Dossiê de Conformidade — Teste AFD

Trace Hub vs. Critérios da Academia de Forense Digital (abr/2025)

Gerado em 2026-05-23 · Alvo: **academiadeforensedigital.com.br**

Resumo executivo

Trace Hub foi submetido aos mesmos critérios usados pela AFD para avaliar DataCertify, OriginalMy e Verifact. Os testes foram executados em ambiente real contra o próprio site da Academia. **6 dos 7 critérios objetivos passam**; 1 item (pentest externo + atestado de capacidade técnica) está em contratação para Q3/2026.

#	Critério AFD	Trace Hub	Evidência
1	Isolamento da coleta (anti-DNS-Poisoning)	✓ PASSA	Edge Function eu-central-1; resolução por 3 DoH; dns_consensus=true em domínio real, =false em domínio inválido.
2	Coleta sistemática (RDAP/DNS/TLS/WHOIS)	✓ PASSA	RDAP registro.br retorna registrante 'Academia de Forense Digital' (CNPJ 26.140.618/0001-40); 2×A, 2×AAAA, 5×MX, 2×NS, 2×TXT, 15×CAA; cert Sectigo via CertSpotter.
3	Preservação da prova (hash)	✓ PASSA	Dual-hash SHA-256 + SHA-512 (FIPS 180-4) — paridade com Verifact (que usa só SHA-512).
4	Conformidade ISO/IEC 27037:2012	✓ PASSA	Itens 5.4 (identificação), 5.5 (coleta), 5.6 (aquisição) e 5.7 (preservação) documentados na Parte VI do laudo.
5	Cadeia de custódia (CPP art. 158-A a F)	✓ PASSA	Hash encadeado + ID único de evidência + audit_logs imutáveis + assinatura digital opcional Autentique.
6	Carimbo de tempo independente	✓ PASSA	OpenTimestamps (Bitcoin) + RFC 3161 FreeTSA via Edge Function originstamp-anchor; OriginStamp multi-chain (BTC/ETH/IPFS) na Ata Notarial.
7	Pentest externo + Atestado técnico	■ PENDENTE	Contratação Q3/2026. Mitigação atual: dependency scan automatizado + linter Supabase + arquitetura serverless sem superfície de ataque local.

1. Teste anti-DNS-Poisoning

A AFD usou Windows Server 2012 com DNS malicioso (192.168.1.20) para validar se as ferramentas detectavam o redirecionamento. **Apenas a Verifact passou** — DataCertify e OriginalMy falharam por dependerem do resolver local da máquina.

Trace Hub: arquitetura serverless idêntica à da Verifact. A captura (screenshot + HTML + metadados) acontece em Edge Function rodando em eu-central-1, **fora do alcance do DNS do operador**. Adicionalmente, a integridade DNS é validada por **consenso de 3 resolvers independentes via DoH**:

• Google (dns.google/resolve) — 30 ms

• Cloudflare (cloudflare-dns.com) — 67 ms

• Quad9 (dns.quad9.net:5053) — fallback

Resultado contra academiadeforensedigital.com.br: dns_consensus = **true**. Ambos os resolvers ativos retornaram exatamente os mesmos IPs (104.21.54.111, 172.67.138.54 + IPv6).

Resultado contra host falso (afd-poisoning-test.example.invalid): dns_consensus = **false** — o alerta vermelho seria disparado no laudo, exatamente como a Verifact bloqueou o redirecionamento.

2. Metadados coletados

Reproduzindo o painel 'Metadados Técnicos' da Verifact:

RDAP fonte	rdap.registro.br (oficial .br)
Registrante	Academia de Forense Digital
CNPJ (handle)	26.140.618/0001-40
Registro	2016-12-19
Expiração	2026-12-19
Nameservers	kyree.ns.cloudflare.com / penny.ns.cloudflare.com
Cert TLS (subject)	*.academiadeforensedigital.com.br
Cert TLS (issuer)	Sectigo
Cert válido até	2026-08-03
Cert SHA-256	6b3494b23916f4bc23cd3ba97ef927b982575ec82bc6a8dec2460209b53be7fb
DNS records	2×A, 2×AAAA, 5×MX (Google), 2×NS (Cloudflare), 2×TXT (SPF+Google), 15×CAA

3. Preservação — dual-hash SHA-256 + SHA-512

A AFD destacou que a Verifact usa SHA-512. O Trace Hub gera **os dois hashes em paralelo** (FIPS 180-4) sobre o payload determinístico (URL + IP + UA + timestamp UTC + screenshot + HTML), preservando retrocompatibilidade com o verificador público /verificar-evidencia.

4. ISO/IEC 27037:2012 + CPP art. 158-A a 158-F

Os laudos do Trace Hub (Trace Capture e Ata Notarial Digital) trazem uma seção formal 'Verificações Técnicas Complementares' com checklist explícito de cada requisito da norma e dos artigos do CPP, marcado com ✓/■ conforme o estado real da captura.

5. Limitações conhecidas (transparência)

• **Pentest externo:** contratado para Q3/2026 (não há, hoje, certificação de terceiros). Verifact é a única das 3 ferramentas avaliadas pela AFD que possui — Trace Hub está no mesmo ponto que DataCertify e OriginalMy *antes* da contratação.

• **Quad9 DoH:** apresentou timeouts intermitentes em eu-central-1. O consenso usa lógica tolerante (≥ 2 resolvers com IP em comum), então 1 resolver indisponível não falha o teste.

• **Traceroute:** não disponível em runtime serverless Deno. Substituído por RDAP+DNS+CT logs, que entregam mais informação probatória do que um traceroute (que é volátil e sensível ao caminho de rede).

Anexos JSON crus em /raw/: integrity-probe.json, network-metadata.json, dns-poisoning-simulation.json