Así cayó GoogleXcoder, el hacker de los 'kits de estafa' que revelan cómo funciona el nuevo cibercrimen en España

La Guardia Civil detiene al joven de 25 años que alquilaba todo lo necesario para lanzar estafas de phishing por 300 euros y ofrecía “soporte técnico” a bandas criminales

— Frena la sensación de urgencia: así hackean tu mente los ciberestafadores y los trucos para evitarlo

Momento de la operación de la UCO contra GoogleXcoder

Carlos del Castillo

SEGUIR AL AUTOR/A

24 de octubre de 2025 -22:30 h **Actualizado el 26/10/2025 -10:47 h** 20

para usted. ¿Le ha surgido algún problema a la hora de utilizar nuestras herramientas? Disponemos de un servicio técnico para ayudarle. Y no se preocupe si lo que necesita es asesoramiento para “robarle todo a las abuelas”: tenemos un canal específico para ello.

Más información

Cae el hacker que diseñó una IA para estafar: su propio ego fue la pista clave

Parece ficción, pero es exactamente la lista de servicios de la última red de ciberdelincuentes detenidos en España. Al mando estaba un desarrollador conocido como GoogleXcoder, un ciudadano brasileño de 25 años que se convirtió en el posibilitador, sospecha la Guardia Civil, de muchas de las campañas de ***phishing*** que se han lanzado a nivel nacional desde 2023. Campañas que “han derivado en una cantidad importante de denuncias de personas afectadas, millones de euros sustraídos y el origen de una incipiente alarma social”, destacan los investigadores.

El *phishing*, como se conoce a los ataques de suplantación de identidad de empresas e instituciones públicas para engañar a las víctimas y quedarse con sus contraseñas o datos bancarios, se ha convertido en una de las ciberestafas más comunes. Son rápidas, relativamente sencillas y gracias a organizaciones como la de GoogleXcoder, muy accesibles para todo tipo de bandas.

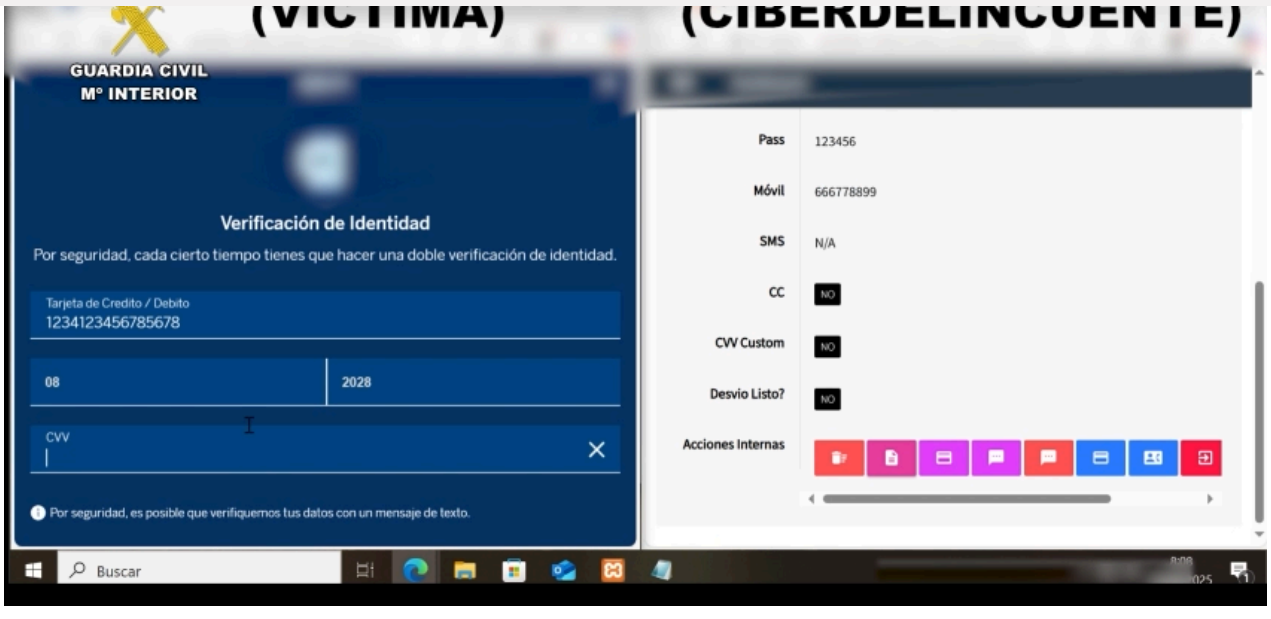
> Se puede definir como una empresa que se dedicaba a dar servicios criminales, en forma de kits para estafar"
>
> **Alberto Rodao** — jefe del Departamento Contra el Cibercrimen de la Unidad Central Operativa (UCO) de la Guardia Civil

“Es la representación perfecta del crimen como servicio”, explica a elDiario.es Alberto Rodao, jefe del Departamento Contra el Cibercrimen de la Unidad Central Operativa (UCO) de la Guardia Civil. “Se puede definir como una empresa que se dedicaba a dar servicios criminales, en forma de kits para estafar”.

Un *modus operandi* que refleja cómo ha evolucionado el crimen en España y aleja la imagen del solitario encapuchado frente a un ordenador. Los nuevos grupos utilizan tácticas profesionales para el ciberdelito, dejando atrás las campañas de *phishing* descuidadas y llenas de faltas de ortografía.

Crimen empaquetado

Los kits de estafa en los que se especializó esta organización eran, en la práctica, paquetes con todo lo necesario para llevar a cabo un ciberataque de *phishing*. Incluían los programas capaces de clonar los portales oficiales de cualquier organismo, diseñados para el robo de datos y contraseñas, así como herramientas para el envío masivo de mensajes (SMS y correos electrónicos). El objetivo era que cualquiera, aun con mínimos conocimientos técnicos, pudiera llevar a cabo estas estafas.



Su método para ponerlo a disposición de sus clientes también copiaba estrategias profesionales. “Él te hacía un paquete personalizado según lo que necesitaras. Era un experto en *phishing*, pero también hacía otros tipos de malware. Te ofrecía todo lo que un criminal podía necesitar para una campaña de *phishing* y lo cobraba como si fuera una licencia de software, por días. Tres días podían valer entre 200 y 300 euros”, revela Rodao.

En su cara más visible, estos programas incluían réplicas muy cuidadas de páginas oficiales (formularios, logos, textos) y un panel web desde el que los clientes de GoogleXcoder podían generar enlaces falsos, personalizar mensajes y seguir en tiempo real las credenciales y datos que iban llegando. No obstante, también incluían una parte oculta, ya que los datos que sus herramientas recogían también se desviaban hacia bases de datos bajo control del desarrollador.

“No era su negocio principal”, detalla el mando de la UCO, pero le eran de utilidad para mantener su anonimato. Gracias a los datos robados, utilizaba la identidad de las víctimas para contratar sus propias líneas de teléfono o tarjetas bancarias para disfrazar sus movimientos. También se desplazaba frecuentemente junto a su familia por distintas ubicaciones de España con el fin de “evitar su localización”.

Una operación de arriba a abajo

GoogleXcoder ofrecía sus servicios en Telegram, “el gran mercado del cibercrimen en los últimos años”, recuerda Rodao. La app ofrece anonimato y **escasa colaboración con las autoridades**, mientras que los canales donde la organización ofrecía sus herramientas de ciberataque eran de acceso privado. Sin embargo, con una cartera de clientes creciente, sus actividades empezaron a llamar la atención.

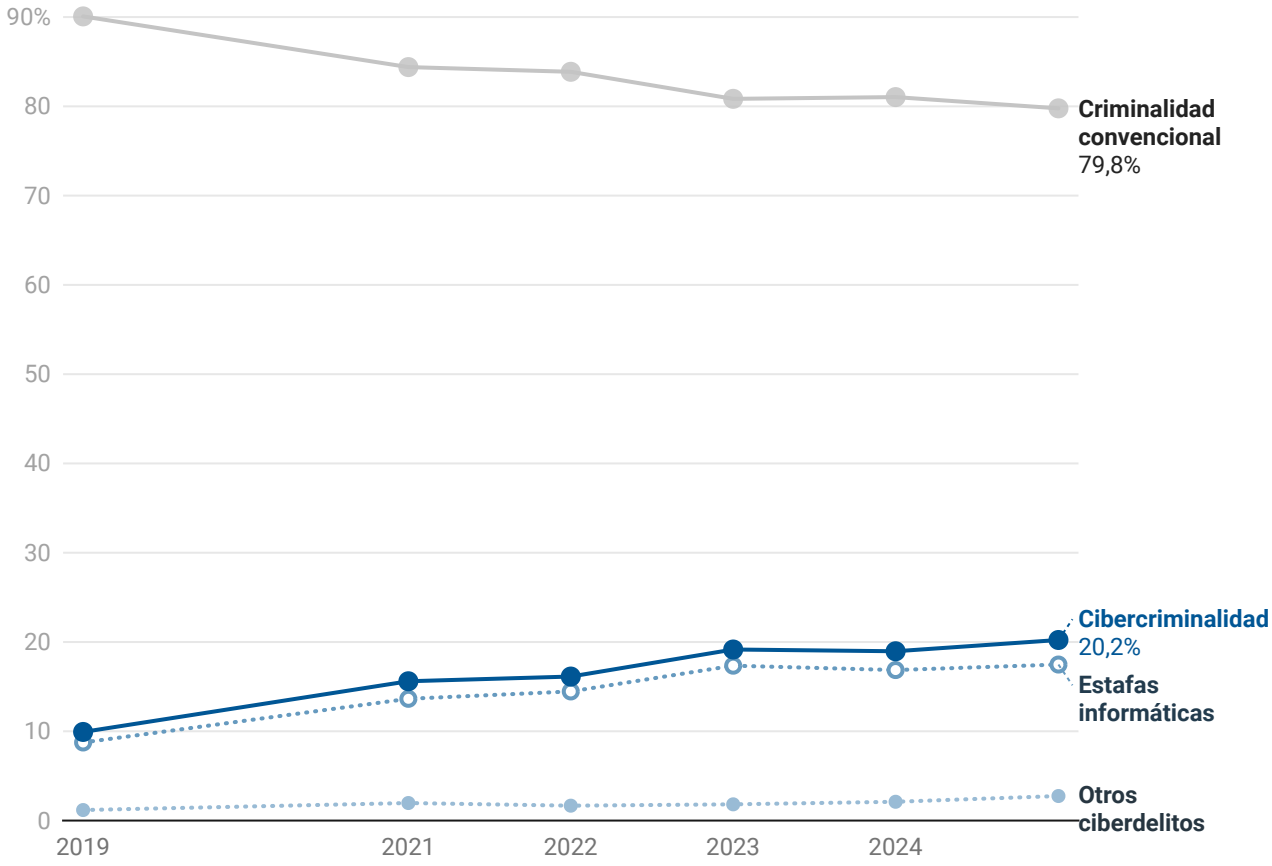
Momento de la operación

La UCO obtuvo “noticias de que el nick de esta persona estaba anunciando estos servicios” a través de varias fuentes. La repetición de “GoogleXcoder” en las declaraciones de los investigados llevó a los agentes a modificar el flujo tradicional de sus pesquisas. “Lo habitual es empezar por las víctimas”, aclara Rodao. Normalmente, una denuncia particular inicia el seguimiento del dinero, un rastro que permite “subir en la escala criminal” desde los escalones más bajos —las 'mulas' que reciben las transferencias— hasta los ejecutores.

En este caso, la UCO actuó “de arriba a abajo”. En lugar de perseguir las cientos de estafas individuales que emanaban de sus herramientas, decidieron ir directamente a por la fuente del problema. El objetivo era neutralizar al “cerebro”, al “desarrollador del malware” que proveía a todos los demás grupos. “Nos costó llegar hasta él y averiguar la persona que se escondía detrás del nick”.

Tras la detención, los agentes emprendieron el camino inverso. “Hemos intentado llegar a las víctimas”, confirma Rodao. El análisis de los dispositivos del detenido reveló la magnitud de su actividad. “En muchos casos, cuando contactamos con las personas cuyos datos habían sido robados, ni siquiera eran conscientes de ello”.

Porcentaje de **cibercriminalidad** (estafas informáticas + otro tipo de ciberdelitos) y de **criminalidad convencional** sobre el total de cada periodo. Datos de 2025 solo hasta el 2º trimestre



Fuente: Balances trimestrales de criminalidad del Ministerio del Interior • Creado con Datawrapper

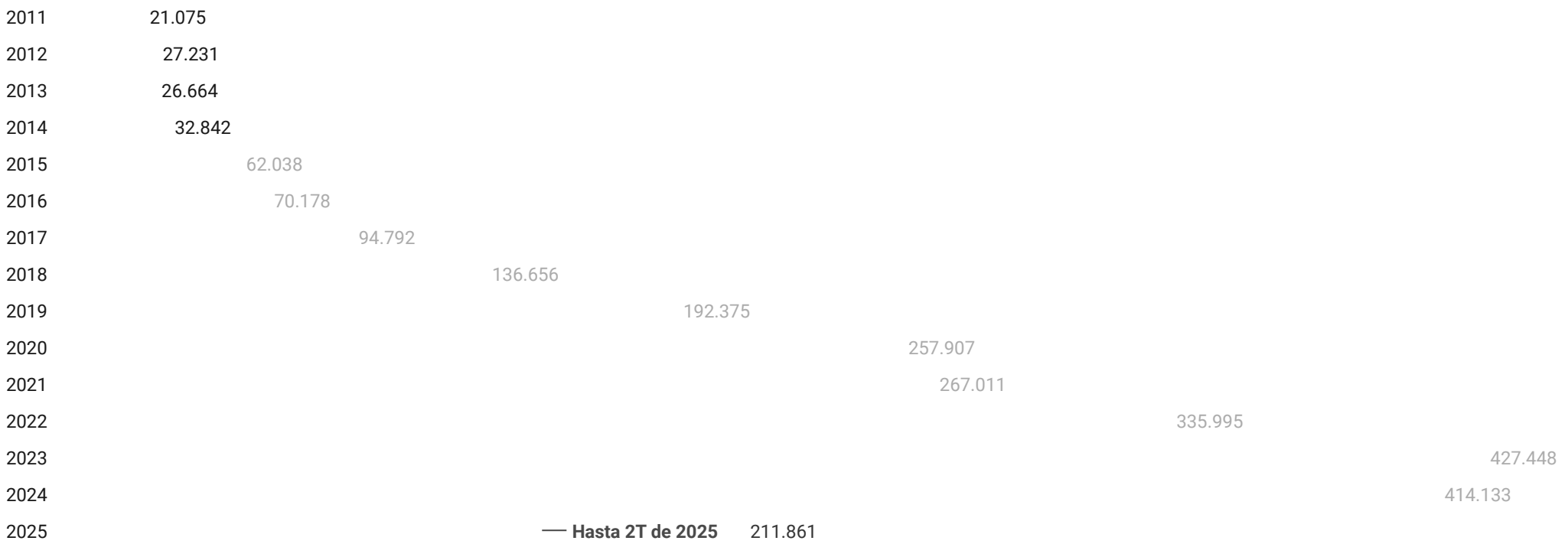
La operación, coordinada por el Juzgado de Instrucción número 1 de San Vicente de la Barquera (Cantabria), culminó con la realización de seis registros en domicilios en Valladolid, Zaragoza, Barcelona, Palma de Mallorca, San Fernando y La Línea de la Concepción. Actualmente, la investigación continúa abierta y no se descartan nuevas actuaciones.

“Robarle todo a las abuelas”

El nombre de uno de los canales de mensajería de GoogleXcoder resume la filosofía de la organización: “Robarle todo a las abuelas”. Es “llamativo”, admite Rodao. Es la definición de una estrategia de negocio. Las personas mayores son “víctimas principales” por una razón puramente mercantil: su brecha digital las convierte en el objetivo perfecto. “Están mucho menos familiarizadas” con el entorno digital y, por tanto, “son más fáciles de engañar”, explica el jefe del cibercrimen de la UCO.

Esta vulnerabilidad tiene un precio en el mercado negro. “Los paquetes de datos de personas mayores siempre están más cotizados”, revela el guardia civil.

Las estafas informáticas se han duplicado desde 2019. Aunque en el año 2024 fue el primero de la última década en que esta tipología de delito se redujo respecto al ejercicio anterior, este 2025 ha vuelto a aumentar. En suma, los ciberdelitos ya representan más de un 20% de toda la criminalidad que se da en España.



Fuente: Balance Trimestral de Criminalidad 2024 del Ministerio del Interior • Creado con Datawrapper

"La gente que se dedica a esto no tiene ninguna piedad", sentencia Rodao. "No se cortan nada ni con las personas vulnerables, ni mayores, ni nada". El único objetivo es el beneficio, sin importar las consecuencias para la víctima: "Aquí es el dinero y me da igual quién seas, cómo seas o en qué situación estés. El objetivo es sacar siempre el máximo dinero".

Los especialistas recomiendan **mantener la cabeza fría ante cualquier comunicación sospechosa**. Los estafadores suelen aprovechar que las defensas de la víctima se relajan ante situaciones de urgencia. Ataques que cada vez cuentan con un mayor grado de perfección gracias a los datos personales robados. "Cuando tú sabes todo de una persona, en qué banco tiene contraseña, qué edad tiene, dónde, etc., te permite ejecutar un ataque muy elaborado", recuerda el mando de la UCO.

Más información

Frena la sensación de urgencia: así hackean tu mente los ciberestafadores y los trucos para evitarlo

En caso de sospecha de haber clicado en un enlace fraudulento o de haber introducido datos bancarios en páginas que podrían estar operadas por ciberestafadores, la recomendación de las fuerzas de seguridad es comunicar lo sucedido de inmediato al banco y denunciar los hechos a la Policía. El Instituto Nacional de Ciberseguridad dispone del número gratuito 017 y del teléfono de WhatsApp 900 116 117 para resolver dudas de seguridad. Atiende a ciudadanos, empresas y profesionales y es confidencial.

ETIQUETAS

Tecnología / Ciberdelincuencia / Ciberseguridad / Hackers / Guardia Civil / UCO - Unidad Central Operativa / Estafas

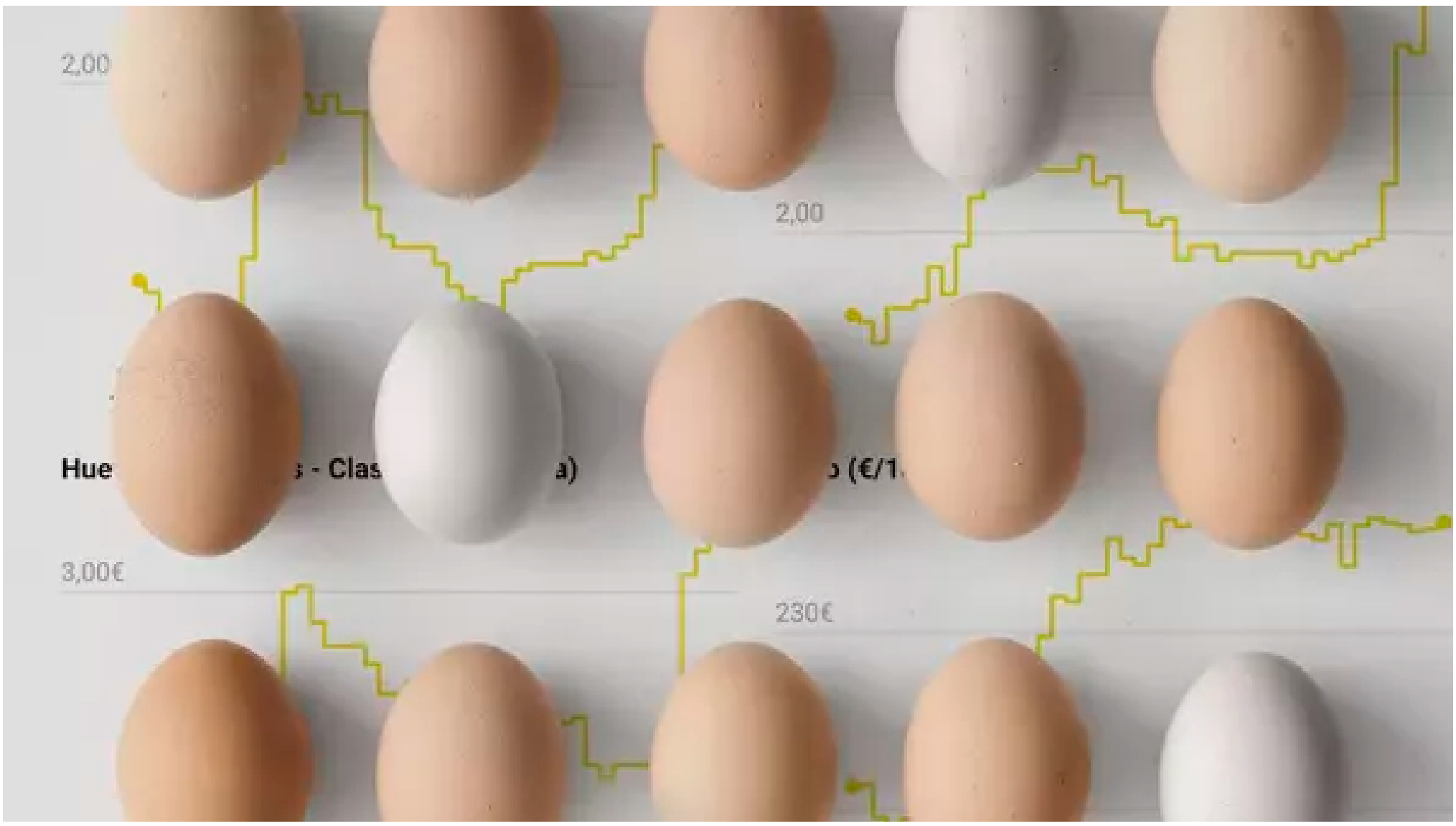
HE VISTO UN ERROR

Únete a la conversación 20

Últimas noticias

Rebeldes por Naturaleza, la sección de Amigas de la Tierra en Carne Cruda

---



La gripe aviar dispara el precio del huevo y los productores temen la especulación: “No va a haber problemas de oferta”

Cristina G. Bolinches

[El Teatro Bretón programa este fin de semana un espectáculo de danza y una obra teatral del Centro Dramático Nacional]
Rioja2

[La ULL convoca 66 nuevas plazas docentes para 2026]
Tenerife Ahora

La relación de Xavi Pascual y el Barça Basket: la continua rememoración de su mejor etapa en el baloncesto

Andrea Blez

Euskadi refuerza el control de las viviendas de uso turístico con ocho nuevos inspectores

Euskadi Brands

[Barakaldo aprueba los pliegos del futuro Plan Integral de Rehabilitación del corredor del Kadagua]
Euskadi Brands

[La Asamblea Nacional francesa da el primer paso para suspender la reforma de las pensiones, la medida estrella de Macron]
EFE / elDiario.es

TEMAS DE INTERÉS Crucigramas Baliza V16 Dormir con sujetador Setas Semana Santa 2026 Libro familia online Programación Televisión Test actualidad Palabra secreta Expertos Noticias TV Noticias Canarias Noticias de