em perícias técnicas para esclarecer eventos, como acessos não autorizados ou alterações indevidas, sendo fundamentais para resolver disputas de forma justa e precisa.

Ademais, o registro de IP deve ser gerenciado com atenção às exigências de legislações como a LGPD, garantindo o tratamento adequado de dados pessoais e respeitando o equilíbrio entre segurança e privacidade. Empresas e indivíduos devem adotar boas práticas na coleta, armazenamento e uso dessas informações para proteger os direitos das partes e assegurar a validade e integridade dos contratos eletrônicos.

Resultado da análise: Endereço IP inconclusivo

Na análise do contrato em questão, não foi possível verificar a consistência entre a cidade do endereço referenciado no documento e a cidade referente ao IP do aparelho utilizado no momento da assinatura do contrato. Tal impossibilidade depõe contra a autenticidade e a integridade do contrato, deixando em dúvida se o documento foi lido e assinado no local declarado e que o processo de assinatura se deu conforme o acordado entre as partes. A desuniformidade entre estas localizações registradas confere menor segurança e transparência ao acordo, aumentando possíveis questionamentos sobre sua validade jurídica em relação à localidade e diminuindo a confiabilidade das informações nele contidas sob esse aspecto.

Conclusão

Resultado: Houve discrepâncias nas análises

Detalhes da análise

Após a análise detalhada das informações associadas ao documento eletrônico fornecido, incluindo o hash do documento, metadados, certificado ou assinatura digital, geolocalização, endereço IP, imagem facial e datas presentes no documento, conclui-se que o documento em questão **não apresenta características suficientes para ser considerado autêntico.**

Resultado da análise: Houve discrepâncias nas análises

Pontos Identificados:
1. **Inconsistências no Hash:** O hash mencionado no documento não corresponde ao calculado, diferentemente do que se espera de um arquivo íntegro e não alterado. Isso sugere que o documento pode ter sido modificado após sua criação original, comprometendo sua autenticidade.
2. **Assinatura Digital:** O documento não apresenta uma assinatura digital. Dessa forma, fica impossível conferir a autenticidade necessária ao documento e a correspondência com a identidade alegada.
3. **Cronologia de datas:** A cronologia das datas presentes no documento não é coerente, sugerindo possíveis adulterações. Discrepâncias entre datas de criação, modificação e assinatura indicam que o documento pode ter sido manipulado ou reeditado de forma não autorizada. A divergência dessas de qualquer uma dessas datas impossibilita assegurar a autenticidade do documento.
4. **Geolocalização:** A geolocalização do endereço associado à transação levanta suspeita, uma vez que não indica com precisão o local origem da transação eletrônica. Adicionalmente, o uso potencial de redes de anonimato ou ferramentas de mascaramento como VPNs sugere uma tentativa de ocultar a localização real, o que compromete ainda mais a credibilidade do documento.
5. **Falha na Verificação Biométrica:** Não foi possível atestar através de uma análise de fotografia "imagem facial" o atendimento aos critérios de correspondência biométrica exigidos. Isso torna essa análise inconclusiva sobre a identidade da pessoa que supostamente assinou ou aprovou o documento.
6. **IP:** A análise comparativa entre a geolocalização do endereço associado a transação em relação ao provável IP do aparelho através do qual o contrato foi firmado não foi possível ser concluída com acurácia. Isso acontece porque os IPs correspondem a áreas que podem variar de extensão e inclusive indicar cidades e regiões diferentes ao endereço informado em contrato. Esse cenário não é necessariamente indicativo de fraude.

Observação importante:

Com base nas inconsistências e suspeitas identificadas, o documento analisado **não pode ser considerado autêntico.** Os resultados obtidos indicam a presença de múltiplos fatores que comprometem a integridade e a veracidade do documento, sugerindo que ele pode ter sido alterado, forjado ou criado de maneira fraudulenta.

Recomendação:
É altamente recomendável que um perito oficial conduza uma revisão completa e independente deste documento para confirmar as conclusões apresentadas. Este laudo, elaborado por um sistema de inteligência artificial, deve ser utilizado como um suporte técnico preliminar e não substitui a avaliação de um profissional especializado.

Ressalvas

Este laudo foi elaborado com base na análise automatizada de informações críticas associadas ao documento eletrônico fornecido, incluindo o hash do documento, metadados, certificado ou assinatura digital, geolocalização, endereço IP, imagem facial e datas presentes no documento. As análises foram conduzidas de acordo com os parâmetros técnicos disponíveis e utilizando algoritmos avançados de inteligência artificial (IA) para identificar possíveis inconsistências, fraudes ou anomalias.

1. **Natureza Automatizada da Análise:** Este laudo foi gerado por um sistema de IA, especializado em verificar a autenticidade de documentos eletrônicos. Embora a IA empregue métodos sofisticados e criteriosos, a análise automatizada não substitui a avaliação humana de um perito oficial. As conclusões aqui apresentadas devem ser interpretadas como um apoio auxiliar e complementar à análise pericial formal.
2. **Limitações Técnicas e Contextuais:** A IA baseia suas conclusões em dados disponíveis no momento da análise. Informações contextuais ou particularidades do caso específico, que podem ser fundamentais para uma análise detalhada, podem não ser capturadas ou interpretadas corretamente por um sistema automatizado.
3. **Autenticidade de Assinatura Digital e Certificados:** A verificação do certificado ou assinatura digital foi realizada conforme os padrões disponíveis, mas a validade jurídica definitiva desses elementos deve ser confirmada por um perito certificado, especialmente em casos de disputas legais ou contratuais.
4. **Geolocalização e Endereço IP:** A análise da geolocalização e do endereço IP foi conduzida com base nas informações técnicas associadas ao documento. Contudo, fatores como o uso de redes VPN, proxies ou outros métodos de mascaramento podem influenciar os resultados e devem ser considerados na análise final.
5. **Imagem e Reconhecimento Facial:** A verificação da selfie/foto para identificação biométrica foi realizada utilizando tecnologias de reconhecimento facial. No entanto, a precisão deste método pode variar conforme a qualidade da imagem e as condições de captura, sendo recomendável uma validação adicional por profissionais especializados.
6. **Datas e Cronologia:** As datas verificadas foram analisadas para identificar possíveis incongruências cronológicas. No entanto, qualquer conclusão definitiva sobre a autenticidade temporal do documento deve considerar também outros elementos contextuais que possam influenciar a linha do tempo apresentada.
7. **Formato do documento:** O usuário é responsável pela indicação precisa da origem do documento. Caso a origem do documento não tenha sido informada de maneira correta, poderá acarretar em imprecisões e distorções na análise do laudo.
8. Alguns Tribunais de Justiça operam por meio de plataformas de processos eletrônicos que, eventualmente, podem modificar os metadados e o código HASH dos documentos digitais. Para assegurar a precisão da análise pericial, é imprescindível que os arquivos sejam enviados em sua forma original, exatamente como foram anexados pela parte interessada, sem qualquer tipo de intervenção, autenticação ou processamento pelo sistema do Tribunal, ou ainda, preferencialmente, recebidos diretamente da instituição de origem por meio eletrônico oficial, como e-mail institucional. Na hipótese de não ser possível o envio do documento original, a integridade da análise dos metadados e do HASH poderá ser comprometida, o que pode afetar a confiabilidade dos resultados periciais.

O Aurellius utiliza inteligência artificial (IA) para a geração de laudos baseados nos documentos fornecidos. Apesar dos esforços contínuos para garantir a precisão e a qualidade das informações processadas, a plataforma não garante que os relatórios gerados estarão isentos de erros, omissões ou imprecisões.

É altamente recomendável que as conclusões deste laudo sejam revisadas e/ou complementadas por um perito oficial, especialmente em contextos onde a autenticidade do documento tem implicações legais ou contratuais significativas. Este laudo deve ser utilizado como uma ferramenta auxiliar, mas ainda não deve ser considerado como substituto para uma análise humana especializada.

O Aurellius também disponibiliza o suporte técnico para o usuário esclarecer dúvidas ou inconsistências.

Laudo gerado em 21/05/2025
aurellius.com.br