Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i8.20684

CONTRIBUIÇÕES DA ABNT NBR ISO/IEC 27037:2013 PARA EVIDÊNCIAS DIGITAIS EM AUDITORIAS GOVERNAMENTAIS FEDERAIS

José Antonio de Carvalho Freitas[1]

RESUMO: O presente estudo investigou como robustecer a confiabilidade das evidências utilizadas no contexto de auditorias governamentais por meio da norma ABNT NBR ISO/IEC 27037:2013. Em um contexto de digitalização ubíqua na sociedade moderna, o uso de Evidências digitais apresenta riscos tanto para Auditorias Governamentais como para a Computação Forense. Assim, procedeu-se à articulação desses campos com a comparação dos atributos do conceito comum de Evidência por meio de análise documental dos seus contextos normativos. Os resultados obtidos apontam para convergência na preocupação com Suficiência, Confiabilidade, Relevância, Repetibilidade e Justificabilidade de informações de potenciais evidência digitais. Na comparação de diretrizes e técnicas, tem-se que a Confiabilidade como descrita na ABNT NBR ISO/IEC 27037:2013 tem potencial de apresentar contribuições relevantes para a normatização da Auditoria Governamental, representada pelas Instruções Normativas da CGU. A ideia de *forensics readiness* também se mostra útil nesse debate como forma preventiva e de preparação de ambientes que podem ser geradores de evidências em eventuais casos. Desse modo, são apresentadas seis diretrizes como sugestões para robustecimento das Evidências Digitais para Auditorias Governamentais. Por fim, pesquisas futuras podem explorar ainda mais essas interfaces, abordando por meio da casuística publicada, como é possível tratar o risco das evidências digitais e ao mesmo tempo seu completo aproveitamento em eventuais investigações.

Palavras-chave: Auditoria Governamental. Computação Forense. Evidência Digital. Forensics Readiness.

ABSTRACT: This study investigated how to strengthen the reliability of evidence used in the context of government audits through the ABNT NBR ISO/IEC 27037:2013 standard. In a context of ubiquitous digitization in modern society, the use of digital evidence poses risks for both Government Audits and Digital Forensics. Thus, these fields were articulated by comparing the attributes of the common concept of evidence through a documentary analysis of their normative contexts. The results indicate convergence in the concern for sufficiency, reliability, relevance, repeatability, and justifiability of potential digital evidence information. In the comparison of guidelines and techniques, reliability as described in ABNT NBR ISO/IEC 27037:2013 has the potential to make relevant contributions to the standardization of Government Auditing, as represented by the CGU's Normative Instructions. The concept of forensic readiness also proves useful in this debate as a preventive and preparatory approach for environments that may generate evidence in potential cases. Accordingly, six guidelines are presented as suggestions for strengthening digital evidence in Government Audits. Finally, future research may further explore these interfaces, addressing, through published case studies, how it is possible to manage the risk of digital evidence while fully leveraging it in potential investigations.

Keywords: Government Auditing. Digital Forensics. Digital Evidence. Forensic Readiness.

[1] Pós-Graduação - Especialista em Computação Forense e Segurança da Informação – IPOG.Mestrado: Gestão do Conhecimento e TI · (2014 - 2016) - Universidade Católica de Brasília. Pós-graduação Lato Sensu - Especialização, Computação Forense · (abril de 2024 - julho de 2025) Universidade de São Paulo. Pós-graduação Lato Sensu - Especialização, Ciência de dados · (janeiro de 2020 - dezembro de 2020) Universidade de Brasília. Especialização, Matemática aplicada à Economia e Administração · (2008 - 2009) Universidade Católica de Brasília. Especialização, Engenharia de Software · (2006 - 2006)Universidade Católica de Brasília.

1. INTRODUÇÃO

A intensificação do processo de digitalização na sociedade contemporânea tem gerado impactos significativos nas estruturas sociais, econômicas e institucionais, reconfigurando a forma como os indivíduos interagem entre si e com o Estado. No contexto da administração pública brasileira, essa transformação tem se materializado na ampliação dos serviços públicos digitais, o que implica uma crescente presença de elementos digitais nas interações entre a sociedade e o poder público. Segundo o próprio Governo Federal[2], cerca de 90% dos 4,7 mil serviços já são oferecidos em formato digital. Assim, conforme observa Castells (1996), tem-se uma sociedade em rede, caracterizada pela centralidade da informação digital na organização das atividades humanas, exigindo novos referenciais para a análise e entendimento dessas dinâmicas.

Nesse cenário, o presente estudo propõe uma articulação entre os campos da Auditoria Governamental e da Computação Forense, tendo como eixo comum o conceito de evidência, que, na sua forma digital, por sua natureza volátil e suscetível a manipulações, a exemplo dos recentes avanços em Inteligência Artificial, tem apresentado desafios específicos à sua coleta, preservação e análise, o que demanda abordagens metodológicas e técnicas que assegurem sua confiabilidade em todos os seus contextos de uso.

De modo geral, apesar de não ser o objeto do presente estudo aprofundar as diferenças semânticas desses dois campos de atuação profissional, se faz necessário preliminarmente registrar os significados básicos dos termos "auditoria" e "perícia". Segundo o Dicionário online Michaelis tem-se o seguinte:

a) "Auditoria: exame analítico, minucioso, relativo às operações contábeis e financeiras de uma empresa ou instituição; Procedimento de análise, investigação e validação de um sistema, atividade ou informação" (AUDITORIA, 2015).
b) "Perícia: exame de caráter técnico, por pessoa especializada, nomeada pelo juiz, de um fato, estado ou valor de um objeto litigioso, cujos resultados servirão de meio de prova que o juiz precisará conhecer para tomar decisão" (PERÍCIA, 2015).

Nota-se com essas descrições básicas que há elementos comuns, acentuando o compartilhamento do sentido de tecnicidade na atuação, como observa-se do uso das expressões iniciais "exame analítico" e "exame de caráter técnico". Por outro lado, há elementos que

[2] Como pode ser observado em leitura à Estratégia de Governo Digital, disponível em https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital. Acesso em 12/07/2025.

indicam diferenças contextuais, com o destaque para o enfoque no contexto judicial (específico) do termo "perícia", além do enfoque mais em processos de gestão organizacional (geral), derivável do termo "auditoria".

1.1 Auditoria Interna Governamental

A atividade de Auditoria Interna Governamental sincroniza suas práticas e normas com as normas internacionais de Auditoria Interna publicadas pela instituição privada IIA (*The Institute of Internal Auditors*), que, por meio dos seus padrões internacionais (The International Professional Practices Framework - IPPF), especifica diretrizes e normas para a prática profissional da auditoria interna, sendo composto de um framework para a sua realização. Como exemplo dessa atividade normativa, tem-se o *Global Practice Guide* sobre o risco de fraude, que prevê como papel da auditoria interna (IIA, 2024):

a) Avaliar se a organização tem uma estrutura eficaz de governança e gestão do risco de fraude;
b) Contribuir com análises, investigações e formação ética, mantendo a independência e a objetividade.
c) Utilizar técnicas como *data analytics*, auditorias contínuas e avaliações proativas para detectar fraudes.

No contexto da União, a função de auditoria pública nasce com a Constituição Federal de 1988 ao estabelecer, em seu artigo 70, que a fiscalização contábil, financeira, orçamentária, operacional e patrimonial da administração pública será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder. Essa disposição dá origem à função de auditoria como instrumento essencial para assegurar a legalidade, legitimidade, economicidade e eficácia na aplicação dos recursos públicos (BRASIL, 1988).

Segundo a Lei nº 10.180, de 6 de fevereiro de 2001, que organiza e disciplina o sistema de planejamento e de orçamento federal, incluindo o sistema de controle interno do Poder Executivo, a Secretaria Federal de Controle Interno, que compõe a Controladoria-Geral da União (CGU), é o órgão central do sistema de controle interno do Poder Executivo Federal, sendo responsável pelas atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização (BRASIL, 2001).

No contexto da CGU, a normatização da atividade de auditoria pode ser encontrada na Instrução Normativa CGU nº 03, de 09 de junho de 2017, que trouxe o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal; e na Instrução Normativa CGU nº 08, de 06 de dezembro de 2017, que aprovou o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (MOT). Essas normas nasceram com o intuito de atualizar o corpo de conhecimento dessa atividade com as normas internacionais (IPPF – IIA, citadas anteriormente) (BRASIL, 2017). O MOT define a atividade de auditoria governamental como uma atividade independente e objetiva, que prima pela aplicação de uma abordagem sistemática e disciplinada para cumprir seus objetivos. Para cumprir essa atribuição, conta com 03 (três) tipos de atividade: avaliações, apurações e consultorias. Sobre avaliações, o manual diz que seu objetivo é a obtenção e a análise de evidências com o intento de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Já as apurações, consistem na execução de procedimentos cuja finalidade é averiguar atos e fatos inquinados de ilegalidade ou de irregularidade praticados por agentes públicos ou privados, na utilização de recursos públicos federais, entrando no escopo de fraudes (BRASIL, 2017:12).

1.2 Evidências de Auditoria

Avaliações e apurações, conforme se depreende da Instrução Normativa CGU nº 08 (MOT), dependem da obtenção de evidências para sustentar suas conclusões. Nesse paradigma, evidências de auditoria são as informações coletadas, analisadas e avaliadas pelo auditor para apoiar os achados e as conclusões do trabalho de auditoria. Esse componente é destacado no MOT em capítulo específico sobre coleta e análise de dados, que destaca os atributos de suficiência, confiabilidade, fidedignidade, relevância e utilidade (BRASIL, 2017:94).

Adicionalmente e com objetivo de detalhamento das orientações contidas no MOT, a CGU, no âmbito da Secretaria Federal de Controle Interno (SFC), publicou a Orientação Prática para Serviços de Auditoria. Nessa norma, destacam-se com mais detalhes no Apêndice III os mesmos atributos essenciais das evidências de auditoria, a saber: suficiência, confiabilidade, fidedignidade, relevância e utilidade. A primeira lida com o aspecto quantitativo das evidências da auditoria; as demais abordam medidas de qualidade e adequação dessas evidências (BRASIL, 2022:56).

Em especial, interessa ao presente estudo o enfoque na confiabilidade das informações de apurações, ou seja, as evidências devem ser confiáveis, fidedignas, válidas e apresentarem de

forma precisa os fatos, sem erros ou tendência. Há também o destaque que essa particular categoria de informações constitui meio de prova para fundamentar uma opinião e, ao mesmo tempo, reduzir o risco de auditoria a um nível aceitável (BRASIL, 2017:93).

Especialmente, no contexto de apurações, essas evidências têm o potencial de demonstrar situações de fraude, onde naturalmente, as evidências podem ser utilizadas ou compartilhadas em contextos jurídicos, tanto na esfera administrativa (a exemplo do cumprimento da Lei nº 12.846/2013, que baliza a abertura de processo sancionador de empresas pela própria CGU ou mesmo em apurações disciplinares), bem como nas esferas cível e penal, no contexto de atuações em parcerias com órgãos desse tipo de persecução, a exemplo da Polícia Federal e do Ministério Público Federal (BRASIL, 2017:26).

1.3 Evidência Digital

Em particular, conforme se depreende de Casey (2011:07), evidência digital pode ser definida como um conjunto de dados armazenados ou transmitidos usando um sistema computacional que suportam ou refutam alguma hipótese de como algum ato ilícito ou infração de fato ocorreu. O autor também destaca que a evidência tem um aspecto de conjunto de elementos mais granulares, podendo reunir dados quantitativos, textos, imagens, áudios ou vídeos, esses elementos podem ser referidos também como vestígios. Silva (2025:16) destaca também as novas fontes de evidência, como dados em nuvem, criptomoedas e inteligência artificial.

Em Oliveira (2023) um aspecto destacável sobre evidências digitais são as fragilidades que esse tipo de informação possui, logo é preciso que seja padronizado o seu tratamento para garantir sua integridade e autenticidade. Segundo os autores, esse tipo de evidência pode ser facilmente alterada, ou mesmo inutilizada durante sua manipulação, principalmente nas fases de coleta e análise.

Por esse aspecto de fragilidade, o tratamento de evidências digitais no contexto da computação forense é foco da norma ISO/IEC 2737:2012, tropicalizada na ABNT NBR ISO/IEC 27037:2013, que padroniza o processo de tratamento de evidências digitais, para preservar a integridade, a admissibilidade, força probatória e relevância em processos judiciais ou administrativos.

Uma das principais técnicas de manutenção da admissibilidade da evidência digital é uso da cadeia de custódia, que, para Magno e Comploier (2021:201), é um documento que registra

todas as interações realizadas com a fonte da evidência, mantendo assim a documentação da história cronológica do item utilizado.

Assim, a evidência digital é a matéria-prima da computação forense, pois é dela que se pode extrair convicção e construção de provas para guiar as instâncias decisórias da melhor forma possível.

1.4 Computação Forense

O advento da computação forense, ou perícia digital forense, como subcampo das ciências forenses tradicionais está em linha com o avanço da digitalização nos diversos aspectos da vida moderna. Segundo Casey (2011), trata-se de novo ramo da ciência forense, dedicado à identificação, preservação, análise e apresentação de informações digitais com valor probatório em procedimentos judiciais e administrativos.

Na mesma linha, a Portaria GSI nº 93/2019 acrescenta que:

> trata-se da aplicação da ciência da computação e procedimentos investigativos para a identificação, exame e análise de dados com a devida preservação da integridade da informação e mantendo uma estrita cadeia de custódia para os dados (BRASIL, 2019)

Em Eleutério e Machado (2019), temos que a "computação forense objetiva determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à informática". Esses autores destacam os cuidados que se tem que ter com mídias de armazenamento, dado que são frágeis e possuem limitações de tempo de vida útil, além de ficarem inoperantes em caso de mal uso.

O produto final do trabalho da computação forense é a confecção de um laudo técnico contendo os resultados e listando as evidências digitais encontradas nos materiais examinados.

1.5 Inteligência Artificial (IA) e *Deepfakes*

Para Singh (2025:21) os avanços recentes em IA tem potencial para a geração de evidências digitais falsas, a exemplos de imagens e vídeos ultrarrealistas. O autor enfatiza também a inadequação atual dos sistemas jurídicos para enfrentarem as dificuldades apresentadas pelas mídias sintéticas geradas por IA.

Já Verdoliva (2020:18) aponta como a inteligência artificial mudou significativamente os limites de falsificação de artefatos digitais, cada vez mais é possível produzir material de alta qualidade. Isso vai exigir segundo a autora, um esforço extraordinário por parte de cientistas e formuladores de políticas públicas vai ser necessário para mitigar essas dificuldades.

O cenário que o uso de IA para falsificação ou adulteração de evidências digitais constitui-se em desafios para quem tem que lidar com essas informações, quer seja em texto, imagem e vídeo. Essa situação exige um esforço de pessoas, entidades privadas e públicas na tentativa de se criar um ambiente propício para a geração e coleta de vestígios digitais que possam ter credibilidade. Essa ideia de atuação estruturante e preventiva para assegurar um melhor ambiente para coleta de evidências confiáveis é foco também do campo de estudo conhecido como *forensics readiness*.

1.6 Forensics Readiness

Segundo Tan (2001), *forensics readiness*, ou prontidão (preparação) forense diz respeito maximizar a capacidade de um ambiente de coletar evidências digitais confiáveis, pensando-se em termo de tratamento futuro de incidentes. Também é um objetivo minimizar o custo da perícia forense em uma resposta a essas situações, pois com sistemas preparados, com trilhas de auditoria, logs, possibilidade de acesso somente leitura a dispositivos de armazenamento, o trabalho de perícia torna-se mais facilitado. Almeja-se preparar as organizações para eventuais necessidades de atuar em processos judiciais, nos quais provas digitais sejam requeridas.

Para Rowlingson (2004) e Brügger e Lorens (2025) a expressão é definida como a capacidade de uma organização maximizar seu potencial de uso de evidências digitais, minimizando os custos de uma investigação. Essa preparação para o uso de evidências digitais envolve monitoramento aprimorado de sistemas e de pessoal técnico envolvido, além de meios técnicos, físicos e processuais para proteger os dados de acordo com os padrões probatórios de admissibilidade. A ideia é assegurar que o pessoal envolvido reconheça a importância das evidências para potenciais processos, quer sejam internos ou externos (jurídicos), facilitando inclusive a interação com as autoridades policiais.

Em Rowlingson (2004:09) encontra-se série de 10 passos para implementação de um ambiente preparado para forense digital, listados a seguir:

1. Mapear cenários de negócio com potencial necessidade probatória, considerando riscos operacionais, requisitos legais e possíveis eventos de segurança que demandem evidências digitais;
2. Inventariar fontes de dados e classificar os tipos de evidências digitais possíveis, como logs de sistemas, registros de rede, e-mails, arquivos transacionais e metadados relevantes;
3. Estabelecer os requisitos técnicos e legais para coleta de evidências, incluindo granularidade, frequência, integridade e tempo de retenção compatíveis com as obrigações normativas;

4. Implementar mecanismos de coleta forense segura e legalmente admissível, com suporte a cadeia de custódia digital e preservação da integridade (a exemplo de uso de *hashing* e bloqueio de escrita);
5. Definir e aplicar políticas de armazenamento seguro e controle de acesso às evidências, com proteção criptográfica, segregação de ambientes e logs de auditoria;
6. Configurar monitoramento contínuo e automatizado para detectar, alertar e mitigar incidentes de alto impacto, com base em análise de comportamento e correlação de eventos;
7. Estabelecer critérios objetivos para escalonamento de investigações formais, acionando protocolos forenses e equipes especializadas mediante gatilhos pré-definidos;
8. Capacitar colaboradores e equipes técnicas sobre resposta a incidentes e tratamento de evidências digitais, reforçando os aspectos jurídicos e as responsabilidades no processo;
9. Elaborar documentação estruturada de incidentes baseada em evidências, incluindo linha do tempo, impactos operacionais e técnicos, e artefatos coletados com validade forense;
10. Submeter os casos a revisão jurídica especializada, visando assegurar conformidade legal, embasamento probatório e suporte a eventuais medidas administrativas, cíveis ou penais.

2. OBJETIVOS

Da leitura do referencial teórico abordado, não foram identificados trabalhos que abordassem a temática aqui trazida de diálogo entre o tratamento de evidências da auditoria governamental e o mesmo processo na computação forense, com enfoque na norma ABNT NBR ISO/IEC 27037:2013. Observa-se que ambas as disciplinas compartilham as dificuldades no mesmo cenário cada vez mais digital que as organizações e a própria sociedade estão inseridas.

Entende-se como um problema de pesquisa pertinente nesse contexto a questão de como robustecer a confiabilidade das evidências utilizadas no contexto de auditorias governamentais do tipo apuração, conforme normatizado no MOT, dado o aspecto atual de majoritariamente dependerem do formato digital e das inúmeras dificuldades que esse tipo de informação pode apresentar. Em especial, pretende-se abordar essa questão como discutido por Smith (2005):

> [...] é importante que a profissão de auditoria considere o papel dos especialistas em computação forense para que dados digitais não sejam destruídos para fins forenses (...) Como uma investigação de fraude pode depender de evidências eletrônicas, é importante que essas duas

> profissões — auditoria e computação forense — se auxiliem mutuamente na coleta e no uso de evidências digitais. Sem essa cooperação, os dados digitais testados durante uma auditoria podem ser inutilizados para fins de perícia forense.

Assim, o presente trabalho objetiva mostrar se é possível articular os aspectos de confiabilidade de evidências de auditorias governamentais do MOT com o que é apregoado pela computação forense, aqui representado no processo contido na norma ABNT NBR ISO/IEC 27037:2013, que também discute critérios de confiabilidade para evidências digitais, somado a como práticas de *forensics readiness* podem ser adotadas para facilitar a preparação para eventual tratamento de incidentes.

3. METODOLOGIA

Como metodologia, pretende-se, com uma abordagem qualitativa, usar o método de análise documental para mostrar as semelhanças, diferenças e pontos de discordância entre as duas normas trazidas aqui como fontes primárias (IN SFC 08 - MOT e ABNT NBR ISO/IEC 27037:2013). Proporcionando o cotejamento entre as duas estruturas, almeja-se abordar a problemática trazida com a hipótese de que o processo constante na norma ISO, bem como a ideia de *forensics readiness*, podem robustecer os aspectos de confiabilidade de evidências desejados pelo processo trazido no MOT, marcando uma relação de complementariedade.

4. RESULTADOS E DISCUSSÕES

Com base nos normativos citados anteriormente separando-se em 02 (dois) blocos: a) CGU (IN SFC 08 - MOT e Serviços de Auditoria), abreviado para MOT; e b) ABNT NBR ISO/IEC 27037:2013, abreviado para ISO27037, foi gerada o seguinte Quadro de resultados da comparação direta do conteúdo dos atributos de evidência de ambos os contextos de estudo:

Quadro 1 – Comparação CGU (MOT e Serviços de Auditoria) e ABNT NBR ISO/IEC 27037:2013

Atributo	MOT	ISO27037	Observação
Suficiência	Medida da **quantidade** de evidência necessária para **suportar conclusões**. Está relacionada à materialidade, risco, custo e qualidade (p. 94).	(Princípio) **quantidade** suficiente de evidência para **permitir uma investigação adequada** (p. 07).	Convergência quanto ao aspecto de quantidade e cobertura.
Confiabilidade	Capacidade da evidência de ser **imparcial, precisa e livre de erros**. As melhores possíveis de	(Princípio) a evidência deve **ser o que diz ser**,	Convergência, apesar de escritas diferentes, entende-se que "livre de

	serem obtidas por meio da utilização de técnicas de auditoria apropriadas (p. 94).	com métodos **auditáveis e repetíveis** (p. 07).	erros" e "ser o que diz ser" remetem à mesma ideia de consistência interna e integridade
Fidedignidade	Evidência deve ser **válida** e **representar com precisão os fatos (atributo componente da confiabilidade** (p. 94).	Não há menção direta	
Relevância	Evidência deve estar **diretamente relacionada** aos objetivos e escopo da auditoria (p. 95).	(Princípio) Evidência contém informação de **valor** no auxílio à investigação e de que há uma boa **razão** para ter sido adquirida (p. 07).	Convergência quanto ao aspecto de relacionamento da Evidência com a situação analisada
Utilidade	Deve **agregar valor**, apoiar recomendações e **melhorar as operações** da unidade auditada (p. 95).	Não há menção direta.	
Persuasão	**Capacidade de convencer auditado e partes interessadas sobre a validade da opinião do auditor** (p. 97)**.**	Não há menção direta	
Auditabilidade	Não há menção direta	(Aspecto-chave) Deve haver documentação completa **para permitir avaliação independente** das ações do investigador (p. 07).	
Repetibilidade	Não há menção direta	(Aspecto-chave) com foco no processo, se o mesmo profissional repetir o processo, será obtido o **mesmo resultado nas mesmas condições** (método, tempo e espaço) (p. 07).	
Reprodutibilidade	Há menção indireta, pois o MOT destaca que as mesmas conclusões devem ser obtidas por terceiros com prudência e conhecimento suficiente (p. 94)	(Aspecto-chave) com foco na pessoa, um outro profissional obtém **mesmo resultado em ambientes distintos** (p. 08).	Apesar do MOT não mencionar diretamente, há convergência quanto ao aspecto de resultado constante, quando executado por pessoas diferentes.
Justificabilidade	Há menção indireta, pois o MOT cita que p**ara justificar a tomada de decisões** o auditor pode usar do **julgamento profissional** (p. 94)	(Aspecto-chave Todas as ações do investigador devem ser justificáveis com **base em boas práticas e evidências documentadas** (p. 08).	Apesar do MOT não mencionar diretamente, há convergência quanto ao aspecto de aplicação de boas práticas e do julgamento profissional, que consiste na aplicação do treinamento, conhecimento e experiência relevantes

Fonte: Elaborado pelo autor

Dessa comparação dos atributos, pode-se apresentar os seguintes pontos de análise:

a) São atributos comuns aos dois contextos: Suficiência, Confiabilidade, Relevância e Reprodutibilidade. São exclusivos do MOT: Fidedignidade, Utilidade e Persuasão. Por sua vez, são exclusivos da ISO27037: Auditabilidade e Repetibilidade.

b) Dos 10 (dez) atributos comparados (existentes em algum dos contextos), metade possuem convergência de significados entre as normas, são eles: Suficiência, Confiabilidade, Relevância, Repetibilidade e Justificabilidade. Desses dois últimos ressalva-se que o MOT não trouxe diretamente, o que sugere uma preocupação mais técnica e científica, principalmente na presença da repetibilidade;

c) Agora separando os que existem somente no MOT (Fidedignidade, Utilidade, Persuasão), percebe-se uma preocupação maior do MOT em agregar valor ao negócio, ou à organização, uma preocupação mais abrangente, principalmente nos dois últimos. Já a ausência da Fidedignidade, pode-se assumir que boa tarde de sua carga semântica pode estar no item de confiabilidade, como o próprio MOT cita: "*para que sejam confiáveis, as evidências devem ser também fidedignas, ou seja, válidas e representarem de forma precisa os fatos, sem erros ou tendências*";

d) Separando, por sua vez, os que existem somente na ISO27037 tem-se a Auditabilidade e a Reprodutibilidade. Essas ausências remetem ao caráter mais técnico-científico que a ISO27037 imprime ao processo de perícia, embora seja estranho pensar que o processo de auditoria também não mereça certa dose de tecnicismo para assegurar maior certeza a seus achados, o que se percebe no geral é que esse anseio é mais exteriorizado no contexto de forense do que de auditoria.

e) Cabe aqui discutir também que pelos itens (a) e (b) percebe-se que a orientação dos dois contextos parece partir de escopos diferentes, o do MOT de auditoria é mais abrangente, almeja analisar aspectos de gestão, já o da ISO27037 é mais individualizado e possui um foco definido, do qual busca extrair uma verdade sobre aqueles fatos em específico. Embora ambos utilizem o mesmo mecanismo de Evidências, a chegada nesse tipo de informação advém de caminhos diferentes, essa percepção está aderente aos conceitos básicos trazidos anteriormente para os campos de "auditoria" e "perícia".

Para suportar e assegurar o atingimento desses atributos mostrados, cada referencial apresenta diretrizes e ferramentas, mostrando sugestões de "como" conseguir o objetivo do atributo. O próximo Quadro a seguir apresenta essa relação entre atributos e técnicas mapeadas para sua consecução:

Quadro 2 – Relação de atributos e técnicas sugeridas pelas normas CGU (MOT e Serviços de Auditoria) e ABNT NBR ISO/IEC 27037:2013

Atributo	**Diretrizes/Técnicas, segundo o MOT/CGU**	**Diretrizes/Técnicas , segundo a ISO**
Suficiência	a) Amostragem (estatística ou não) (p. 85-86); b) Ceticismo e julgamento profissional (p. 94);	Não há uma menção direta de técnicas para este atributo, mas sim uma diretriz sobre o fato de que potencial evidência digital suficiente deve ser

	c) Supervisão/Revisão de trabalhos (p. 35).	coletada ao ponto de permitir que elementos da questão sejam adequadamente examinados ou investigados, além da indicação de documentar todas as ações (p. 14)
Confiabilidade	a) Diretrizes gerais, conforme a fonte da informação: a.1) evidência obtida de terceiros independentes tende a ser mais imparcial do que aquela obtida junto à Unidade Auditada; a.2) evidência produzida por um processo ou sistema com controles efetivos é mais confiável do que aquela produzida por um processo ou sistema com controles ineficazes; a.3) evidência obtida diretamente pelo auditor interno tende a ser mais confiável do que evidência obtida indiretamente; a.4) evidência proporcionada por documentos originais é mais confiável do que a evidência proporcionada por fotocópias; a.5) evidência corroborada por informações oriundas de outras fontes tende a ser mais confiável do que aquela que é obtida em uma única fonte. (p. 95) b) Uso de evidência corroborativa para reforçar a evidência principal, buscando em outras fontes que podem confirmar algum aspecto da informação (p-96);	a) Cópia de evidência digital – minimizando o manuseio da fonte ou dispositivo original, priorizando o manuseio por meio de cópias (técnica de imageamento ou cópia bit-a-bit), evitando a espoliação da evidência (alteração por inclusão/exclusão dos dados ou metadados) (p. 2) ; b) Atuação de pessoal com os requisitos de autoridade, treinamento a qualificação com o primeiro contato com a fonte da evidência (p. 2); c) Considerar quaisquer alterações e documentar ações tomadas (p. 9); d) Atentar para configuração de data e hora da fonte da evidência, comparando sempre com uma fonte de tempo externa confiável e documentando eventuais diferenças (p. 15) e) Não utilizar programas do sistema da fonte da evidência, utilizar suas próprias ferramentas binárias estáticas validadas (p. 29) f)Uso de e uma função de verificação para assegurar que as cópias são iguais aos dados originais, geralmente essa função utiliza de técnicas de hashing (p. 4, 9, 29); g) Cadeia de Custódia - documento identificando a cronologia de movimento e do manuseio da potencial evidência digital (p. 11); h) Atentar para as diferenças entre evidência volátil e não volátil, priorizando a volátil dado o fator tempo e a criticidade quanto a sua obtenção (depender de fonte de energia) (p. 18).
Fidedignidade	Não há uma menção direta de técnicas para este atributo, porém o mesmo é referenciado como um componente da confiabilidade, logo herda todas as diretrizes do mesmo (p. 94)	Não há menção direta ao atributo (vide Quadro 1)
Relevância	a) Ceticismo e julgamento profissional para assegurar que a evidência esteja diretamente relacionada aos objetivos e ao escopo do trabalho. (p. 94-95).	a) Documentar todas as ações, descrevendo os procedimentos seguidos e esclarecendo como a decisão para obter cada item foi tomada (p. 7); b) Quando permitido, ligar dispositivos digitais no local para determinar sua relevância para a investigação e examiná-los para verificar a necessidade (p. 20).

Utilidade	Não há uma menção direta de diretrizes ou técnicas.	Não há menção direta ao atributo (vide Quadro 1)
Persuasão	a) Hierarquia de confiabilidade (do mais persuasivo ao menos) (p-97): a.1) exame físico; a.2) observação direta; a.3) informações de terceiros; a.4) informações documentais a.5) testemunhais; b) Uso de fontes múltiplas, externas e confiáveis (p. 97-98)	Não há menção direta ao atributo (vide Quadro 1)
Auditabilidade	Não há menção direta ao atributo (vide Quadro 1)	a) documentação de todas as ações realizadas (p. 7) b) transporte e armazenamento seguro de evidências com segurança física, e de sistemas, com controle de acesso, objetivando preservar a evidência para assegurar a auditabilidade; c) A Norma apresenta como um dos objetivos dos princípios relevância, confiabilidade e suficiência assegurar a auditabilidade do processo como um todo, logo o atingimento desses princípios cria condições para que este também se cumpra (p. 7); d) Um dos principais elementos destacados pela Norma como forma de documentação para auditabilidade é a Cadeia de Custódia (p. 11).
Repetibilidade	Não há menção direta ao atributo (vide Quadro 1)	a) Controle de qualidade do processo e documentação atualizada, com foco na padronização total de procedimentos, métodos de medição, instrumentos e condições (p. 7); b) A Norma apresenta como um dos objetivos dos princípios relevância, confiabilidade e suficiência permitir repetições do processo como um todo, logo o atingimento desses princípios cria condições para que este também se cumpra (p. 7).
Reprodutibilidade	Como o atributo é mencionado indiretamente, com foco na capacidade das evidências de gerarem as mesmas conclusões por terceiros, não há também menção direta a diretrizes e técnicas para tal.	a) Controle de qualidade do processo e documentação atualizada, com foco na padronização total de procedimentos, métodos de medição, instrumentos e condições (p. 7); b) A Norma apresenta como um dos objetivos dos princípios relevância, confiabilidade e suficiência permitir repetições do processo como um todo, logo o atingimento desses princípios cria condições para que este também se cumpra (p. 7).

Justificabilidade	Como o atributo é mencionado indiretamente, com foco no uso do julgamento profissional para tomar a melhor decisão, não há também menção direta a diretrizes e técnicas para tal.	a) Documentar todas as decisões tomadas, com as devidas informações que embasaram aquele caminho de ação (p. 8).

Fonte: Elaborado pelo autor

Dos resultados do Quadro anterior, podem ser apresentadas as seguintes considerações em termos de detalhamento de diretrizes e técnicas para cada atributo:

a) O atributo de Suficiência aparenta ser mais bem trabalhado no MOT, com a menção a técnicas estatísticas, capacidade do próprio auditor (data sua experiência) contribuir com a decisão da quantidade de evidências, além também da menção direta à necessidade de supervisão dos trabalhos. Na ISO27037 entende-se que dado o caráter de especificidade do trabalho de perícia, não se tem de antemão controle prévio sobre o que se vai achar em campo, enquanto na auditoria há ainda a possibilidade de se relacionar com o órgão auditado e solicitar informações. Logo, o espaço de informação potencial no contexto da ISO27037 é mais restrito pela própria natureza do fato em estudo.

b) Agora, quanto a Confiabilidade, percebe-se que a ISO27037 apresenta um cabedal de preocupações maior que o MOT, principalmente no tocante a apresentar formas de assegurar integridade e documentação do manuseio das evidências. Esse conjunto mais expandido de técnicas pode ampliar o espaço também de atuação de auditores seguindo o MOT, principalmente quando se verifica que evidências digitais necessitam de controle de integridade e espoliação, além do uso de certos elementos da cadeia de custódia para assegurar um mínimo de rastreabilidade ao longo do tempo, destaca-se também a possibilidade do uso de hashing na coleta e guarda de arquivos digitais.

c) Quanto aos demais atributos, não se observam grandes contribuições mútuas.

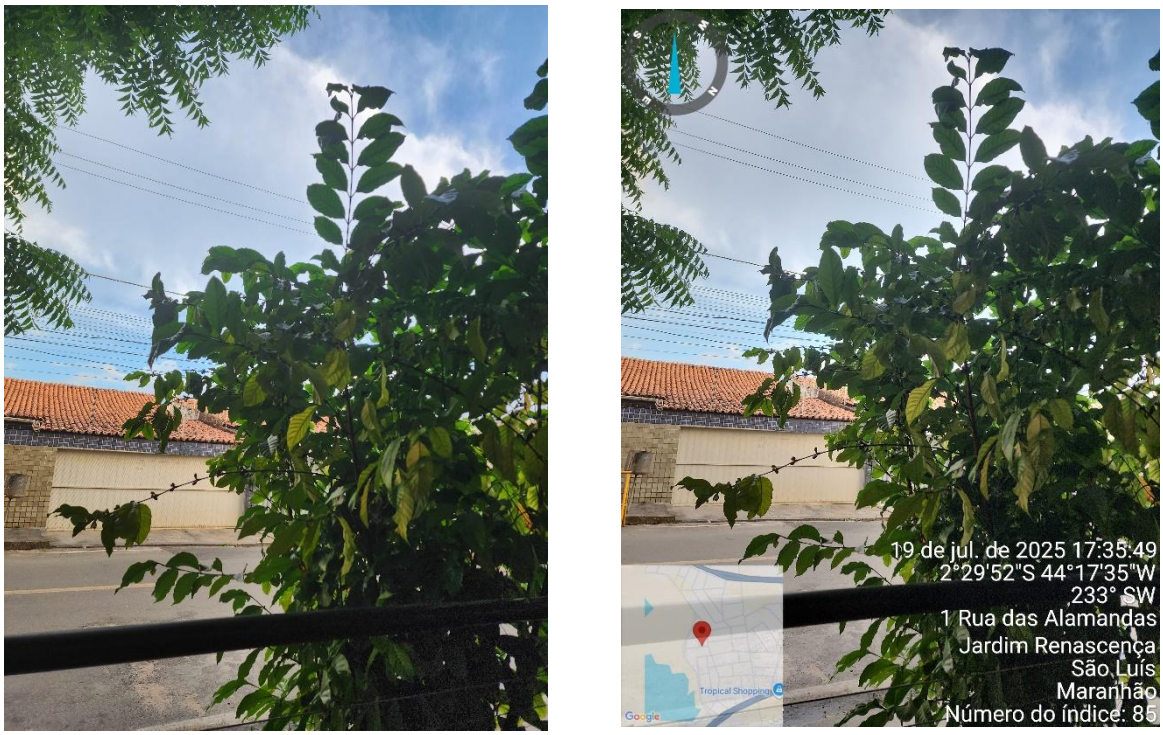
Dado o exposto, compila-se a seguir diretrizes que podem contribuir o aprimoramento da confiabilidade de Evidências Digitais em Auditorias Governamentais Federais do tipo Apuração com o uso de técnicas de Computação Forense, segundo a ABNT NBR ISO/IEC 27037:2013. Como exemplo de contribuição do item Confiabilidade da ISO27037 para o MOT, pode-se tomar o item "5.7.4 ESTRUTURA, ORGANIZAÇÃO E ARMAZENAMENTO DOS PAPÉIS DE TRABALHO", que possuiu as subseções "Estrutura" e "Organização e armazenamento" como espaço para a inclusão das seguintes sugestões:

Diretriz 1 - Sempre que possível, evitar trabalhar em arquivos originais, preservando-os exatamente como foram recebidos e utilizando cópias para o manuseio direto nas análises necessárias;

Diretriz 2 - Realizar cálculo de *hash* dos arquivos digitais utilizados como evidência para suportar os achados, indicando qual algoritmo foi usado se MD5, SHA256, SHA512, etc;

Diretriz 3 - Utilizar elementos de carimbo de data (*timestamp*) para guardar o momento exato de coleta ou de algum outro ponto de interesse do trabalho. Como exemplo prático, existem aplicações de dispositivos móveis que permitem o registro de imagens ou vídeos com os respectivos metadados de origem geográfica e temporal diretamente junto com as imagens, um exemplo é o app TimeStamp Camera[3], as Imagens a seguir ilustram evidências digitais com as duas possibilidades com relação a metadados:

Imagem 1 – Registro de evidências digitais sem e com



Fonte: Elaborado pelo autor com uso do App TimeStamp Camera na plataforma Android

Diretriz 4 - (elementos de Cadeia de Custódia[4], segundo a ISO27037) este elemento de documentação é um dos mais importantes, sendo o registro de todas as interações realizadas com a evidência ou sua fonte desde a coleta até o descarte, trazendo um histórico de quem, como, onde e motivação do manuseio. Sua importância é assegurada pela própria legislação penal quando aborda a questão de provas, conforme pode ser visto

[3] Disponível em https://play.google.com/store/apps/details?id=com.jeyluta.timestampcamerafree&pli=1.
[4] Observar que existe o conceito segundo a Lei nº 13.964, que no seu artigo 158A a define assim: *"Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte."*

na Lei nº 13.964, de 24/12/2019 (art. 158A). A seguir, sugere-se alguns itens que podem compor os Papeis de Trabalhos de Auditoria que induzem a construção desse artefato ou sua facilitação:

c.1) Identificador único da evidência;

c.2) Quem acessou a evidência, o tempo e local em que ocorreu (desde sua coleta e durante o trabalho);

c.3) Quem revisou o trabalho e a evidência armazenada e preservada;

c.4) Alterações na evidência, bem como quem e o motivo de tais alterações.

De forma mais preventiva, na seção 5.6 RECOMENDAÇÕES, dado que auditores de modo geral atuam em processos organizacionais de forma estruturante e realizam recomendações no sentido de melhoria, podendo focar na causa, na condição ou na consequência dos problemas verificados, observa-se que recomendar juntamente medidas de facilitam a computação forense - *forensics readiness – 10 passos segundo* Rowlingson (2004:09) - pode repercutir em melhores evidências digitais em futuras ações, com impacto direto em qualidade e custo. Exemplo dessas medidas podem ser:

Diretriz 5 - Ao recomendar sobre sistemas de negócio, assegurar que eles gerem *logs* de acesso das transações realizadas; que tenham rastreabilidade dessas transações por meio de controles de acesso com usuários pessoais, evitando-se usar usuários genéricos ou impessoais; que assegurem que os sistemas possuem sincronização de data e hora com algum recurso oficial, a exemplo dos servidores de NTP[5];

Diretriz 6 - Na mesma linha, recomendar que haja políticas mínimas de Segurança da Informação, com uso constante de soluções de *backups* e controle de atualização de software e correção de vulnerabilidades.

Entende-se que com essas melhorias, tem-se atributos mínimos presentes em trabalhos de auditoria, que não necessariamente serão utilizados em litígios perante o sistema judiciário, mas que trazem incrementos de confiabilidade ao próprio processo de trabalho. Sabe-se que em casos que houver essa necessidade de uso em processos judiciais haverá o momento de atuação das autoridades policiais e da Perícia Oficial, conforme o caso. Porém o que se pretende com essas medidas é facilitar a atuação dessas, permitindo que, nas vezes que o auditor for o (acidentalmente) o *First Responder* (quem chegar primeiro ao local de algum incidente), as evidências terão asseguradas certa sintonia com o restante do processo, buscando manter força probatória (necessária tanto para a auditoria quanto para a perícia).

[5] Disponível em https://ntp.br/ .

CONCLUSÃO

Dado o exposto, acredita-se que o uso das técnicas e diretrizes propicia condições para robustecer a confiabilidade das evidências utilizadas no contexto de auditorias governamentais, dado que foi possível articular os dois contextos trazidos de auditoria e perícia. A análise dos atributos, diretrizes e técnicas das Evidências, mostrou que de fato é possível buscar complementariedade entre este elemento comum e suas nuances em cada área.

Sabe-se que cada vez mais auditores estão sendo chamados a promover processos de investigação em suas esferas de atuação correcional, a exemplo de processos envolvendo pessoas físicas (Lei nº 8.112/90) e, mais recentemente, pessoas jurídicas, com o advento da Lei nº 12.846/13 e os Processos Administrativos de Responsabilização (PAR).

De modo geral, como os auditores governamentais estão na linha de frente dos processos finalísticos dos órgãos públicos, convém destacar a importância da promoção de iniciativas de *forensics readiness* e de possíveis melhorias de evidências digitais, dado o grande avanço na digitalização de políticas e serviços públicos.

Ademais, em atualizações futuras do Referencial Teórico para a auditoria interna governamental, sugere-se a inserção de elementos aqui discutidos, em especial a menção direta à norma ABNT NBR ISO/IEC 27037:2013 e seus conteúdos de confiabilidade, balizando assim o cuidado necessário com as evidências digitais coletadas para suportar achados em trabalhos de auditoria.

Em organizações onde existam estruturas atuando como equipes especializadas do tipo *Computer Security Incident Response Team* (CSIRT), muito do que foi comentado aqui fica a cargo desse time que fará o primeiro contato com os cenários de trabalho. Contudo, essas estruturas não excluem as responsabilidades de integração com a área de Auditoria, principalmente quando se pensa no potencial de práticas de *Forensics Readiness* tem de facilitar a atuação destes, necessitando de comunicação clara e eficaz entre essas duas áreas.

Como novas frentes de estudo, sugere-se a investigação casuística, tornada pública por força dos mecanismos de transparência ativa, para se colher percepções de como esses atributos estão operando e sendo comunicados no momento final das ações de auditoria governamental nos diversos órgãos da administração pública brasileira. Na mesma linha, podem ser realizados estudos sobre como esses auditores estão recomendando melhorias diversas em processos e sistemas estruturantes que tem potencial para geração de evidências digitais.

REFERÊNCIAS

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27037**: resumo: Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2013.

AUDITORIA In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. São Paulo: Editora Melhoramentos Ltda, 2015. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/auditoria/ Acesso em: 17/07/2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em12/07/2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 93, de 26 de setembro de 2019. Diário Oficial da União, Poder Executivo, Brasília, DF, 1 out. 2019. Seção 1. Disponível em https://govti.trt8.jus.br/conformidade/media/base_juridica/PORTARIA%20PR-GSI%20N%C2%BA%2093-2019%20Gloss%C3%A1rio%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A30.pdf. Acesso em 14/07/2025.

BRASIL. **Instrução Normativa nº 03**, de 09 de junho de 2017. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Disponível em https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-1.pdf . Acesso em 12/07/2025.

BRASIL. **Instrução Normativa nº 08**, de 06 de dezembro de 2017. Aprova o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Disponível em https://repositorio.cgu.gov.br/bitstream/1/33405/19/Instrucao_Normativa_8_Manual_Auditoria_2017.pdf . Acesso em 15/07/2025.

BRASIL. **Lei nº 10.180**, de 12 de fevereiro de 2001. Dispõe sobre a organização e funcionamento da Comissão de Ética Pública e dá outras providências. Brasília, DF: Disponível em https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10180.htm. Acesso em 12/07/2025.

BRASIL. **Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal**. Brasília: CG. 2017. Disponível em https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/pgmq/arquivos/in-sfc-08-2017-mot.pdf/view. Acesso em 15/07/2025.

BRASIL. Orientação Prática: Serviços de Auditoria. **Base de Conhecimento da CGU**, nov. 2022.

IIA. **Global Practice Guide: Internal Auditing and Fraud, 3rd Edition | The IIA**. Disponível em:<https://www.theiia.org/en/content/guidance/recommended/supplemental/practiceguides/global-practice-guide-internal-auditing-and-fraud/>. Acesso em: 15 jul. 2025.

ROWLINGSON, Robert. A ten step process for forensic readiness. **International Journal of Digital Evidence**, v. 2, n. 3, p. 1–28, 2004.

BRÜGER, Ana Carmen Collodetti; LORENS, Evandro Mário. **Forensic readiness: uma abordagem proativa de apoio à análise forense digital - Fronteiras em Ciências Forenses**. Fronteiras em Ciências Forenses, Brasília, ano 01, nº 02, p. 37-49. Disponível em: https://fronteirasemcienciasforenses.apcf.org.br/publicacoes/forensic-readiness-uma-abordagem-proativa-de-apoio-a-analise-forense-digital . Acesso em: 15 jul. 2025.

CASEY, Eoghan. **Digital evidence and computer crime: Forensic science, computers, and the internet.** Academic press, 2011.

CASTELLS, Manuel. **A Sociedade em Rede**. São Paulo: Paz e Terra, 1999. (Volume I da trilogia "A Era da Informação: Economia, Sociedade e Cultura").

ELEUTÉRIO, Pedro Monteiro da Siliva; MACHADO, Marcio Pereira. **Desvendando a computação forense**. Novatec Editora, 2019.

IIA. **Global Practice Guide: Internal Auditing and Fraud, 3rd Edition | The IIA**. Disponível em: https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/global-practice-guide-internal-auditing-and-fraud/. Acesso em: 15 jul. 2025.

MAGNO, Levy Emanuel; COMPLOIER, Mylene. **Cadeia de custódia da Prova Penal**. Cadernos Jurídicos, São Paulo, ano 22, nº 57, p. 195-219, janeiro-março/2021. Disponível em: https://www.tjsp.jus.br/ Acesso em: 10 abr 2023.p.203.

OLIVEIRA, Daiana Souza; SANTIAGO, Vinícius Vale; DA COSTA, Adriana Vieira. **Perícia forense computacional: a admissibilidade e a fragilidade das evidências coletadas via computação forense. Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 5, p. 3978-3997, 2023.

PERÍCIA In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. São Paulo: Editora Melhoramentos Ltda, 2015. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/auditoria/ Acesso em: 17/07/2025

ROWLINGSON, Robert et al. A ten step process for forensic readiness. International Journal of Digital Evidence, v. 2, n. 3, p. 1-28, 2004.

SINGH, Rishita. **Deepfake Evidence And Criminal Trials–Challenges To Justice In the AI Era**. Journal of Legal Research and Polity, v. 1, n. 1, p. 11-22, 2025.

SILVA, Paulo Daniel Bonfim; DA ROCHA, Siomara Dias. **Estado da Arte sobre a perícia digital forense. Cuadernos de Educación y Desarrollo**, v. 17, n. 6, p. e8601-e8601, 2025.

SMITH, G. Stevenson. **Computer forensics: helping to achieve the auditor's fraud mission**. Journal of Forensic Accounting, v. 6, n. 1, p. 119-134, 2005.

VERDOLIVA, Luisa. **Media forensics and deepfakes: an overview**. IEEE journal of selected topics in signal processing, v. 14, n. 5, p. 910-932, 2020.