

Is quintapata.com.ar a scam? TrustSniffer's high-risk assessment: 0/100

quintapata.com.ar

Verdict

0

OUT OF 100

CRITICAL RISK

quintapata.com.ar shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-19 by automated analysis. Classification confidence 55%.

What this site appears to be

GPT summary status=skipped | No usable content for GPT summary (clean/dom/html all empty)

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	15 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	5.3 years old Registered history	CLEAR
Web archive	Archived since 2007 Public history exists	CLEAR
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2007.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

quintapata.com.ar is a web domain whose available capture contains no substantive visitor-facing business, product, or legal content, so its apparent purpose and operating model cannot be established from the supplied evidence.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because external security intelligence records a confirmed blacklist condition, including 15 malicious detections and one suspicious detection, with Fortinet and Sophos among the flagged vendors. This is a direct contradiction to safe use for login, credential submission, or financial activity. The available behavioral evidence did not observe wallet connections, wallet-drainer activity, hidden forms, clipboard hijacking, or suspicious inline scripts; those limited technical observations do not offset the external threat detections. No separate identity inconsistency, impersonation, or phishing contradiction is marked present in the structured findings, but the blacklist evidence alone requires a security-forward posture.

EVIDENCE

- External reputation assessment recorded 15 malicious and 1 suspicious detections; Fortinet and Sophos were identified among the flagged vendors.
- The domain was marked by two blacklist sources, with the external kill-switch condition active.
- Behavioral testing recorded 0 wallet-connect runs, 0 wallet-drainer runs, 0 hidden forms, and 0 clipboard-write detections.
- Domain registration continuity is recorded as 5.26 years; the archival record shows 0 snapshots, with first-seen date 2007-07-05, last-seen date 2026-04-15, and 20 years tracked.

Regulatory Verification Notes

Real-world operator identity remains unverified, and the available evidence indicates ownership and governance opacity. Licensing, registration, and the responsible legal entity cannot be established from the supplied site material; this is a regulatory verification gap rather than an independent finding of fraud. The low page-authority signal provides little corroboration for the site’s standing. A valid domain-validated certificate and identifiable hosting are positive technical conditions, but they do not establish legal operation or regulatory authorization.

EVIDENCE

- The identity-verification status is recorded as unknown, with no independently verified connection to a real-world entity.
- The site's TLS certificate is issued by Sectigo Public Server Authentication CA DV R36, uses DV validation, and is valid through 2027-02-22.
- The site is hosted on AS27823, Dattatec.com, AR.
- Page-authority assessment is in the low band.

What to Verify Next

Any proposed engagement should remain limited to non-sensitive inspection until an independently confirmed operator, legal entity, and applicable authorization are established. The relevant financial, payments, or digital-asset regulator should be checked directly for the entity and service involved; contact channels should be confirmed through an independent offline route, and any payment destination or account beneficiary should be matched to the verified legal entity before funds or credentials are considered.

EVIDENCE

- The supplied material does not establish the site's legal operator or licensing status.
- The domain's external reputation contains confirmed malicious and blacklist detections requiring independent validation before sensitive interaction.
- The certificate provides transport encryption but only domain-validated assurance, not organizational identity validation.

Summary Verdict

The overall posture is critical, with the available evidence supporting a conclusion of unacceptable risk for sensitive interaction. The site's legitimacy and operator identity are not independently established, and the external threat evidence materially outweighs the limited benign technical observations.

Infrastructure Integrity

The domain resolves directly to a single likely origin address on AS27823, Dattatec.com, with no detected CDN or WAF layer. Its Sectigo DV certificate remains valid through 2027-02-22, supporting encrypted transport but offering no assurance about the operator's identity or the site's legitimacy.

Closing Assessment

Enterprise controls should block or isolate the domain for credential, payment, account, and other sensitive workflows pending independent resolution of the threat detections and confirmation of the responsible entity.

Written analysis generated 2026-08-19 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, external reputation.

01 Governance Risk

- The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.

Analysis engine signal:direct_threat

- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.

External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNKNOWN
Identity score	50/100
Identity verification confidence	30%

- AI page analysis unavailable (page captured; identity not AI-verified)

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of quintapata.com.ar.

- The request stayed on quintapata.com.ar. It was not redirected to another domain. [CLEAR](#)
- The earliest public archive of this site is from 2007-07-05. [CLEAR](#)
- It is hosted on AS27823, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	AS27823 - Dattatec.com, AR
Country	US
Server IP	66.97.40.248
Name servers	Not available
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2027-02-22
Domain age	5.26 years (continuous registration)
Domain expiry	Not available

Archive first seen	2007-07-05
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about quintapata.com.ar at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/quintapata.com.ar> · assessed 2026-08-19