Llamadas internacionales que timbran y cuelgan: operadoras peruanas son parte de flujo fraudulento

Las llamadas “wangiri”, una modalidad de fraude que consiste en timbrar y colgar desde números internacionales, puede generar grandes beneficios económicos para las mafias detrás de este sistema. OjoPúblico reconstruyó el flujo por el que pasan estas llamadas e identificó que los operadores nacionales y un grupo de empresas de origen estadounidense son parte de la cadena que permite que estas lleguen a los usuarios peruanos.

Jackeline Cárdenas

@Jackeline_CI

Jackeline@ojo-publico.com

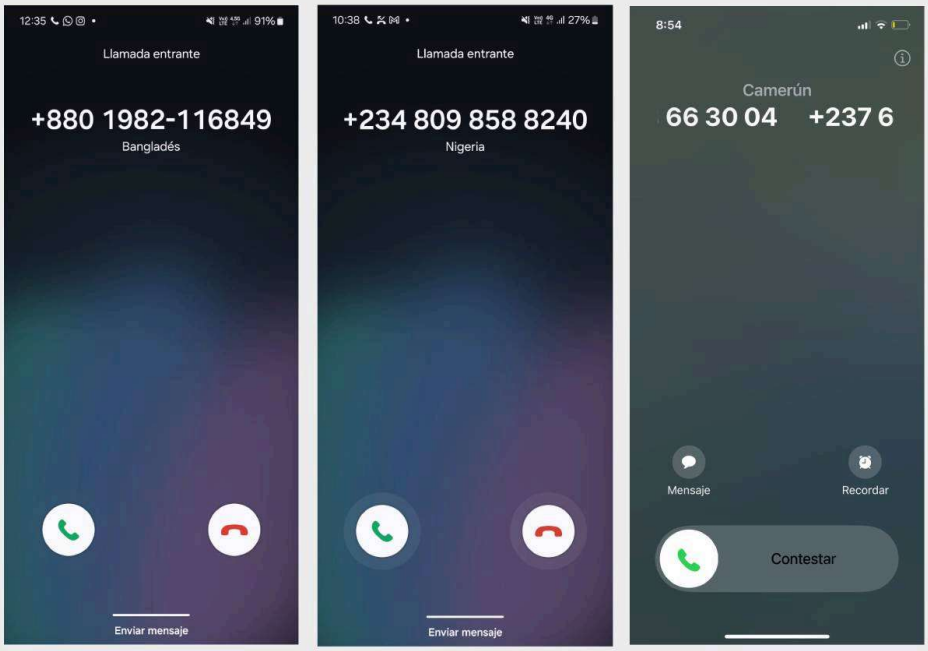
28 Junio, 2026

Suena el celular y en la pantalla aparece un número con más de nueve dígitos y códigos de países como Nigeria o Bangladés. Lo ignoras o cuelgas, y el momento queda en el olvido. En Perú, sin embargo, no todos los usuarios corren la misma suerte.

Este tipo de llamadas internacionales dirigidas a usuarios peruanos tiene un objetivo claro: que la persona devuelva la llamada para generar cargos elevados por conexión o por minuto. En muchos casos, se trata de números con tarifas especiales o premium, similares a los usados en servicios como concursos, lecturas de tarot y contenido de adultos.

El mecanismo de estafa no es nuevo. Se le conoce como llamadas “wangiri”, que viene del término japonés para referirse a “una timbrada y cortar”. La principal recomendación de los especialistas es no devolver este tipo de llamadas para no caer en la estafa. Pero ¿cómo funciona y quiénes se benefician?

OjoPúblico reconstruyó el recorrido de las llamadas wangiri e identificó la cadena que permite que lleguen a usuarios peruanos, desde números internacionales hasta operadores y plataformas de comunicación utilizadas para cursarlas.



TIMBRADAS. Usuarios reportan una ola de llamadas de números extranjeros. Se trata de una modalidad de estafa conocida como llamadas "wangiri": timbrar y cortar.

Foto: Jackeline Cárdenas I.

Estas llamadas ingresan a las redes de operadoras nacionales como Movistar (Integratel Perú), Entel, Bitel (Viettel Perú) y Claro (América Móvil Perú), que reciben la comunicación y la dirigen hacia los usuarios. Por este enlace, cobran una tasa por la interconexión.

Entre enero y diciembre de 2025, estas compañías tuvieron ingresos promedio de S/70 millones por el concepto "enlaces y cargos de interconexión", según **datos** de Osiptel. Este medio les consultó a todas las empresas qué porcentaje de este monto representa las llamadas de larga distancia que reciben. Hasta el cierre de esta investigación, no respondieron.

De acuerdo a fuentes consultadas, la mayor parte de este monto refleja lo que cobran por conectar todas las llamadas que gestionan, y en menor medida, incluyen las llamadas de origen internacional con fines fraudulentos.

Para que este sistema funcione son clave también las plataformas de comunicaciones en línea, que permiten adquirir números virtuales de distintos países y cursar llamadas internacionales. Entre ellas figuran empresas como Twilio, Telnyx, Plivo y Vonage Communications APIs, de Estados Unidos; Sinch de Suecia, y Bird, de Países Bajos.

“Existe un rango de números llamados premium y son los estafadores quienes los compran con la excusa de operar como call centers para llamar desde esos números”, explicó el ingeniero Herminio Paucar Curasma, docente de Programación de la Universidad Nacional Mayor de San Marcos.

El último **informe** de TrueCaller pone en contexto lo extendido del problema con las llamadas no deseadas: en 2025, dos de cada 10 llamadas en Perú, fueron identificadas como spam, lo que incluye no solo a las agresivas estrategias de venta de distintas empresas sino también a modalidades de estafa o fraude.

El cobro inicia apenas se devuelve la llamada, explica Hobber Siccha Ayvar, especialista en Tecnologías de la información y docente de la Pontificia Universidad Católica del Perú.

“Suficiente que pasen 5 o 10 segundos tratando de comunicarte y no te respondan para que, en ese tiempo, ya se genere un cargo relacionado con el consumo de llamada. Por eso es mejor no responder a este tipo de números”, indica.

El esquema

El flujo de las llamadas “wangiri” inicia con una red criminal internacional o un estafador ubicado en cualquier parte del mundo. Para operar, estos grupos pueden recurrir a números IPRN (International Premium Rate Numbers) o Números Internacionales de Tarifa Premium, que permiten generar ingresos a partir de llamadas entrantes.

En este mercado también operan plataformas de comunicaciones en la nube, como Twilio, Telnyx, Plivo, Vonage Communications APIs, Sinch y Bird, que ofrecen servicios de telefonía virtual y conexión internacional utilizados para distintos fines legítimos, aunque también pueden ser aprovechados por redes fraudulentas.

Luego, mediante granjas de bots o softwares que simulan llamadas de voz —conocidos como inyectores de tráfico SIP—, los estafadores ejecutan cientos de llamadas simultáneas. Ese tráfico pasa por operadores internacionales, que finalmente se conectan con las empresas de telecomunicaciones peruanas: Claro, Movistar, Entel y Bitel.

En la etapa final, los operadores nacionales reciben las llamadas internacionales y la dirigen hacia los usuarios en Perú. Estas llamadas pueden durar apenas unos segundos: el tiempo suficiente para una sola timbrada y cortar, lo que no genera ningún cobro para los estafadores.

Sin embargo, cuando el usuario ve la llamada perdida y, por impulso o curiosidad, la devuelve, el operador peruano la procesa como una llamada de larga distancia internacional y genera un registro de tasación para realizar el cobro.

Debido a reglas de la Unión Internacional de Telecomunicaciones (UIT) y a contratos bilaterales, el operador peruano cobra la tarifa al usuario y transfiere el dinero en dólares, previa comisión, al operador internacional. Según especialistas consultados, en estos esquemas una parte del monto puede terminar en manos de quienes originan la estafa.

CADENA. El flujo de las llamadas “wangiri” inicia con una red criminal internacional o un estafador ubicado en cualquier parte del mundo.

Elaboración: Jackeline Cárdenas I.

Precisamente, para la UIT, uno de los **motivos** por los que hasta ahora no se ha podido eliminar este tipo de fraude es “el gran volumen de llamadas entrantes que genera y, por lo tanto, importantes ingresos” para los operadores que participan del esquema.

Para Ximena Cuzcano Chavez, analista en seguridad y resiliencia digital de la organización Derechos Digitales, los estafadores encontraron una forma de sacarle la vuelta a una herramienta que fue creada para servicios como llamadas concurso o de tarot, que suelen tener tarifas elevadas. Ellos se aprovechan de países “sin techo regulatorio para inflar las tarifas”, dijo a **OjoPúblico**.

Hasta hace un par de años era más común que los estafadores usaran granjas de bots para realizar llamadas automatizadas. Sin embargo, ahora el proceso puede ser más sencillo: ya no necesitan esa infraestructura, pues también pueden adquirir softwares que generen este tipo de llamadas. “Es un sistema que se implementó para los call centers, pero ahora se está usando de manera fraudulenta”, explicó Cuzcano Chavez.

Este medio se comunicó con las operadoras nacionales Claro, Movistar, Entel y Bitel, y las compañías que venden los números de tarifas especiales Twilio, Plivo, Vonage Communications APIs, Sinch y Bird, para solicitar sus descargos, pero ninguna respondió hasta el cierre de este informe. Solo Telnyx dijo que toman “muy en serio” la prevención del uso fraudulento de sus servicios y que tienen “políticas estrictas para mitigar estos riesgos”.

La regulación ausente

En febrero último, el Gobierno peruano **publicó** un decreto legislativo que establece medidas “para enfrentar las estafas y fraudes cometidos mediante llamadas telefónicas y mensajes de texto con números falsos o enmascarados”.

Con la norma, los operadores de telecomunicaciones estarán obligados a implementar mecanismos para identificar, validar y controlar el uso adecuado de la numeración. Aunque el reglamento debió estar listo en mayo, la propuesta se publicó en abril y hasta la fecha no se ha aprobado.

En la exposición de motivos de este documento se **señala** que una de las medidas para alertar al usuario de llamadas fraudulentas como las “wangiri” es agregar el prefijo 00 antes de la numeración. De esta forma, el usuario podría identificarlas.

Para Luis Reyes Vivanco, experto en telecomunicaciones y docente de la Universidad Nacional de Ingeniería (UNI), esta propuesta no solucionará el problema. La medida es “muy general” y no ataca la raíz del problema, indicó. Por el contrario, sostuvo que la Asociación del Sistema Global para Comunicaciones Móviles —o GSMA por sus siglas en inglés— y la Unión Internacional de Telecomunicaciones (UIT) ya han brindado recomendaciones más eficientes.

Lo principal es la detección de las llamadas mediante herramientas de inteligencia artificial y machine learning: los algoritmos pueden identificar rafagas masivas de llamadas cortas dirigidas a miles de usuarios y perfilar a los operadores.

RUTA. El fraude de las llamadas "wangiri" funciona a través de la infraestructura tecnológica de grandes empresas, entre ellas los operadores peruanos.

Foto: Jackeline Cárdenas I.

También se pueden implementar firewalls de señalización, que permiten monitorear el tráfico de voz y bloquear las llamadas de suplantación de identidad. Además, se pueden rechazar llamadas con prefijos de países con alto historial de fraude.

El ingeniero Herminio Paucar Curasma advirtió que las llamadas “wangiri” también pueden ejecutarse por llamadas de internet —sistema conocido como voz sobre protocolo de internet (VoIP)— y que esta es solo una de las decenas de formas que existen en la actualidad para vulnerar la seguridad de los usuarios.

La tecnología permite enmascarar número fraudulentos con números validados de grandes empresas y realizar llamadas desde allí para solicitar datos como claves o contraseñas, con el fin de robar dinero no solo al dueño del número, sino también a sus contactos.

Por ello, para Paucar Curasme la comunidad académica tiene un rol importante en contrarrestar este avance. Señaló que próximamente la universidad creará la carrera de ciberseguridad, que abarcará el estudio de todo tipo de fraudes en el sistema de comunicaciones. “Cualquier persona tiene un celular; por lo tanto, puede ser susceptible a uno de estos fraudes”, finalizó.

Este medio consultó al Ministerio de Transportes y Comunicaciones (MTC) qué medidas ha implementado para combatir este tipo de fraudes, pero no respondió hasta el cierre de esta edición. Por su parte, el Organismo Supervisor de Inversión Privada en Telecomunicaciones (Osiptel) indicó que la “modalidad de comunicación asociadas a tipos fraude no tienen vinculación” con sus competencias.

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) respondió que la investigación y sanción de esta práctica no le corresponde. Agregó que actualmente fiscaliza el cumplimiento de la Ley 32323, que prohíbe las llamadas spam, “cuyos resultados podrían dar lugar al inicio de procedimientos sancionadores”.

Relacionados

Wangiri, Claro, movistar, Entel, Bitel