Informe de Inteligencia

Investigación fraude/estafa digital



Actor investigado:

Categoría: Fraude / Estafa digital

Fecha de inicio: 2-2026

Fecha de finalización: 0-2026

Investigador: David Padron

Contacto:

Índice

1. Alcance y Objetivos....5
   1.1 Objetivo de la investigación....5
   1.2 Alcance de la investigación....6
   1.3 Límites de la investigación....6
2. Metodología....8
   2.1 Planificación y definición del alcance....8
   2.2 Recopilación de datos....8
   2.3 Análisis y procesamiento....8
   2.4 Generación de inteligencia....9
   2.5 Aplicación estratégica....9
3. Técnicas y procedimientos....10
   3.1 Investigación de fuentes abiertas — OSINT....10
   3.2 Inteligencia de redes sociales — SOCMINT....10
   3.3 Reconocimiento de infraestructura digital....10
   3.4 Análisis de direcciones IP....11
   3.5 Análisis de cabeceras y tecnologías web....11
   3.6 Análisis geoespacial....11
   3.7 Análisis de filtraciones y exposición de información....11
   3.8 Análisis relacional y construcción de grafos....11
   3.9 Análisis temporal....11
4. Herramientas para recopilar y procesar datos....12
5. Resumen ejecutivo....13
   5.1 Hallazgos clave....14
      5.1.1 Infraestructura de comercio electrónico....14
      5.1.2 Uso de [redacted]....14
      5.1.3 Infraestructura DNS....14
      5.1.4 Vínculo con [redacted]....14
      5.1.5 Infraestructura IP....15
      5.1.6 Vinculación entre actores....15
      5.1.7 Medios de pago....16
         Cuenta [redacted]....16
         Cuenta [redacted]....16
      5.1.8 Actividad en redes sociales....16
      5.1.9 Indicadores de comportamiento anómalo....17
      5.1.10 Reclamos y patrón operativo....17
1. Análisis de inteligencia....19
   1. Perfil corporativo [redacted]....19
      1.2 Domicilio – Tienda física....20
   2. Roles y organización [redacted]....20
   3. Perfiles de los actores investigados....21
   3.1 [redacted]....21
      3.1.2 Información Fiscal....22
      3.1.3 Domicilio Legal – ARCA....22
      3.1.4 Evidencia – Constancia de Monotributo....23
   3.2 [redacted]....24
      3.2.1 [redacted]....25
      3.2.2 [redacted]....25
      3.2.3 [redacted]....26
   3.3 [redacted]....26
      3.3.1 Consideraciones sobre la identificación de [redacted]....27
      3.3.2 Información Fiscal – Perfil 1 ([redacted])....27

3.3.3 [redacted] 28
3.3.4 [redacted] 28
3.3.5 [redacted] 29
3.3.6 [redacted] 29
3.3.7 [redacted] 30
3.4 [redacted] 30
3.4.1 [redacted] 31
3.4.2 [redacted] 31
3.4.2 [redacted] 32
3.5 [redacted] 32
3.5.1 [redacted] 33
3.5.2 [redacted] 33
3.5.3 [redacted] 34
3.5.4 [redacted] 34
[redacted] 35
Historial Crediticio [redacted] 36
3.5.5 Evidencia – Datos Bancarios identificados 36
3.6 [redacted] 37
3.6.1 [redacted] 38
3.6.2 [redacted] 38
3.6.3 [redacted] 39
3.6.4 Actividad crediticia 39
3.6.5 Evidencia – [redacted] 39
3.6.6 Evidencia – Estudios [redacted] 40
4. Redes sociales [redacted] 41
4.1 Evidencia – Cuentas activas 42
4.2 Evidencia – Cuentas [redacted] 44
4.3 Vinculación teléfonos y cuentas 46
4.4 Evolución de seguidores y comportamiento de las cuentas 46
4.4.1 Evidencia – Incremento de seguidores en [redacted] 47
5. Redes sociales personales 50
5.1 Evidencia – [redacted] 51
5.2 Evidencia – [redacted] 51
5.3 Evidencia – [redacted] 52
5.4 Evidencia – [redacted] 54
5.5 Evidencia – [redacted] 54
5.6 Evidencia – [redacted] 55
6. Números de teléfono 57
6.1 Evidencia - ([redacted]) 57
6.2 Evidencia - ([redacted]) 58
6.3 Evidencia - ([redacted]) 58
7. Correos electrónicos 59
7.1 Evidencia – [redacted] 59
7.2 Evidencia – [redacted] 60
7.3 Evidencia - [redacted] 60
8. Logística – [redacted] 61
8.1 Evidencia 1 62
8.2 Evidencia 2 63
8.2.1 Instagram Storie 63
8.2.2 Elemento 1 – [redacted] 65
8.2.3 Elemento 2 – Cartel publicitario 65
8.2.4 Elemento 3 – Cartel nomenclador 65

8.2.5 Elemento 4 – Edificio comercial....66
9. Infraestructura y dominio web....67
9.1 Evidencia – Whois....67
9.2 Evidencia - DNS....68
9.3 Evidencia – CNAME....69
9.4 Evidencia – HTTP Headers....69
Vinculación con [redacted]....70
9.5 Evidencia -[redacted]....70
10. Inteligencia geoespacial....71
10.1 Ubicaciones – Residenciales....71
10.2 Ubicaciones – Comercio – [redacted]....72
11. Correlación de infraestructura, identidades y medios de operación....73
12. Modus operandi observado en las operaciones online....73

1. Alcance y Objetivos

1.1 Objetivo de la investigación

El objetivo principal de la presente investigación consiste en **identificar, caracterizar y correlacionar la infraestructura digital, personas, medios de contacto, relaciones comerciales y patrones de comportamiento asociados al** [redacted], con especial atención a las actividades desarrolladas a través de sus canales digitales y de comercio electrónico.

La investigación busca generar inteligencia a partir de fuentes abiertas y registros disponibles públicamente, con el propósito de determinar:

- La identidad y función de los principales actores vinculados al [redacted]
- Las relaciones existentes entre las personas identificadas y la actividad comercial investigada.
- La infraestructura tecnológica utilizada para la operación de la tienda online.
- Los dominios, direcciones IP, servicios de alojamiento, proveedores tecnológicos y mecanismos de protección asociados.
- Los canales de comunicación y medios utilizados para concretar operaciones comerciales.
- Los mecanismos empleados para recibir pagos y gestionar los envíos de productos.
- La existencia de patrones de comportamiento relevantes para la investigación.
- La posible existencia de vínculos entre los diferentes actores, cuentas, números telefónicos, perfiles sociales, medios de pago e infraestructura digital.
- La identificación y documentación de indicadores que permitan comprender el posible modus operandi asociado a las operaciones investigadas.

El resultado esperado es la elaboración de un **producto de inteligencia basado en evidencia**, destinado a facilitar la comprensión del ecosistema investigado y apoyar posteriores procesos de validación, investigación o toma de decisiones.

1.2 Alcance de la investigación

La investigación comprende el análisis de información correspondiente al [redacted] sus canales digitales y los actores que, de acuerdo con la información recopilada, presentan algún grado de vinculación con su actividad comercial.

El alcance comprende las siguientes dimensiones:

Identidad y organización:
Identificación de personas relacionadas con el [redacted], sus posibles funciones, relaciones interpersonales y vínculos con las actividades comerciales observadas.

Presencia digital:
Análisis de perfiles y cuentas utilizadas en redes sociales, números telefónicos,

direcciones de correo electrónico, dominios web y demás identificadores digitales asociados.

Infraestructura tecnológica:
Reconocimiento del dominio [redacted], registros WHOIS, DNS, resolución de nombres, direcciones IP, proveedores de infraestructura, [redacted] plataformas de comercio electrónico y cabeceras HTTP.

Actividad comercial:
Análisis de los canales utilizados para la comercialización de productos, recepción de pagos, comunicación con clientes y gestión de pedidos.

Logística:
Identificación de los servicios utilizados para el despacho y distribución de productos adquiridos mediante la tienda online.

Análisis relacional:
Correlación de identidades, cuentas, teléfonos, correos electrónicos, ubicaciones, infraestructura y demás indicadores obtenidos durante la investigación para determinar posibles relaciones entre los diferentes elementos.

Análisis temporal:
Cuando la información disponible lo permitió, se consideraron fechas de creación, modificación, actividad y evolución de los diferentes activos digitales para establecer una posible secuencia temporal de los acontecimientos.

1.3 Límites de la investigación

La presente investigación se encuentra limitada a la **información disponible mediante fuentes abiertas, registros públicos, servicios de consulta y fuentes accesibles legalmente** durante el período de investigación.

No se realizaron actividades destinadas a obtener acceso no autorizado a sistemas, cuentas, dispositivos, bases de datos o infraestructura perteneciente a terceros.

Asimismo, debe considerarse que:

- La información disponible públicamente puede encontrarse incompleta, desactualizada o presentar errores.
- La asociación de una persona con una cuenta, teléfono, dirección de correo electrónico o activo digital no implica por sí misma que dicha persona haya realizado determinada actividad.
- Las relaciones inferidas mediante correlación de datos deben considerarse hipótesis hasta contar con evidencia independiente que permita su validación.
- La geolocalización de direcciones IP representa una aproximación del punto de presencia de la infraestructura y **no debe interpretarse como la ubicación física del operador o usuario**.
- La utilización de un proveedor tecnológico determinado no implica necesariamente una relación contractual directa entre dicho proveedor y el sujeto investigado.

- La eliminación, modificación o ausencia de contenido en redes sociales puede dificultar la reconstrucción completa de determinadas actividades.
- Los datos obtenidos de servicios de terceros pueden presentar limitaciones de cobertura, precisión o actualización.
- Las conclusiones relacionadas con posibles conductas fraudulentas deben ser consideradas **valoraciones de inteligencia e hipótesis investigativas**, y no determinaciones judiciales.

En consecuencia, las conclusiones del presente informe deben interpretarse en función del **grado de confianza asignado a cada hallazgo y de la evidencia que lo sustenta**.

2. Metodología

El proceso de investigación se desarrolló mediante una metodología estructurada de **Open Source Intelligence (OSINT), Social Media Intelligence (SOCMINT) y Cyber Threat Intelligence aplicada al análisis de infraestructura digital**, orientada a recopilar, procesar, correlacionar y transformar información dispersa en inteligencia accionable.

El ciclo de investigación se estructuró en las siguientes etapas:

2.1 Planificación y definición del alcance

Se definieron el objeto de investigación, los activos digitales iniciales, los actores de interés y las principales preguntas de inteligencia.

A partir de los identificadores iniciales se establecieron diferentes líneas de investigación relacionadas con identidad, infraestructura tecnológica, redes sociales, medios de contacto, actividad comercial, medios de pago y logística.

2.2 Recopilación de datos

Se realizó la obtención sistemática de información procedente de fuentes abiertas, registros públicos, motores de búsqueda, redes sociales, bases de datos disponibles públicamente, servicios de consulta de infraestructura y herramientas especializadas.

La información recopilada fue clasificada según su naturaleza y origen, procurando mantener la trazabilidad de los hallazgos y diferenciar información primaria de información obtenida mediante servicios de terceros.

2.3 Análisis y procesamiento

Los datos obtenidos fueron sometidos a procesos de normalización, comparación y correlación.

Se analizaron coincidencias entre nombres, identificadores, números telefónicos, cuentas de redes sociales, correos electrónicos, dominios, direcciones IP, ubicaciones, registros comerciales y demás indicadores.

Esta etapa permitió establecer relaciones entre elementos aparentemente independientes y construir una representación del ecosistema digital y operativo asociado al objeto de investigación.

2.4 Generación de inteligencia

Los hallazgos fueron transformados en productos de inteligencia mediante la elaboración de perfiles, líneas temporales, relaciones entre actores, análisis de infraestructura, identificación de patrones y formulación de hipótesis.

Las conclusiones fueron diferenciadas entre:

- **Hecho confirmado:** información respaldada directamente por una fuente.
- **Correlación:** relación identificada entre dos o más indicadores independientes.
- **Inferencia:** conclusión obtenida a partir del análisis de diferentes elementos.

- **Hipótesis:** explicación posible que requiere validación adicional.

2.5 Aplicación estratégica

La inteligencia generada permite comprender la estructura digital y operativa del emprendimiento investigado, identificar puntos de interés para futuras investigaciones y establecer nuevas líneas de adquisición de información.

Asimismo, los resultados pueden utilizarse como base para posteriores procesos de validación mediante fuentes oficiales, requerimientos legales, análisis forense u otras técnicas de investigación autorizadas.

3. Técnicas y procedimientos

Durante la investigación se empleó un conjunto de técnicas de **OSINT, SOCMINT y reconocimiento de infraestructura digital**, orientadas a obtener y correlacionar indicadores técnicos, personales y comerciales.

Entre las principales técnicas utilizadas se encuentran:

3.1 Investigación de fuentes abiertas — OSINT

Se realizaron consultas sobre motores de búsqueda, bases de datos públicas, registros comerciales, registros gubernamentales y servicios de información disponibles en Internet.

El objetivo fue identificar información relacionada con personas, organizaciones, dominios, teléfonos, correos electrónicos, ubicaciones y actividad comercial.

3.2 Inteligencia de redes sociales — SOCMINT

Se analizaron perfiles públicos de Facebook, Instagram, TikTok, LinkedIn y otras plataformas con el objetivo de identificar:

- Relaciones entre personas.
- Vínculos entre cuentas personales y comerciales.
- Actividad y evolución de perfiles.
- Publicaciones y contenido multimedia.
- Información laboral y comercial.
- Números telefónicos y otros identificadores expuestos públicamente.
- Patrones de interacción entre los diferentes actores.

3.3 Reconocimiento de infraestructura digital

Se efectuó reconocimiento pasivo y activo de la infraestructura asociada al dominio investigado mediante consultas WHOIS, DNS, resolución de nombres, trazas de red, identificación de proveedores, análisis de certificados y reconocimiento de tecnologías web.

Esta actividad permitió identificar componentes relacionados con [redacted], [redacted] y [redacted], así como analizar la relación aparente entre los registros administrativos y la infraestructura actualmente utilizada.

3.4 Análisis de direcciones IP

Se analizaron las direcciones IPv4 asociadas al dominio, incluyendo información ASN, organización responsable, proveedor de red y geolocalización aproximada.

La información fue posteriormente correlacionada con las trazas de red obtenidas para determinar la presencia de servicios intermediarios como [redacted] y la infraestructura de backend asociada.

3.5 Análisis de cabeceras y tecnologías web

Se analizaron las respuestas HTTP/HTTPS del dominio con el objetivo de identificar tecnologías, mecanismos de protección, redirecciones, políticas de seguridad, servicios [redacted] y otros indicadores técnicos.

3.6 Análisis geoespacial

Se utilizaron herramientas cartográficas y servicios de imágenes para analizar ubicaciones asociadas al emprendimiento y a los actores investigados.

Cuando fue posible, se efectuó reconocimiento visual mediante imágenes públicas y Street View para establecer correspondencias entre ubicaciones físicas y la información obtenida mediante otras fuentes.

3.7 Análisis de filtraciones y exposición de información

Se realizaron consultas en servicios especializados para determinar la posible exposición de direcciones de correo electrónico, identificadores y otros elementos en bases de datos conocidas o incidentes de filtración.

Los resultados obtenidos de este tipo de fuentes fueron considerados **indicadores de investigación** y no evidencia suficiente por sí mismos para atribuir una actividad determinada a una persona.

3.8 Análisis relacional y construcción de grafos

Los diferentes indicadores obtenidos fueron relacionados mediante grafos para representar visualmente las conexiones existentes entre personas, cuentas, teléfonos, dominios, direcciones, empresas, servicios tecnológicos y otros elementos relevantes.

Esta técnica permitió identificar nodos con mayor cantidad de conexiones y posibles puntos centrales dentro del ecosistema investigado.

3.9 Análisis temporal

Se compararon fechas de creación, modificación y actividad de diferentes activos digitales con el objetivo de establecer una posible línea temporal y detectar cambios en la infraestructura, cuentas o actividad del [redacted].

4. Herramientas para recopilar y procesar datos

Para la adquisición, procesamiento, análisis y representación de información se utilizaron las siguientes herramientas y fuentes:

Categoría	Herramientas / fuentes
Bases de datos abiertas	Dateas, ARCA, ARBA, ANSES
Motores de búsqueda	Google, DuckDuckGo
Cartografía y geolocalización	Google Maps, Google Street View
Redes sociales	Facebook, Instagram, X/Twitter, LinkedIn, TikTok
Telefonía y mensajería	WhatsApp, Ph0mber, Movistar, Mi Claro, Personal, Tuenti
Reconocimiento de cuentas	GHunt, Holehe, Sherlock
Exposición de datos	Have I Been Pwned, Pentester, BreachDirectory
Análisis IP	IP-API, IPinfo
Tratamiento de imágenes	Pixelcut
Diagramación	diagrams.net
Ofimática	LibreOffice Writer
Análisis de grafos	Gephi
Reconocimiento de infraestructura web	WHOIS, dig, nslookup, mtr, OpenSSL, WhatWeb, Wafw00f
Descubrimiento de URLs	Katana, Waybackurls, GAU, Hakrawler

Nota metodológica: las herramientas constituyen mecanismos de adquisición y análisis, pero la utilización de una herramienta no convierte automáticamente un resultado en evidencia concluyente. Los resultados fueron sometidos a procesos de validación cruzada y correlación con otras fuentes disponibles.

5. Resumen ejecutivo

La investigación permitió identificar y caracterizar un **ecosistema comercial y digital compuesto por infraestructura web, redes sociales, medios de contacto, actores individuales, mecanismos de pago y servicios logísticos**, asociados al [redacted].

El análisis técnico del dominio [redacted] permitió determinar con un alto grado de confianza la utilización de [redacted] **como plataforma de comercio electrónico**, mientras que [redacted] interviene como capa de protección y proxy inverso. La resolución DNS autoritativa observada corresponde a [redacted].

En relación con [redacted]

[redacted]

Estos elementos, considerados en conjunto, constituyen **indicadores relevantes para profundizar la investigación**, aunque determinadas hipótesis requieren validación mediante fuentes independientes y evidencia adicional.

5.1 Hallazgos clave

5.1.1 Infraestructura de comercio electrónico

Se identificó que [redacted] utiliza infraestructura asociada a [redacted], evidenciada principalmente mediante el [redacted] hacia [redacted] y las características observadas en las respuestas HTTP.

Nivel de confianza: Alto.

5.1.2 Uso de [redacted]

El dominio se encuentra detrás de [redacted], que actúa como intermediario entre los usuarios y la infraestructura de origen, proporcionando funciones asociadas a [redacted].

[redacted]

Nivel de confianza: Alto.

5.1.3 Infraestructura DNS

Las consultas DNS actuales muestran cuatro servidores autoritativos pertenecientes al esquema de [redacted]:

- ns-[redacted]
- ns-[redacted]
- ns-[redacted]
- ns-[redacted]

[redacted]

Nivel de confianza: Alto.

5.1.4 Vínculo con [redacted]

Los registros WHOIS identifican a [redacted] como contacto asociado al registro del dominio y muestran adicionalmente [redacted].

[redacted]

Nivel de confianza: Alto para la asociación registral; bajo/moderado para atribuir una función operativa actual.

5.1.5 Infraestructura IP

Las direcciones [redacted] se encuentran asociadas a infraestructura de [redacted], mientras que el tráfico observado hacia el dominio atraviesa previamente infraestructura de [redacted].

[redacted]

[redacted]

Nivel de confianza: Alto para la infraestructura observada; limitado para determinar propiedad física del servidor.

5.1.6 Vinculación entre actores

Se identificaron múltiples coincidencias entre personas investigadas, perfiles de redes sociales, números telefónicos, cuentas comerciales y actividades relacionadas con el [redacted].

[redacted]

[redacted]

Nivel de confianza: Alto para las relaciones digitales observadas; variable respecto de la función exacta de cada persona.

5.1.7 Medios de pago

La investigación identificó cuentas bancarias utilizadas como mecanismos de recepción de transferencias asociadas a las operaciones comerciales investigadas.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Nivel de confianza: Alto respecto de la titularidad y existencia de los identificadores cuando fueron corroborados mediante fuentes disponibles; variable respecto de la finalidad de las operaciones.

5.1.8 Actividad en redes sociales

Las cuentas comerciales presentan una actividad significativa en Instagram, Facebook y TikTok, siendo utilizadas para promoción, atención de clientes, generación de contenido y difusión de la tienda online.

[redacted]

[redacted]

Nivel de confianza: Alto.

5.1.9 Indicadores de comportamiento anómalo

Durante el monitoreo se observaron patrones de crecimiento de seguidores y comportamiento de las cuentas que podrían resultar atípicos. [redacted]

Nivel de confianza: Bajo/Moderado.

5.1.10 Reclamos y patrón [redacted]

Se identificaron múltiples [redacted]

Nivel de confianza: Moderado/Alto, dependiendo de la cantidad, independencia y trazabilidad de las fuentes analizadas.

Versión limitada de informe



El presente documento corresponde a una versión limitada y parcialmente anonimizada del informe de investigación desarrollado en el marco de actividades de reconocimiento orientadas a investigación privada sobre un caso de estafa de comercio digital (ecommerce).

El acceso a la versión completa del informe requiere la coordinación previa de una reunión virtual, instancia en la que será posible dialogar directamente con el investigador responsable del trabajo, analizar los hallazgos obtenidos y abordar aspectos técnicos específicos de la investigación.

La publicación de este material tiene como único propósito exponer las capacidades, metodologías y competencias técnicas aplicadas por el investigador en entornos reales. En ningún caso se busca comercializar, divulgar o comprometer información privada, sensible o confidencial de terceros.

Este contenido está dirigido exclusivamente a reclutadores, profesionales de recursos humanos, responsables de contratación y organizaciones interesadas en la contratación de servicios de investigación, ciberinteligencia o propuestas

laborales, tanto en modalidad de relación de dependencia como de servicios profesionales independientes.