



INVESTIGACIÓN DE CAMPO · CASHCLOAK LATAM · CTI-LATAM-2026-001

Anuncios verificados, destinos que no coinciden

Cómo llegan las falsas inversiones y los formularios de tarjeta a usuarios argentinos. En dos días de uso normal de un teléfono vi anuncios pagos, marcados como "Patrocinado" y con la identidad del anunciante verificada por Google, que llevaban a falsas notas periodísticas, chatbots de inversión, formularios de tarjeta con marca de un broker argentino y captación de teléfonos para un call center. Las piezas comparten público, marcas y técnicas de persuasión, pero no un dueño demostrado.

ID DEL INFORME

CTI-LATAM-2026-001 · v2

AUTOR

Ezequiel Jorge La Terra
[ORCID 0009-0008-1677-4218](https://orcid.org/0009-0008-1677-4218)

OBSERVACIÓN

30/9 y 1/10/2026 (hora
de Argentina)

PUBLICACIÓN

octubre de 2026

CLASIFICACIÓN · LICENCIA

TLP: CLEAR · CC BY 4.0

ÍNDICE

01 Resumen ejecutivo

02 Hallazgos clave

03 Qué es y qué no es

04 Qué prueba un anuncio verificado

05 El recorrido

06 Las verticales

07 Lo que comparten

08 Demostrado y no demostrado

09 Impacto

10 Indicadores (IOCs)

11 MITRE ATT&CK

12 Recomendaciones

13 Método y limitaciones

14 Conclusión

15 Divulgación coordinada

16 Cómo citar y licencia

▲ No es una banda: es un mercado de tráfico

Entre el 30 de septiembre y el 1 de octubre de 2026 (hora de Argentina) observé, como usuario común, anuncios pagos dirigidos a usuarios argentinos, muchos con la identidad del anunciante verificada por Google, que llevaban a falsas notas periodísticas con chat de inversión, chatbots que simulan a un "gestor personal" de Mercado Libre y un recorrido de "CFD de Mercado Pago" que termina en captación para un call center. En los mismos días documenté además un formulario de tarjeta con código de seguridad que usa la marca Balanz sin ser Balanz.

Los anunciantes declarados están en al menos seis países (Reino Unido, Chipre, Países Bajos, Ucrania, Australia y Brasil) y no pude establecer un operador común. La evidencia describe un **circuito de adquisición de tráfico**: compradores de tráfico y plantillas que trabajan sobre el mismo público, no una persona ni un grupo. Para los defensores, eso significa que bloquear dominios sirve pero llega tarde: el punto de intervención más temprano es el anuncio, y el más concreto para un banco es la primera operación del cliente hacia un "broker" que nadie conoce.

CASHCLOAK LATAM es el nombre de seguimiento que uso en Cyber Threat Intelligence LATAM para esta investigación. Es una etiqueta de trabajo, no el nombre de un grupo ni de un actor.

▲ Siete hallazgos

01 La puerta de entrada es publicidad paga y verificada.

Anuncios de Google en el navegador y en Gmail Promociones con la leyenda "Identidad del anunciante verificada por Google". Esa verificación acredita quién paga el anuncio, no que la oferta sea legítima.

02 Los anunciantes declarados son muchos y están dispersos.

Anunciantes declarados en al menos seis países (Reino Unido, Chipre, Países Bajos, Ucrania, Australia y Brasil), con anuncios dirigidos a usuarios argentinos. Es coherente con un mercado de compradores de tráfico, no con un operador único.

03 El dominio del anuncio y el del destino pueden no coincidir.

Un anuncio que mostraba un sitio de moda femenina llevó a una falsa nota de inversión en otro dominio. Es compatible con una redirección o con cloaking; desde el lado del usuario no se puede determinar cuál de los dos ocurrió.

04 Mercado Libre es la marca más usada como señuelo,

en al menos tres formatos: falsa nota con chat, chatbot de "gestor personal" y "CFD de Mercado Pago". Que compartan marca no demuestra que compartan operador.

05 Un sitio con la marca Balanz pide la tarjeta completa con código de seguridad.

No es Balanz. Pedir el CVC en un formulario propio para "depositar" es una señal de riesgo grave, aunque no se pudo confirmar que se hayan robado tarjetas.

06 No todo lo que aparece en este circuito es fraude.

Una landing de "Guía Créditos ANSES" mostraba contenido temático sin pedir datos sensibles. Se incluye como contexto, no como phishing.

07 Un anuncio verificado apuntaba a un subdominio genérico

que no remite a ninguna marca conocida. Se publica como indicador de búsqueda, sin afirmar qué contenido servía.

▲ 03 • ALCANCE

▲ **Qué es y qué no es esta publicación**

Todo lo que describo lo vi como lo vería cualquier usuario: los anuncios que se mostraron en un teléfono, la información que Google ofrece en "Mi centro de anuncios" al tocar los tres puntos de cada anuncio, y las páginas que se abrieron al tocar el anuncio. Conservo las capturas con su hash criptográfico para que cada afirmación pueda auditarse.

Esta edición **no** atribuye nada a personas, **no** afirma que los anunciantes declarados operen los sitios de destino y **no** sostiene que todos los destinos pertenezcan a una misma operación. Tampoco afirma que Google, Mercado Libre, Balanz, YPF, La Nación, ANSES o los bancos cuyos logos aparecen hayan participado: son plataformas o marcas usadas como señuelo.

LOS ROLES ANTES QUE LOS NOMBRES

ROL	QUÉ HACE	QUÉ NO IMPLICA
Anunciante declarado	Figura como pagador del anuncio en "Mi centro de anuncios", con país e identidad verificada	No implica que diseñe el fraude, que controle el destino ni que sepa qué contenido se sirve
Dominio mostrado	El sitio que aparece en el anuncio	Puede ser un sitio de pantalla, distinto del destino real
Destino o landing	La página que efectivamente se abre	Puede rotar, cambiar de contenido o pertenecer a un tercero
Paso de conversión	Chat, formulario de teléfono, formulario de tarjeta	El tipo de paso define el daño: no es lo mismo un lead que un CVC
Marca suplantada	Mercado Libre, Balanz, La Nación, YPF, bancos, ANSES	Es víctima, no parte
Plataforma publicitaria	Sirve el anuncio y publica el disclosure	Su verificación es de identidad del pagador, no de la oferta

A los anunciantes que figuran como pagadores no los nombro ni los identifico de ninguna forma, ni indico de qué tipo son; sus datos van solo a la plataforma, por el canal de reporte correspondiente. Hablo únicamente de su país declarado, porque lo que importa es el patrón y no quién figura como titular.

▲ 04 • LA SEÑAL DE CONFIANZA

▲ Qué prueba un anuncio "verificado" y qué no

"Mi centro de anuncios" es una de las herramientas de transparencia más útiles que tiene un usuario: al tocar un anuncio de Google se puede ver quién lo pagó, su ubicación declarada y si su identidad fue verificada. En todos los anuncios relevantes que observé aparecía la leyenda "Identidad del anunciante verificada por Google".

Esa información prueba que existe una cuenta publicitaria cuyo titular declarado pasó la verificación de identidad y pagó ese anuncio. **No prueba** que ese titular haya diseñado el contenido de destino, que cobre o que opere la estafa: puede ser un afiliado que cobra por clic o por lead, un intermediario o alguien cuya identidad comercial fue usada por otro. Por eso trato el disclosure como un punto de partida para la plataforma, no como una atribución.

El problema de fondo: la señal de verificación describe al pagador, pero el usuario la lee como si describiera la oferta. Un anuncio "verificado" que lleva a una nota con el diseño de un diario nacional se percibe como doblemente confiable.

▲ 05 • EL RECORRIDO

▲ De la atención al dato

Las verticales observadas no recorren todas los mismos pasos, pero encajan en un esquema común:

1

Anuncio pago

"Patrocinado", con identidad del anunciante verificada.



2

Dominio mostrado → destino real

A VECES DISTINTOS

El sitio del anuncio puede no ser la página que se abre.



3

Persuasión

Falsa nota, marca conocida, autoridad prestada, urgencia.



4

Conversión

Chat · teléfono (+54) · tarjeta completa con CVC.



5

Siguiente paso fuera de la página

Llamada, "fianza", "depósito".

Las flechas describen el recorrido de un usuario, no una relación entre operadores. Que dos destinos compartan un paso no significa que los opere la misma persona.

▲ 06 • RECORRIDO DE LOS ANUNCIOS

▲ Seis verticales y un destino genérico

Vistas una por una parecen estafas sueltas. Lo que se observa es que casi todas llegaron por el mismo camino: publicidad paga, mostrada como "Patrocinado" en el navegador, en la pestaña Promociones de Gmail o en redes de anuncios nativos. Algunos destinos piden datos de tarjeta; otros, un teléfono; otros solo muestran contenido. No todos son fraude, y se aclara en cada caso.

La falsa nota periodística con chat de inversión

Un anuncio de Google mostraba un sitio de moda femenina; su disclosure identificaba como pagador a un anunciante declarado en Ucrania. Al tocarlo se abrió `lunarbutton[.]site`, con una nota que imitaba el diseño de La Nación: una plataforma de inversión "vinculada a Mercado Libre" y "respaldada por figuras públicas" prometía 450 % sobre un mínimo de 200.000 pesos. Seguía un chat con estética de WhatsApp, logos de bancos que operan en Argentina y la palabra clave del fraude de anticipo: una "fianza" a pagar antes de cobrar.

Otro anuncio, con pagador declarado en Australia, llevaba a una falsa nota con el mismo diseño que usaba el nombre de figuras públicas. El cambio de dominio es compatible con una redirección o con cloaking; no afirmo ninguna de las dos.

Por qué importa. Una revisión publicitaria que mira el dominio mostrado (un sitio de ropa) y no el destino final pierde exactamente el paso donde está el fraude.

El "gestor personal" de Mercado Libre

`epicharvest[.]info` llegó por un anuncio de Google con pagador declarado en Países Bajos e identidad verificada. Era un chatbot que simulaba a un "gestor personal" de Mercado Libre, con planes de 5, 10 y 20 millones de pesos, "verificado por YPF", que prometía convertir 150.000 pesos en 5.000.000 por mes. Terminaba en un formulario con prefijo +54 y una página de "¡Gracias!".

Evalúo con **confianza moderada** que comparte plantilla de chat con la vertical 1. No alcanza para decir que los opere la misma persona: estas plantillas se venden y se copian.

Por qué importa. El producto no es un pago inmediato sino un contacto: un teléfono argentino dispuesto a escuchar una oferta de inversión.

Formularios de captación con "apalancamiento"

En Gmail Promociones, un banner de Mercado Libre ofrecía operar con "apalancamiento 200:1" (anunciante declarado en el Reino Unido). Otro anuncio (anunciante declarado en Chipre) llevaba a un formulario idéntico: mismo diseño, depósito mínimo de 100 dólares y las mismas billeteras electrónicas. Evalúo con **confianza moderada** que es una misma plantilla usada por dos pagadores, patrón típico de las redes de afiliación de inversión de alto riesgo.

No afirmo que estas páginas sean fraudulentas; por eso sus dominios no se publican como indicadores y quedan para el reporte a la plataforma.

Una tarjeta pedida para "depositar"

`app.balanztrading[.]com` usa la marca de Balanz, una entidad financiera argentina real, con un formulario de "depósito" que pide número de tarjeta, titular, vencimiento y código de seguridad, acompañado de sellos de "Cumple PCI-DSS" y 3-D Secure. **No es Balanz**: la marca suplantada es víctima. Las capturas no registran qué anuncio llevó a esta página, así que no se asocia a ningún anunciante.

Pedir el CVC en un formulario propio, fuera de un procesador de pagos reconocible, es una señal de riesgo grave. No se pudo confirmar que se hayan robado tarjetas ni hecho cargos.

Por qué importa. Para un banco, una tarjeta cargada en un sitio así es una tarjeta potencialmente comprometida antes del primer cargo sospechoso.

"CFD de Mercado Pago" y el call center

En redes de anuncios nativos (los bloques de "contenido recomendado" al pie de sitios de noticias), tres anunciantes distintos ofrecían "CFD de Mercado Pago/Mercado Libre". El recorrido: una landing que imitaba una "app de pagos" y pedía un teléfono +54; luego `falcon-press[.]com`, con el aviso de que "un ejecutivo de inversiones lo llamará"; por último `lpa.voltfalcon-press[.]com`, con un identificador de sub-afiliado que no se publica.

Evalúo con **confianza moderada** que es captación de interesados para un call center de inversión: la presión y el pedido de dinero ocurren después, por teléfono.

Por qué importa. Cuando la conversión es un teléfono, bloquear el dominio llega tarde. La defensa útil está antes (en el anuncio) y después (en la alerta del banco ante la primera transferencia a un "broker").

ANSES como gancho comercial, sin phishing observado

Publicidad con temática de ANSES en Gmail Promociones llevaba a una landing "Guía Créditos ANSES" en un subdominio argentino de un sitio brasileño (anunciante declarado en Brasil). El dominio no se publica como indicador. No se observó formulario de datos sensibles ni pedido de pago. **No se califica como phishing.** Se incluye como contexto porque usar a un organismo de la seguridad social como gancho confunde a un público especialmente expuesto.

Un subdominio sin marca, pagado y verificado

Un anuncio "Patrocinado", de un anunciante declarado en Brasil con identidad verificada, llevaba a `descubre.upmegaconnectnotification[.]click`. No hay captura del contenido, así que no se describe ni se le atribuye vertical. Se publica para **búsqueda, no para bloqueo**, por tres rasgos: destino pagado y verificado, nombre genérico sin marca y extensión de bajo costo frecuente en infraestructura descartable.

▲ 07 • PATRÓN

▲ Lo que comparten: un repertorio, no un servidor

- **Autoridad prestada.** Un diario nacional, una petrolera estatal, bancos, un broker, un organismo público, el marketplace más grande de la región.
- **Verificación como escudo.** El anuncio "verificado" transfiere su credibilidad al destino, aunque solo cubra al pagador.
- **Promesas desproporcionadas.** 450 %, 150.000 pesos convertidos en 5.000.000 por mes, apalancamiento 200:1.
- **Un cobro anticipado.** "Fianza", "depósito mínimo", "depositar con tarjeta".
- **Una conversión que sale de la página.** Chat, llamada, formulario: el daño se completa en un canal que la página no muestra.

Ese repertorio es compatible con un mercado de plantillas, afiliados y compradores de tráfico. No se pudo establecer un operador común, y la diversidad de pagadores y países sugiere lo contrario: muchos actores que compiten por las mismas víctimas con las mismas herramientas.

▲ Qué está demostrado y qué no

AFIRMACIÓN	ESTADO
Hubo anuncios pagos dirigidos a usuarios argentinos con identidad del anunciante verificada por Google	OBSERVADO
Esos anuncios llevaban a falsas notas, chatbots de inversión, captación de teléfonos y un formulario de tarjeta con CVC	OBSERVADO
Al menos un anuncio mostraba un dominio y llevaba a otro	OBSERVADO
Ese salto se debe a cloaking	NO DETERMINADO Compatible con redirección o cloaking
Dos chatbots usan la misma plantilla	EVALUACIÓN • MODERADA
Dos formularios de captación usan la misma plantilla	EVALUACIÓN • MODERADA
El recorrido de "CFD de Mercado Pago" alimenta un call center	EVALUACIÓN • MODERADA
Los anunciantes declarados operan los destinos	NO ESTABLECIDO
Todas las verticales pertenecen a una misma operación o actor	NO ESTABLECIDO
Se robaron tarjetas o se produjeron cargos	NO CONFIRMADO
La landing de ANSES es phishing	NO No se observó captura de datos sensibles
Google, las marcas o los bancos participan	NO Son plataforma o marcas suplantadas

▲ A quién le pega y dónde

Usuarios. El fraude llega con todas las señales de legitimidad que se les enseñó a buscar: un buscador conocido, la etiqueta de verificación, el diseño de un diario nacional, el logo de su banco. "Desconfíe de los sitios raros" no alcanza cuando el sitio raro llega envuelto en señales oficiales.

Marcas suplantadas. Daño de reputación y de soporte: los usuarios estafados reclaman a Mercado Libre, a Balanz o a su banco, no al anunciante.

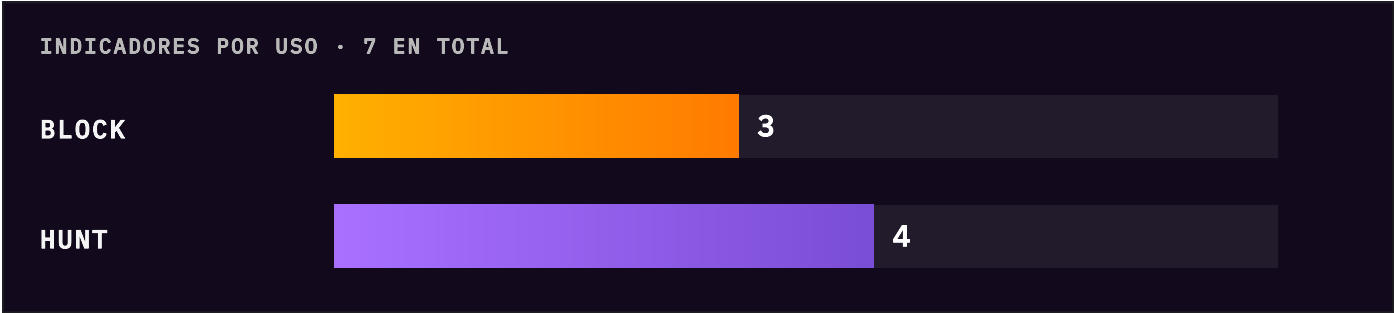
Bancos y fintech. El riesgo se materializa en la tarjeta cargada en un formulario de "depósito" y en las transferencias que siguen a la llamada de un "ejecutivo de inversiones". En ambos casos el primer indicio llega al banco antes que a cualquier lista de bloqueo.

Plataformas publicitarias. El caso muestra el límite de verificar solo la identidad del pagador cuando el destino puede cambiar o no coincidir con el dominio mostrado.

▲ 10 • INDICADORES

▲ Indicadores de compromiso (IOCs)

Siete dominios, todos **defangeados** ([.]): **no los visites**. Para importarlos, reemplazá [.] por . .
 `first_seen` es la fecha de mi primera observación (hora de Argentina), no la de creación del dominio.



INDICADOR	USO	VISTO	NOTA
<code>lunarbutton[.]site</code>	BLOCK	2026-10-01	Falsa nota con diseño de La Nación y chat de inversión con marca Mercado Libre (mínimo ARS 200.000, 450 %, "fianza"). Se llegó desde un anuncio de Google que mostraba otro dominio.
<code>epicharvest[.]info</code>	BLOCK	2026-09-30	Chatbot falso de "gestor personal" de Mercado Libre ("verificado por YPF"), formulario +54. Bloquear solo el FQDN. Vínculo con los demás indicadores: no establecido.
<code>app.balanztrading[.]com</code>	BLOCK	2026-09-30	Formulario de "depósito" con marca Balanz que pide tarjeta completa, titular, vencimiento y CVC. No es Balanz . Bloquear solo el FQDN; el dominio padre no se publica como indicador.
<code>descubre.upmegaconnectnotification[.]click</code>	HUNT	2026-09-30	Destino de un anuncio de Google con identidad del anunciante verificada. Contenido no documentado. Solo búsqueda en registros.
<code>upmegaconnectnotification[.]click</code>	HUNT	2026-09-30	Dominio padre del anterior. Solo búsqueda; no bloquear (baja especificidad pública).
<code>falcon-press[.]com</code>	HUNT	2026-10-01	Paso de un recorrido de "CFD de Mercado Pago" desde anuncios nativos ("un ejecutivo de inversiones lo llamará"). Evaluado como captación para call center. Solo búsqueda. No se afirma quién es el titular del dominio.
<code>lpa.voltfalcon-press[.]com</code>	HUNT	2026-10-01	Paso final del mismo recorrido, con identificador de sub-afiliado (no publicado). Solo búsqueda. No se afirma quién es el titular del dominio.

- **BLOCK** destinos con contenido fraudulento observado. Se pueden bloquear por FQDN.
- **HUNT** buscar en registros de DNS y proxy; no bloquear sin análisis propio.

▲ Mapeo a MITRE ATT&CK

ATT&CK se usa solo donde representa bien lo observado.

TÉCNICA	QUÉ SE OBSERVÓ
T1583.008 · Acquire Infrastructure: Malvertising	Anuncios pagos que llevan a destinos de falsa inversión
T1656 · Impersonation	Uso de las marcas Mercado Libre, Balanz, La Nación, YPF y bancos
T1056.003 · Input Capture: Web Portal Capture	Formulario de tarjeta con CVC (captura de datos no confirmada)

Como complemento, el [MITRE Fight Fraud Framework \(F3\)](#) es más adecuado que ATT&CK Enterprise para describir fraude financiero contra consumidores.

▲ Qué hacer, según el rol

USUARIOS

- Antes de dejar datos, conviene mirar la dirección real de la página, no la del anuncio.
- Conviene desconfiar de cualquier rendimiento garantizado y de cualquier "fianza" para liberar ganancias.
- Ningún broker legítimo te pide el código de seguridad de la tarjeta en un formulario propio para "depositar".
- "Identidad verificada" habla de quién paga el anuncio, no de la oferta.
- Si un anuncio parece engañoso, reportalo desde el propio anuncio.

BANCOS, FINTECH Y MARCAS

Bancos y fintech

Tratar como señal de riesgo las primeras transferencias o pagos con tarjeta hacia "brokers" de CFD o plataformas de inversión desconocidas, sobre todo de clientes sin historial de inversión. Avisar en la comunicación con clientes que nadie legítimo pide el CVC para "depositar" ni una "fianza".

Prevención de fraude

Buscar los indicadores en registros de proxy y DNS y cruzar esos accesos con operaciones posteriores. Vigilar las palabras del guion en reclamos: "fianza", "gestor personal", "verificado por YPF", "un ejecutivo lo llamará".

Marcas suplantadas

Monitorear el uso de su nombre en anuncios pagos con las herramientas públicas de transparencia publicitaria y publicar canales oficiales claros sobre qué nunca piden.

PLATAFORMAS Y COMUNIDAD

Plataformas publicitarias

Revisar el destino final y no solo el dominio mostrado, y tratar la discrepancia entre ambos como señal. Comunicar al usuario que la verificación cubre al pagador, no a la oferta.

SOC y CTI

Bloquear los BLOCK, buscar sin bloquear los HUNT. Analizar los destinos con un perfil parecido al de la víctima (teléfono, conexión local, llegada desde un anuncio): desde otro contexto se puede ver una página distinta.

CERT y CSIRT

Recibir los indicadores y, si corresponde, coordinar con las marcas y con los registradores de los dominios marcados para bloqueo.

▲ 13 • MÉTODO Y LIMITACIONES

▲ Cómo se hizo y hasta dónde llega

MÉTODO

- **Observación pasiva, como usuario.** Anuncios mostrados en un teléfono durante dos días de uso normal (30/9 y 1/10/2026, hora de Argentina), en el navegador, en Gmail Promociones y en redes de anuncios nativos.
- **Fuente del pagador.** La información pública de "Mi centro de anuncios" de Google para cada anuncio: pagador declarado, ubicación y estado de verificación.

- **Destinos.** Solo las páginas que se abrieron al tocar el anuncio, documentadas con capturas conservadas con su hash criptográfico.
- **Lenguaje de certeza.** Cada afirmación se marca como observada, evaluada (con nivel de confianza) o no establecida.

LIMITACIONES

- Es una muestra chica: un teléfono, dos días. **No mide prevalencia** ni alcance.
- Desde el lado del usuario no se puede distinguir una redirección de un cloaking, ni saber qué ve otro visitante o el revisor de la plataforma.
- No hay captura del contenido del destino genérico, y no quedó registrado qué anuncio llevó al formulario con marca Balanz.
- No se establecieron relaciones técnicas entre destinos; las coincidencias de plantilla son evaluaciones de confianza moderada.
- No se sabe quién opera los destinos, si alguno comparte dueño con otro ni cuántas personas dejaron sus datos.
- Los destinos pueden rotar o cambiar de contenido después de la observación.

▲ 14 • CONCLUSIÓN

▲ La puerta de entrada, no la infraestructura

Estas estafas no se parecen por su infraestructura sino por su puerta de entrada. Cada vertical por separado es conocida: la falsa nota, el chatbot de inversión, el broker que pide la tarjeta. Lo que cambia la lectura es verlas juntas, en los mismos días, llegando por anuncios pagos y verificados, con pagadores en al menos seis países (Reino Unido, Chipre, Países Bajos, Ucrania, Australia y Brasil) y la misma lista de marcas argentinas como señuelo.

La amenaza no es una banda sino un mercado: anunciantes que compran tráfico, plantillas que se reutilizan y destinos que convierten la atención en un teléfono, un depósito o una tarjeta. Bloquear dominios sirve, pero llega después. **No uní lo que la evidencia no une.**

▲ 15 • DIVULGACIÓN COORDINADA

▲ Divulgación coordinada

Antes de publicar, se notificaron los hallazgos a equipos de respuesta a incidentes de la región y a las marcas suplantadas.

▲ Cómo citar

La Terra, Ezequiel Jorge (2026). *CASHCLOAK LATAM: anuncios verificados y destinos de fraude de inversión y de tarjeta dirigidos a usuarios argentinos* (CTI-LATAM-2026-001, edición pública v2). Cyber Threat Intelligence LATAM. <https://cyberthreatintelligence.lat/informe/cashcloak-latam/>

```
@techreport{laterra2026cashcloak,  
  author      = {La Terra, Ezequiel Jorge},  
  title       = {{CASHCLOAK LATAM}: anuncios verificados y destinos de fraude  
                de inversión y de tarjeta dirigidos a usuarios argentinos},  
  institution = {Cyber Threat Intelligence LATAM},  
  number      = {CTI-LATAM-2026-001},  
  year        = {2026},  
  note        = {Edición pública v2, TLP:CLEAR},  
  url         = {https://cyberthreatintelligence.lat/informe/cashcloak-latam/},  
}
```

LICENCIA

Textos y datos bajo [Creative Commons Atribución 4.0 Internacional \(CC BY 4.0\)](#). Pueden reutilizarse y adaptarse, también con fines comerciales, citando la autoría.

AVISO

Esta publicación describe observaciones hechas como usuario y evaluaciones analíticas señaladas como tales. No atribuye responsabilidad a personas ni a empresas. Los anunciantes declarados se mencionan solo por su país y no se presumen responsables de los destinos. Las marcas y plataformas nombradas son víctimas de suplantación o proveedores de un servicio, no partes. Las correcciones se publican en el [registro de correcciones](#) con su fecha.