



# Tendencias de Fraude y Seguridad 2026

Analizamos miles de millones de interacciones en nuestra plataforma para identificar las principales tendencias de fraude, las amenazas de seguridad y los riesgos emergentes para los que las empresas deben prepararse en 2026.

```
{  
  "phoneNumber": "+441134961234",  
  "maxAge": 15  
}
```







## Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

Hace veinte años, el fraude en la mensajería era relativamente simple: SIM boxes aisladas, campañas básicas de spam e intentos de phishing poco sofisticados. Los atacantes operaban a pequeña escala y las defensas podían mantenerse al día mediante actualizaciones manuales de reglas y revisiones periódicas. Hoy, ese panorama ha cambiado por completo. Las herramientas disponibles para los delincuentes han evolucionado más en los últimos cinco años que en los quince anteriores.

Hemos sido testigos en primera fila de esta transformación. Este año celebramos 20 años en los que Infobip ha contribuido a definir la forma en la que las empresas se comunican con sus clientes en todo el mundo. Durante este tiempo, hemos visto cómo el fraude y la seguridad pasaron de ser un desafío operativo de nicho a convertirse en una prioridad estratégica para toda la organización y, por ellos, nuestras soluciones han evolucionado al mismo ritmo.

Como líderes reconocidos en la prevención del fraude en la mensajería móvil, ofrecemos una perspectiva única basada en datos globales de comunicaciones, el análisis de patrones de fraude en constante evolución y nuestra experiencia práctica protegiendo las interacciones entre las empresas y sus clientes.

Este Informe de Fraude y Seguridad documenta un año marcado por fuertes contrastes: volúmenes récord de tráfico fraudulento bloqueado junto con tasas históricamente bajas de filtración de mensajes; una disminución del fraude relacionado con contraseñas de un solo uso (OTPs) a nivel mundial, mientras surgían nuevas regiones de alto riesgo; y una mayor adopción de mecanismos de autenticación empresarial, a medida que las organizaciones avanzan hacia estrategias de seguridad que van más allá del uso exclusivo de SMS.

Los datos revelan un entorno de amenazas cada vez más complejo, en el que el fraude impulsado por inteligencia artificial, las tácticas de phishing cada vez más sofisticadas y el abuso de los canales de comunicación continúan creciendo a escala. Al mismo tiempo, las empresas recurren cada vez más a soluciones de seguridad inteligentes y en tiempo real para proteger la confianza de sus clientes.

77%

de incremento de mensajes fraudulentos detectados en 2025 en nuestra plataforma

**La detección de fraude basada en patrones creció un 105 % en 2025.**

94%

de incremento en el bloqueo de mensajes de phishing en 2025

**El phishing representó el 49% de los mensajes bloqueados.**

38%

de reducción en el tráfico de AIT en 2025, detectado por Infobip Signals

**Europa y LATAM registraron el incremento más grande en actividad AIT sospechosa.**

71%

de crecimiento en detección del fraude potenciada por IA

**La detección del fraude mediante imágenes basada en IA se amplió a medida que aumentó la cobertura en 2025.**

27%

de incremento en el tráfico SMS bloqueado a nivel de la red del operador por Anam Protect SMS Firewall

**El tráfico bloqueado mensualmente del Q4 se mantuvo por encima del promedio mensual anual.**





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

# El nuevo campo de batalla del fraude

Cada año, los delincuentes invierten en nuevas herramientas, nuevas rutas y nuevas superficies de ataque. En 2025, enfocaron gran parte de sus esfuerzos en aumentar la escala de sus operaciones. Las implicaciones financieras son significativas. La Communications Fraud Control Association (CFCA) estima que las pérdidas globales por fraude en telecomunicaciones aumentaron de aproximadamente 39 mil millones de USD a 42 mil millones de USD en 2025.

El fraude digital es un problema crítico para las empresas que afecta directamente la confianza de los clientes, la reputación de la marca, los ingresos y la eficiencia operativa. Cuando un usuario no puede completar una transacción porque su OTP se retrasó o, peor aún, fue interceptado, no culpa al delincuente, culpa a la marca.

En 2025, observamos que la actividad de mensajería maliciosa se volvió más compleja. Los actores maliciosos están utilizando IA y automatización para optimizar sus ataques, identificar vulnerabilidades con mayor rapidez y adaptarse rápidamente a las medidas de bloqueo.

Además del aumento en el bloqueo de amenazas, la reducción del tráfico fraudulento también está impulsada por cambios en la actividad del fraude, incluida la creciente presencia del fraude a través de canales OTT.

Infobip procesa miles de millones de interacciones cada mes a través de SMS, voz, correo electrónico, WhatsApp, RCS y otros canales y productos de mensajería. Esta escala nos brinda tanto visibilidad como responsabilidad, ya que nos permite identificar patrones de fraude en nuestra plataforma que operadores individuales o empresas no podrían detectar. Nuestras capacidades de fraude y seguridad abarcan toda la superficie de amenazas de las comunicaciones digitales:



## Anam Protect

Firewall A2P de SMS y voz de nivel operador que protege a más de 120 operadores y a 1.200 millones de suscriptores a nivel mundial frente a rutas grises, fraude con SIM boxes, spam y tráfico no autorizado, al tiempo que convierte el tráfico bloqueado en ingresos monetizables. Combina monitoreo y bloqueo del tráfico SMS impulsado por IA con consultoría especializada en monetización por parte de expertos.



## Infobip Signals

Detección en tiempo real de OTPs y SMS pumping integrada en los flujos empresariales de entrega de mensajes, utilizando aprendizaje automático para identificar y bloquear tráfico artificial antes de que genere cargos.



## APIs de red

Inteligencia de fraude a nivel operador; detección de SIM Swap, verificación de números y KYC, proporcionando señales en tiempo real desde la red móvil que ninguna capa de aplicación puede replicar.



## Number Masking

Comunicación basada en la privacidad desde el diseño mediante el uso seguro de números telefónicos virtuales, permitiendo interacciones en tiempo real sin exponer los datos de contacto personales.



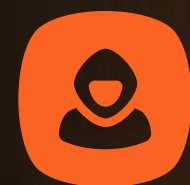
## Authenticate

Entrega multicanal de OTPs a través de SMS, voz, WhatsApp, RCS, Viber y otros canales, con selección inteligente de canales y conmutación automática para entregar cada autenticación mediante el canal disponible y el más adecuado, según la probabilidad de entrega, el costo y la disponibilidad regional.

## Lo que hallarás en este reporte

- Datos y tendencias provenientes de miles de millones de transacciones globales.
- Comparaciones interanuales entre diferentes tipos de fraude y regiones.
- Análisis específicos por industria y región sobre los riesgos de fraude y las estrategias de prevención.
- Ejemplos reales de cómo la IA y las plataformas inteligentes están mejorando la detección y prevención del fraude.





EL PANORAMA GLOBAL DEL FRAUDE Y EL SPAM EN 2026

# Tipos de spam y patrones para estar alerta



# Las interacciones bloqueadas aumentan y son cada vez más inteligentes

Si hay una conclusión en la que coinciden los datos de todas nuestras capas de detección del fraude, es que el entorno global del fraude y el spam en 2025 es más intenso que en 2024, y que 2024 ya había sido más intenso que en 2023. El volumen aumentó. La sofisticación se elevó. El alcance geográfico se está expandiendo.

Pero los datos también coinciden en otro aspecto: los volúmenes bloqueados están aumentando y algunos mercados muestran mejores resultados a medida que la infraestructura de detección ha madurado.



# 77% de crecimiento en la detección multicapa del fraude

Los datos de nuestra plataforma muestran que los volúmenes bloqueados crecieron un 77% entre 2024 y 2025, lo que refleja tanto un aumento en la actividad de amenazas como una expansión de las capacidades de detección. Sin embargo, el volumen por sí solo cuenta solo una parte de la historia. Tan importante como la cantidad de tráfico bloqueado es comprender qué se bloqueó y cómo fue identificado.

El fraude y el spam global en 2025 abarcan varias categorías de mensajes claramente diferenciadas, cada una asociada con un patrón de abuso distinto. El phishing sigue siendo la categoría de fraude más directa, ya que utiliza mensajes engañosos para manipular a los destinatarios y lograr que compartan credenciales, datos de pago u otra información sensible.

El tráfico relacionado con apuestas representa mensajes vinculados a actividades de juego no autorizadas o restringidas por políticas, mientras que el contenido regulatorio abarca mensajes bloqueados por incumplir normativas locales de comunicación o requisitos de cumplimiento. El contenido explícito incluye mensajes con material para adultos u otro tipo de contenido prohibido que no es adecuado para su distribución a través de canales legítimos de mensajería.

En conjunto, estas categorías demuestran que el abuso de la mensajería no se limita a una sola táctica. Algunas amenazas están diseñadas para robar dinero o datos, mientras que otras buscan evadir las reglas de las plataformas, los límites regulatorios o las restricciones de contenido.

Para abordar estos diferentes tipos de amenazas, múltiples capas de detección trabajan en conjunto, cada una analizando distintas señales sobre la forma en que se distribuye el tráfico malicioso:

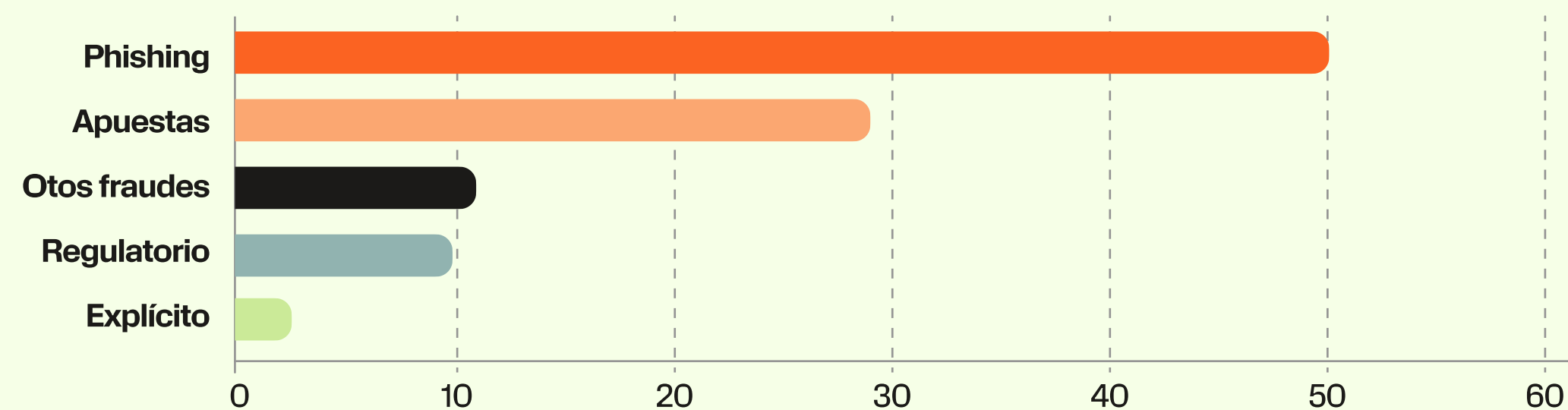
- **La detección basada en patrones** identifica el spam mediante firmas de contenido, coincidencia de palabras clave y análisis de patrones de tráfico.
- **La detección de URL** identifica mensajes que contienen enlaces maliciosos o fraudulentos mediante el análisis en tiempo real de las URLs incluidas, con el fin de detectar sitios de phishing, redirecciones maliciosas, portales de apuestas y otros destinos web perjudiciales.
- **La detección impulsada por IA** opera en dos capas: detección de texto, que identifica contenido malicioso que no coincide con patrones conocidos (nuevos tipos de fraude y lenguaje de campañas en evolución), y detección de imágenes, que analiza las imágenes incluidas en los mensajes para identificar contenido dañino oculto en ellas.

## Crecimiento de los métodos de detección en 2025

| Método de detección          | Crecimiento interanual |
|------------------------------|------------------------|
| Detección basada en patrones | 105%                   |
| Detección de URL             | 31%                    |
| Detección impulsada por IA   | 71%                    |

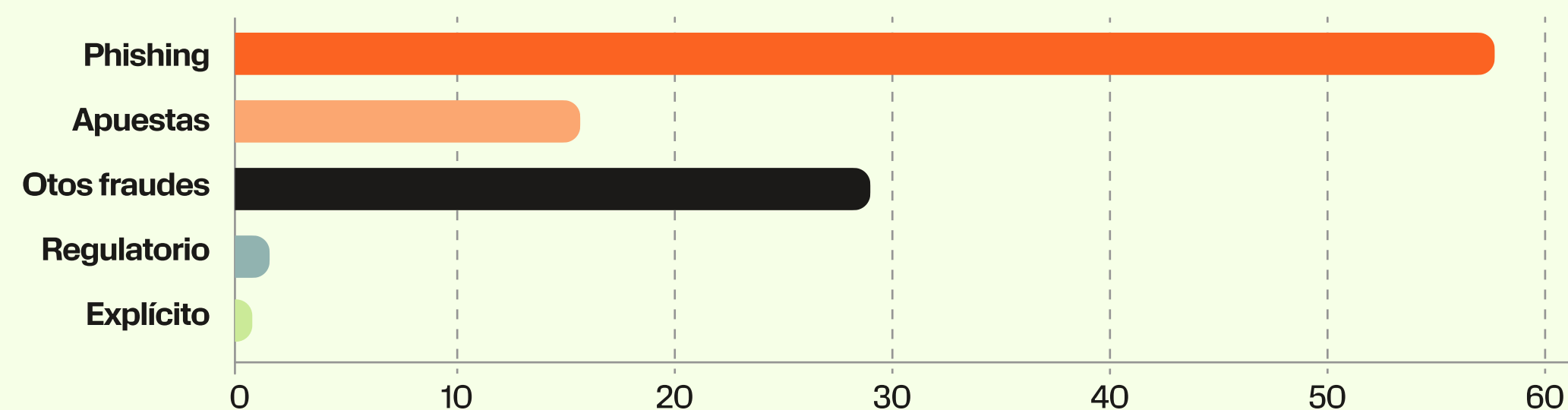
# Lo que cada capa de detección descubrió en 2025

## Mensajes bloqueados mediante patrones



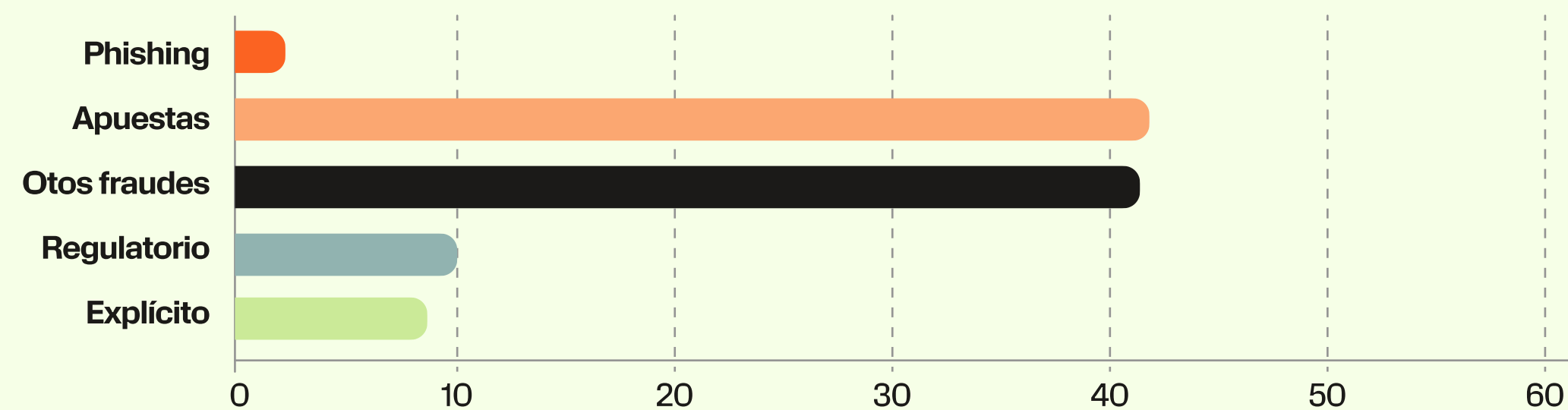
**La detección basada en patrones** sigue siendo la capa dominante, representando el 69% de todos los mensajes bloqueados en 2025. Su crecimiento del 105% superó la tasa de crecimiento general del 77%, lo que indica que las reglas basadas en patrones se ampliaron y se volvieron más efectivas para detectar una gama más amplia de amenazas, especialmente de phishing (que representa casi el 50% de lo que captura la detección basada en patrones).

## Mensajes bloqueados por detección de URL



**La detección de URL** tuvo un crecimiento más moderado del 31%. El phishing basado en URL sigue siendo significativo, representando el 57% de todos los mensajes detectados mediante URLs, mientras que las apuestas (15%) constituyen la mayor parte del resto.

## Mensajes bloqueados por detección vía IA



**La detección impulsada por IA** contiene la señal más relevante de cara al futuro dentro de nuestro conjunto de datos. Dentro de esta capa, la detección de texto creció un 59%. De forma más significativa, la detección de imágenes creció un 628% en un solo año.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

# Cuando el fraude se oculta en las imágenes

El crecimiento de la detección de imágenes impulsada por IA refleja una táctica de fraude en aumento: en lugar de incluir texto sospechoso directamente en los mensajes, los delincuentes ocultan contenido malicioso dentro de imágenes para evadir los filtros basados en texto.

A medida que esta táctica se vuelve más común, el análisis de imágenes basado en IA se está convirtiendo en una capa fundamental de la detección del fraude. El **crecimiento de 7x en los bloqueos detectados mediante imágenes** demuestra que esta técnica ya se está utilizando a gran escala.



# El phishing sigue siendo dominante

En 2024, el phishing representó el 45% de todo el contenido dañino bloqueado. En 2025, esta proporción aumentó al 49%; casi uno de cada dos mensajes bloqueados correspondió a un intento de phishing. Al mismo tiempo, el volumen del phishing creció un 94% interanual.

Esta no es una categoría que esté creciendo al mismo ritmo que el volumen general del spam. Es una categoría que se está acelerando por encima de este, impulsada por la industrialización de las campañas de robo de credenciales.

## Total de mensajes dañinos bloqueados

- Phishing - 49.0%**  
Robo de credenciales, toma de control de cuentas, suplantación de identidad y phishing de entrega.
- Apuestas - 26.4%**  
Promociones de apuestas no autorizadas.
- Otras Estafas - 16.0%**  
Fraude financiero, estafas de pago anticipado y estafas de soporte técnico.
- Regulatorio - 7.3%**  
Incumplimientos normativos y mensajes comerciales no solicitados.
- Contenido Explícito - 1.3%**  
Contenido para adultos y material inapropiado.





## ¿Por qué el phishing sigue ganando?

El phishing funciona porque explota el comportamiento humano más que las vulnerabilidades técnicas.

Un mensaje que parece provenir de un banco, una empresa de mensajería o una entidad gubernamental genera una sensación de urgencia, y esa urgencia suele hacer que las personas bajen la guardia.

Por ejemplo, a medida que los SMS se convirtieron en el principal canal para la autenticación de transacciones, también pasaron a ser el principal canal para que los ciberdelincuentes se hicieran pasar por las organizaciones que envían esos mensajes. El problema se agrava: cuanto más confían los consumidores en los SMS para recibir alertas de seguridad legítimas, más creíbles parecen las alertas de seguridad fraudulentas enviadas por SMS. En el panorama general del phishing, los mensajes relacionados con entregas —es decir, aquellos que suplantán a empresas de mensajería y servicios postales— han disminuido un 30 % interanual.

Esta es una señal positiva: la concientización de los consumidores sobre las estafas relacionadas con entregas está aumentando, lo que hace que esta táctica específica sea menos efectiva. Sin embargo, el phishing en términos generales aún no ha alcanzado ese mismo nivel de resistencia por parte de los usuarios





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

# Temporadas de compras que impulsan picos de fraude

Diciembre de 2025 fue el mes con mayor volumen de contenido dañino bloqueado, con un nivel de +2x superior al promedio mensual registrado a principios de 2025 y un 31% por encima de diciembre de 2024. Noviembre, coincidiendo con eventos como Singles Day, Black Friday y Cyber Monday, también mostró un aumento evidente. El patrón estacional es aún más claro al compararlo con el promedio anual total: en 2024, Q4 estuvo un 108% por encima del promedio mensual de 2024, mientras que en 2025 se mantuvo un 28% por encima del promedio mensual de ese año.

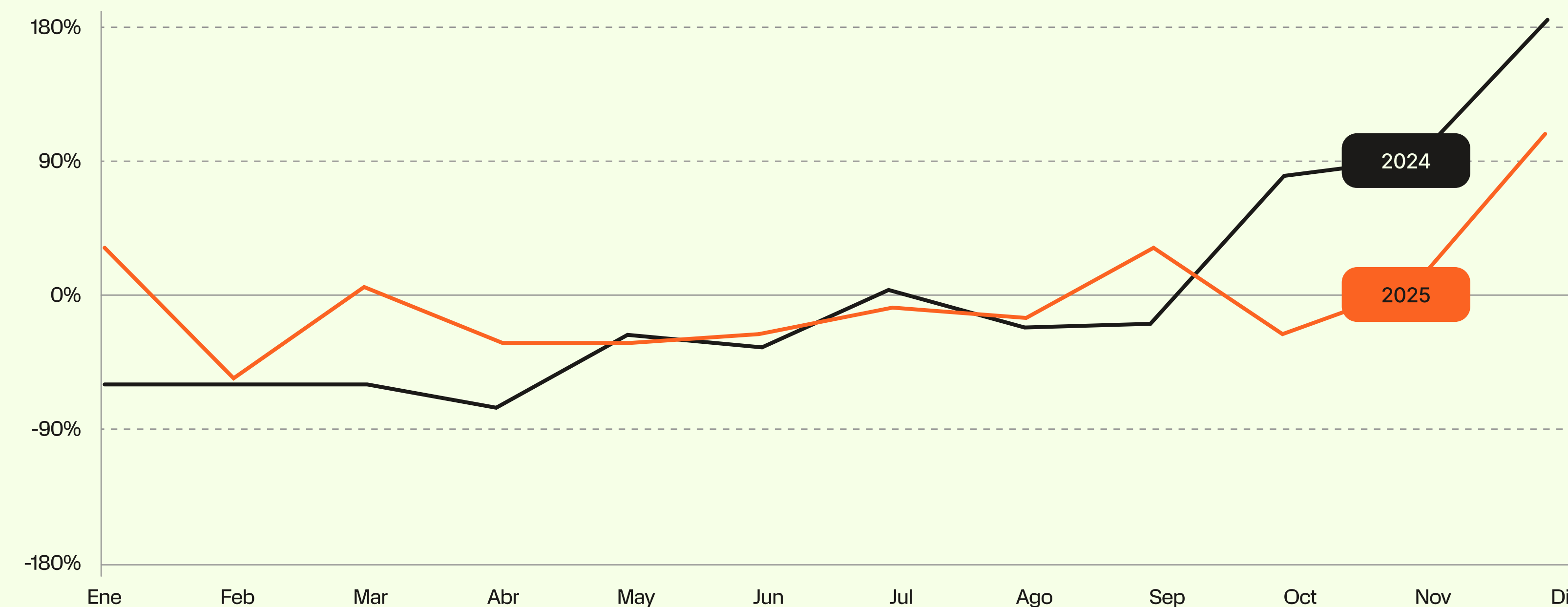
El patrón estacional es generalizado, aunque no idéntico en todas las categorías. En 2024, el Q4 estuvo por encima del promedio mensual anual en todas las categorías principales, lideradas por el phishing, incluido el phishing de entrega **(+120%)**, el contenido explícito **(+171%)**, el contenido regulatorio **(+119%)** y las apuestas **(+117%)**. En 2025, el pico estacional siguió siendo visible, pero el patrón estuvo menos concentrado: phishing **(+35%)**, contenido regulatorio **(+26%)** y apuestas **(+12%)** continuaron por encima de sus promedios mensuales anuales, mientras que el contenido explícito mostró un comportamiento más estable.

En 2025, la presión del fraude parece haber estado distribuida de manera más uniforme a lo largo del año, con volúmenes mensuales más cercanos al promedio anual y una menor variación que en 2024, cuando la estacionalidad del Q4 fue mucho más marcada.

Esto es importante desde el punto de vista operativo, ya que los períodos de mayor actividad comercial hacen que el tráfico malicioso sea más difícil de distinguir del tráfico legítimo mediante reglas estáticas. La clasificación en tiempo real es la única defensa capaz de escalar al ritmo de las amenazas durante los períodos de alta demanda.

## Se detectaron más mensajes dañinos durante los períodos de mayor actividad

Contenido dañino bloqueado mensualmente en comparación con el promedio mensual de cada año





Panorama regional de mensajes bloqueados

| Región | Crecimiento Interanual |
|--------|------------------------|
| LATAM  | 56%                    |
| NAM    | 223%                   |
| EUROPA | 119%                   |
| INDIA  | 28%                    |
| ÁFRICA | 118%                   |

LATAM

Crecimiento sostenido

En 2025, LATAM registró un aumento del 56% en los mensajes bloqueados.

El perfil de amenazas de la región está definido principalmente por el phishing, que representa el 50% de los mensajes bloqueados a nivel regional.

NAM

La escalada regional más significativa

Entre las regiones cubiertas por los datos de nuestra plataforma, Norteamérica fue la región principal con mayor crecimiento en 2025, con un aumento del 223% en los mensajes bloqueados.

El perfil de amenazas de Norteamérica difiere del de LATAM: el phishing lidera con un 55%, y las infracciones regulatorias (11%) también tienen una mayor relevancia en Norteamérica que en otras regiones. En la categoría de apuestas, aunque representa una proporción menor del total regional, los mensajes bloqueados crecieron 12 veces interanualmente.

Europa

Crecimiento generalizado con una expansión de las apuestas como factor clave

Los mensajes bloqueados en Europa crecieron un 119% en 2025. El perfil de amenazas de Europa muestra una dimensión distintiva relacionada con las apuestas: el contenido de apuestas representa el 33% de todos los mensajes bloqueados en la región.

El aumento del 352% en los mensajes de apuestas bloqueados en Europa indica una expansión estructural de las operaciones de spam relacionado con apuestas hacia los mercados europeos, en línea con el crecimiento de las actividades de apuestas en línea reguladas y no reguladas en el continente.

África

Fuerte crecimiento con patrones de fraude en evolución

El volumen de mensajes bloqueados en África creció un 118% en 2025. En 2024, el phishing representaba una proporción mucho mayor del tráfico bloqueado, pero para 2025 había disminuido y representaba el 15% del tráfico bloqueado, mientras que las apuestas aumentaron hasta superar el 11% de los mensajes bloqueados.

Este cambio refleja una evolución en la combinación de amenazas de fraude en África, donde la presión se está desplazando de un patrón dominante hacia múltiples categorías de fraude.





**SMS FIREWALL**

# Protegiendo redes y usuarios

```
{  
  "name": "2fa application name",  
  "enabled": true,  
  "configuration": {  
    "pinAttempts": 5,  
    "allowMultiplePinVerifications": true,  
    "pinTimeToLive": "10m",  
    "verifyPinLimit": "2/4s",  
    "sendPinPerApplicationLimit":  
    "5000/12h",  
    "sendPinPerPhoneNumberLimit": "2/1d"  
  }  
}
```

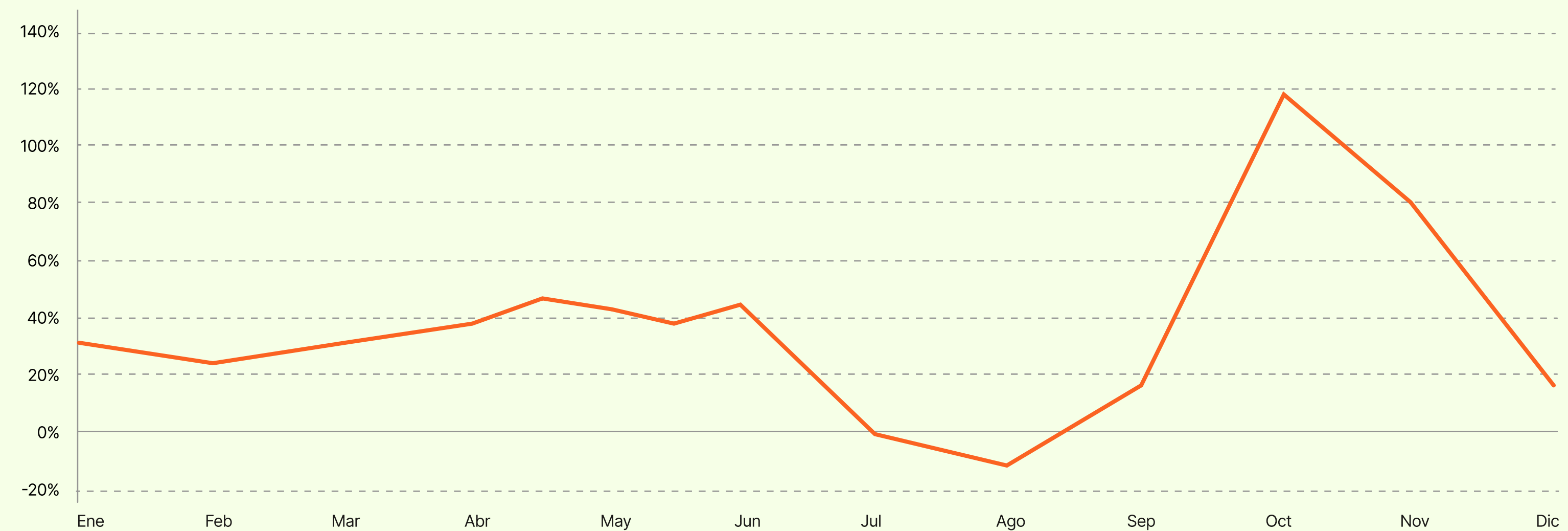


# El firewall impulsado por IA bloqueó un 27% más de amenazas SMS en 2025

La solución de firewall Anam Protect está diseñada exclusivamente para operadores de redes móviles (MNO). A diferencia de los productos de seguridad empresarial que operan en la capa de aplicaciones, Anam Protect funciona dentro de la propia infraestructura de red del operador, brindando a las empresas de telecomunicaciones control directo sobre el tráfico SMS A2P que circula por sus sistemas.

Nuestra solución de firewall SMS bloqueó un mayor volumen de mensajes SMS fraudulentos en 2025 que en 2024; un incremento interanual del 27%. Este aumento refleja el crecimiento sostenido del tráfico fraudulento y no autorizado en las redes de operadores móviles, incluyendo SMS mediante rutas grises que evaden los canales oficiales de facturación, tráfico OTP inflado artificialmente y campañas de spam y phishing que aumentan en volumen y sofisticación.

## Volumen mensual de SMS bloqueados – Variación interanual en 2025







Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

# La realidad operativa detrás del dominio de SMS

La magnitud de este desafío está estrechamente relacionada con la escala del propio SMS. El Reporte de Tendencias de Mensajería de Infobip muestra que el SMS representó el 62% de todo el tráfico de la plataforma en 2025, convirtiéndose por amplio margen en el canal de comunicación dominante, incluso mientras las empresas adoptan cada vez más múltiples canales digitales.

Su posición predominante se explica por una realidad operativa sencilla: el SMS sigue siendo el canal preferido cuando la confiabilidad y la velocidad de entrega son factores críticos. Notificaciones, contraseñas de un solo uso (OTP), alertas de transacciones, recordatorios de citas o cualquier situación en la que una pequeña cantidad de información sensible al tiempo deba llegar al usuario con certeza dependen del SMS.

## EL EFECTO DE LA TEMPORADA DE COMPRAS Q4 como el período de mayor fraude

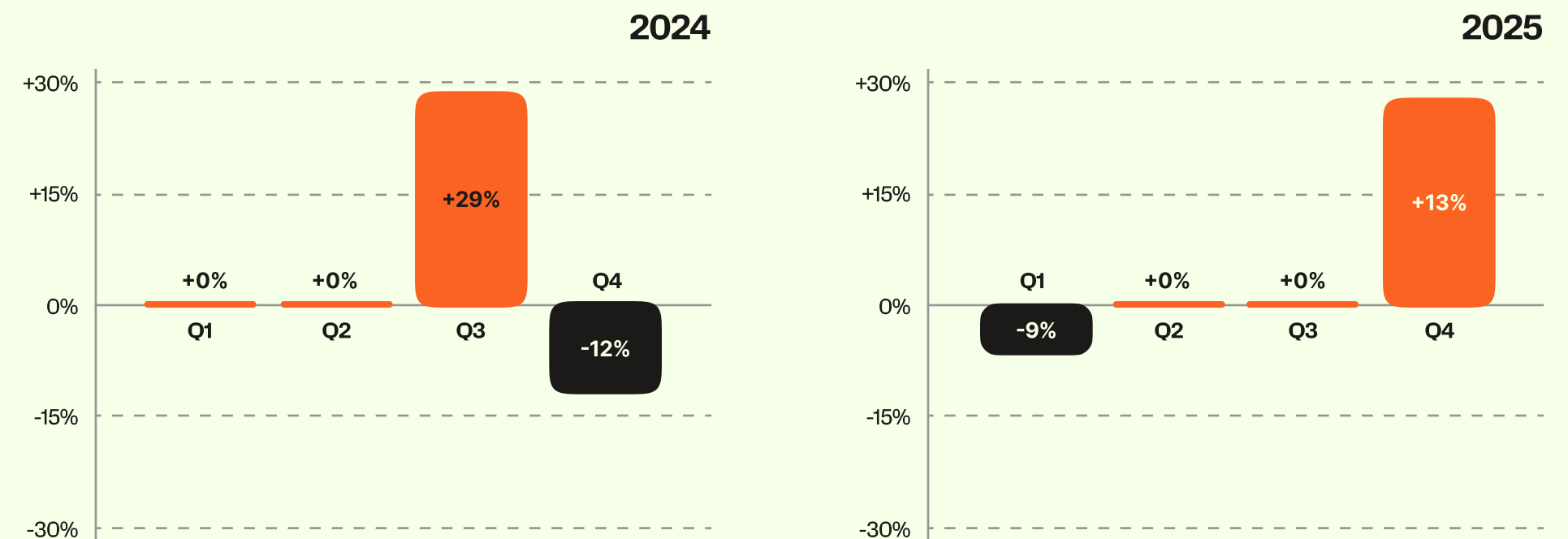
Los datos del Q4 de 2025 revelan un patrón constante y comercialmente relevante: los meses con mayores volúmenes de transacciones de consumidores a nivel mundial también generan la mayor presión de fraude sobre las redes de operadores móviles.

Esto no es una coincidencia. La actividad fraudulenta tiende a aumentar donde se concentra la actividad económica, y el período de octubre a diciembre reúne más comercio digital, más autenticaciones basadas en SMS y más comunicaciones con consumidores que cualquier otro trimestre.

Los datos del firewall de 2025 muestran que el tráfico bloqueado promedio mensual del Q4 estuvo un 13% por encima del promedio mensual anual, mientras que el Q1 estuvo un 9% por debajo. Octubre y noviembre fueron, en conjunto, el período con mayor volumen del año, y noviembre de 2025 estableció el récord mensual de tráfico bloqueado, coincidiendo con Singles Day, Black Friday y Cyber Monday.

Este patrón sugiere que la presión del fraude en 2025 estuvo cada vez más sincronizada con el calendario global de compras. El aumento hacia finales de año no se distribuyó de manera uniforme durante el trimestre; fue más

## Tráfico bloqueado en Q4 vs. promedio anual



intenso durante los principales períodos promocionales, mientras que diciembre registró niveles inferiores a los meses de mayor actividad. Esto podría indicar que la exposición al fraude está impulsada menos por la temporada festiva en general y más por eventos comerciales concentrados y de alta intensidad que generan picos en el tráfico de autenticación y en las comunicaciones con clientes.

Este representa un cambio importante respecto a 2024, cuando el patrón era diferente: Q4 estuvo un 12% por debajo del promedio mensual anual, y el período más fuerte del año fue el Q3, que se ubicó un 29% por encima del promedio anual. Para 2025, este patrón se revirtió, con la mayor presión trasladándose al Q4. En términos interanuales, esto podría indicar que la actividad fraudulenta en 2025 estuvo más estrechamente alineada con los ciclos comerciales estacionales que en 2024, reforzando la relación entre el aumento de la actividad minorista y el incremento del abuso en las redes.

## Crecimiento regional interanual del tráfico bloqueado por el firewall SMS en 2025

86% APAC

14% África

África y APAC continuaron registrando una fuerte actividad de firewall SMS en 2025. El tráfico bloqueado en África aumentó un 14% interanual, reflejando una demanda A2P sostenida en servicios de alto volumen como alertas bancarias, OTP de fintech y notificaciones logísticas. APAC creció aún más rápido, con un aumento del 86% en el tráfico bloqueado durante 2025, demostrando cómo el incremento de los volúmenes de tráfico y la complejidad de las rutas están aumentando la necesidad de filtrado en tiempo real y control del tráfico.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

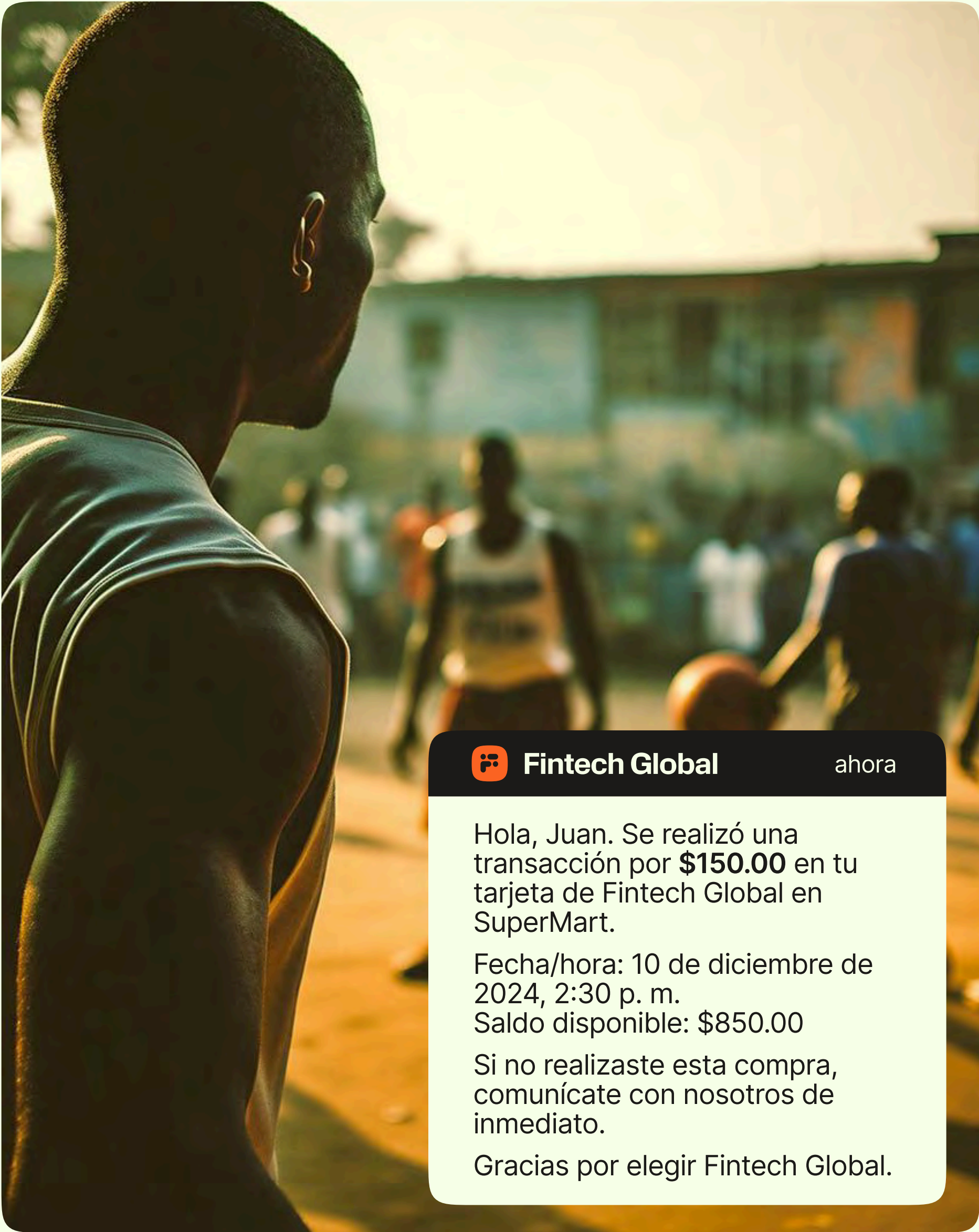
Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad



Fintech Global

ahora

Hola, Juan. Se realizó una transacción por **\$150.00** en tu tarjeta de Fintech Global en SuperMart.

Fecha/hora: 10 de diciembre de 2024, 2:30 p. m.  
Saldo disponible: \$850.00

Si no realizaste esta compra, comunícate con nosotros de inmediato.

Gracias por elegir Fintech Global.

## EL FIREWALL DEJA PASAR MENOS AMENAZAS

# 99,9% del tráfico fraudulento bloqueado en 2025

El tráfico bloqueado mide la presión externa, mientras que el tráfico filtrado mide lo que logra superar las defensas. En 2025, el tráfico filtrado disminuyó un 42% interanual, lo que demuestra que una cantidad significativamente menor de tráfico no autorizado logró evadir el firewall y llegar a las capas de facturación o entrega.

En todas las principales regiones, el firewall bloqueó el 99,9% del tráfico, reforzando la magnitud de la protección ya implementada.

Las empresas que adoptaron detección en tiempo real redujeron significativamente su exposición al fraude frente a aquellas que dependían de conciliaciones mensuales de facturación. A medida que las tendencias de fraude también se ven influenciadas por cambios más amplios en la industria, incluido el creciente uso de mensajería alternativa y canales OTT, la distribución del fraude continúa evolucionando entre los distintos canales de comunicación.

MENA registró la mayor mejora regional: **el tráfico filtrado disminuyó un 55%.**

### EL FIREWALL REDUJO EL TRÁFICO FILTRADO EN TODAS LAS REGIONES

| Región | Cambio Interanual |
|--------|-------------------|
| ÁFRICA | -23%              |
| APAC   | -17%              |
| LATAM  | -38%              |
| MENA   | -55%              |





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

# El fraude con SIM boxes sigue los picos estacionales del tráfico

## El fraude con SIM boxes continuó siendo una de las amenazas más relevantes asociadas a las rutas grises.

El fraude con SIM boxes es uno de los diversos esquemas de rutas grises utilizados para evadir acuerdos oficiales de interconexión y evitar una facturación adecuada. A menudo implica grupos de tarjetas SIM registradas localmente, pero el patrón más amplio consiste en enrutar tráfico no autorizado fuera de la ruta comercial prevista. Esto puede afectar tanto al tráfico de telecomunicaciones local como internacional y generar exposición al fraude en múltiples industrias.

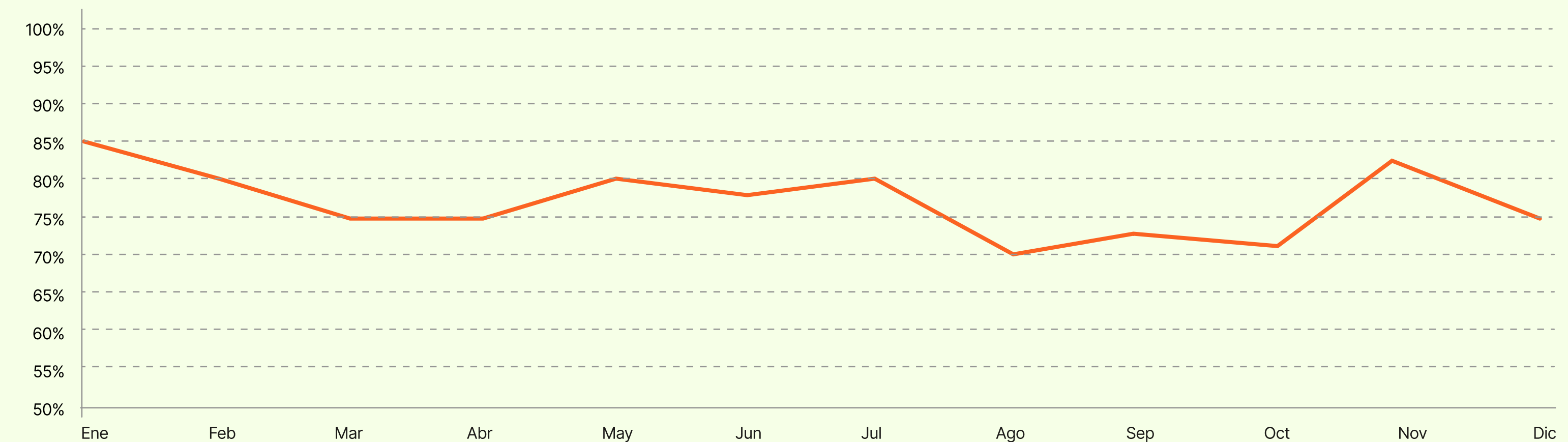
En 2025, la actividad de bloqueo siguió patrones estacionales claros, aumentando durante períodos de mayor tráfico legítimo y reduciéndose cuando el volumen de tráfico era menor. Este patrón fue especialmente visible en la actividad de SIM boxes, que continuó siendo una de las amenazas de rutas grises más importantes a pesar de la mejora interanual. Aunque el tráfico filtrado relacionado con SIM boxes disminuyó un 27% en comparación con 2024, siguió representando una parte importante de las filtraciones por rutas grises, confirmando que el fraude con SIM boxes continúa siendo una de las formas más relevantes y escalables de enrutamiento no autorizado.

El patrón mensual sugiere que la estacionalidad tuvo un mayor impacto en la presión del fraude que en los resultados del control. Los períodos de mayor tráfico legítimo probablemente generaron más oportunidades para el abuso mediante SIM boxes, pero los controles de bloqueo mejorados parecen haber reducido la medida en que esos aumentos de tráfico se tradujeron en filtraciones exitosas. En este sentido, 2025 muestra tanto una exposición continua a campañas estacionales de SIM boxes como una mayor capacidad para contenerlas.

A finales de 2025, más de tres cuartas partes de las decisiones de bloqueo se automatizaban mediante el motor de detección de SIM Box de Anam Protect, que utiliza IA y aprendizaje automático para clasificar y bloquear automáticamente el tráfico sospechoso, ayudando a los operadores a responder con mayor rapidez a campañas que cambian según la estacionalidad del tráfico. Este aumento en la automatización probablemente contribuyó a una aplicación más sólida de las medidas de control durante todo el año, favoreciendo tanto mayores volúmenes de bloqueo como menores niveles generales de filtración.

### TENDENCIAS MENSUALES DE DETECCIÓN REFLEJARON LA DINÁMICA ESTACIONAL DEL TRÁFICO

Tasa de detección de SIM boxes – Tendencia mensual 2025



En enero de 2025 se observó un aumento del 86% en la detección de SIM boxes, probablemente impulsado por el arrastre de campañas de fraude de finales de diciembre que continuaron durante el inicio del nuevo año. La disminución de agosto (68%) probablemente refleja una menor actividad estacional en el tráfico legítimo, reduciendo temporalmente el contraste disponible para la detección. El repunte de noviembre (82%) coincide con los picos de comercio electrónico previos a las fiestas, un período que suele ser aprovechado por los operadores de SIM boxes, quienes incrementan su actividad cuando los altos volúmenes de tráfico legítimo les proporcionan mayor cobertura.



Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

## La filtración por rutas grises internacionales SS7 disminuyó en 2025

Mientras que el fraude con SIM boxes mostró la estacionalidad más clara vinculada al tráfico, otros tipos de rutas grises siguieron un patrón diferente. El enrutamiento gris internacional basado en SS7 continuó siendo un vector de fraude más pequeño, pero aún relevante, que generalmente aprovecha vulnerabilidades en la capa de señalización para desviar tráfico fuera de la ruta comercial prevista. En 2025, el tráfico internacional SS7 filtrado disminuyó un 22% interanual, lo que indica un mayor control sobre el abuso relacionado con la señalización. Su comportamiento mensual mostró una menor estacionalidad que el fraude con SIM boxes, con picos más pequeños y menos consistentes, lo que sugiere que la actividad de rutas grises internacionales basadas en SS7 podría estar más impulsada por explotaciones específicas que por aumentos generales de tráfico.

## La filtración por rutas grises SMPP disminuyó considerablemente

El enrutamiento gris mediante SMPP también siguió siendo un área importante de atención, ya que puede permitir el envío no autorizado de mensajes a través de canales técnicos no oficiales o que no cumplen con las normativas, evadiendo el modelo de monetización previsto. Este tipo de ruta gris es especialmente relevante en la mensajería empresarial, donde el control de rutas y la gobernanza de los envíos son fundamentales. En 2025, el tráfico SMPP filtrado disminuyó un 60% en comparación con 2024, marcando una de las mejoras más significativas entre las categorías de rutas grises. Esto sugiere que controles más estrictos, mejores mecanismos de filtrado y una mayor supervisión de socios redujeron considerablemente este tipo de filtración.

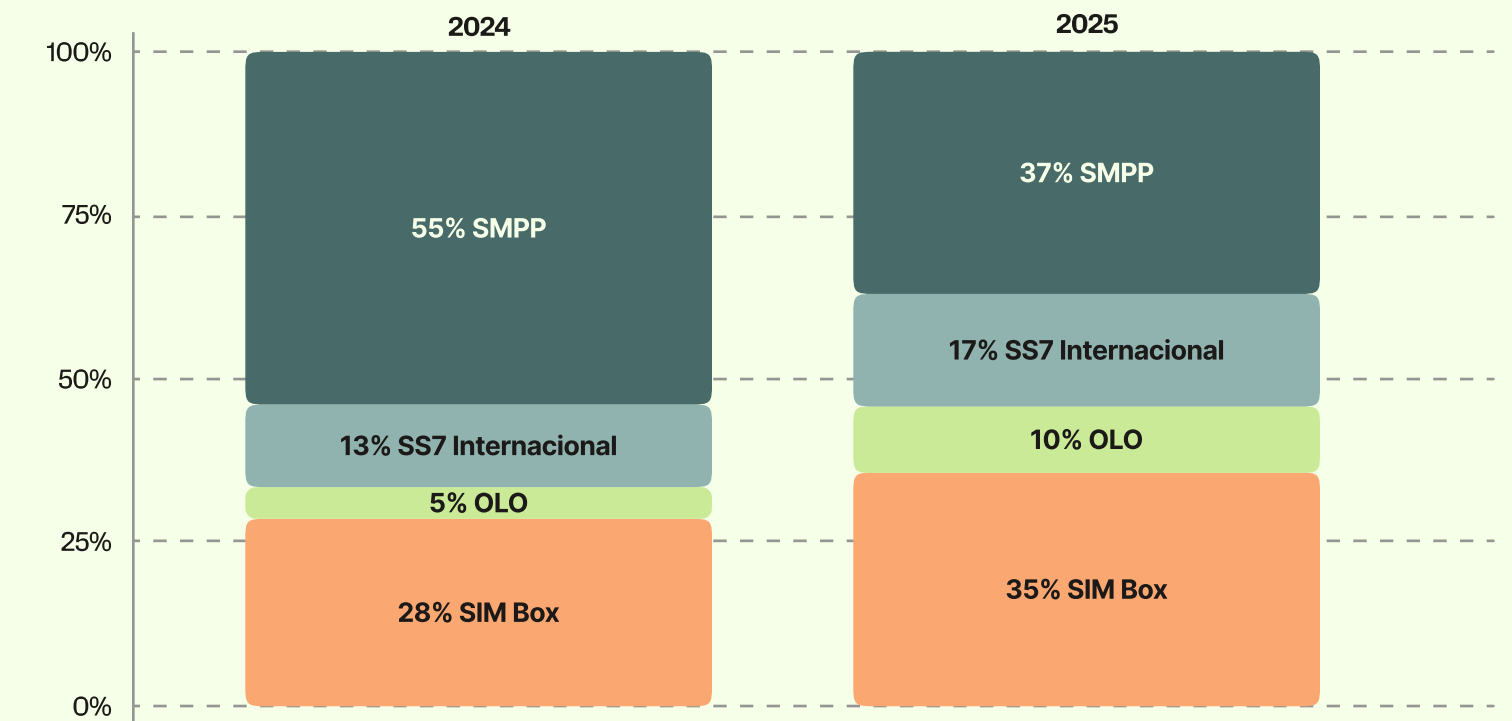
## La filtración OLO aumentó a medida que la presión se desplazó entre canales

En contraste, la filtración relacionada con OLO aumentó pese a las mejoras observadas en otros ámbitos. Las rutas grises OLO suelen reflejar tráfico desviado a través de acuerdos no autorizados con operadores externos o rutas de interconexión que no cumplen con las normas. En 2025, el tráfico OLO filtrado aumentó un 24% interanual. Aunque sigue siendo menos relevante que el fraude con SIM boxes, este crecimiento sugiere que parte de la presión del fraude se desplazó hacia rutas alternativas de operadores a medida que se fortalecieron los controles sobre canales más establecidos como SMPP y SS7 internacional.

## 2025 mostró un mejor desempeño en bloqueo y menor filtración

En general, los datos muestran que el fraude con SIM boxes siguió siendo el ejemplo más claro de actividad de rutas grises sensible a la estacionalidad en 2025, aumentando junto con los picos de tráfico legítimo de mensajería y continuando como una de las principales fuentes de filtración, mientras que SMPP se mantuvo como la categoría individual con mayor participación. Al mismo tiempo, el entorno general de rutas grises continuó evolucionando: las filtraciones por SS7 internacional y SMPP se redujeron significativamente, la filtración OLO aumentó y la filtración total disminuyó de forma considerable. Esta combinación refleja un mercado en el que los controles contra el fraude se volvieron más efectivos, automatizados y específicos, aunque los actores maliciosos continuaron adaptándose rápidamente a medida que mejoraban las medidas de protección.

DISTRIBUCIÓN GLOBAL DE RUTAS GRIS EN 2024 Y 2025



### Vodafone Fiji

Después de implementar Anam Protect, el tráfico SMS fraudulento de Vodafone Fiji se redujo drásticamente, mientras que las fuentes de ingresos legítimos fueron protegidas y monetizadas.

**29x** mayor ingreso mensual vía SMS

**23x** más tráfico SMS monetizado



### PLDT Enterprise

Después de implementar Anam Protect SMS Firewall de Infobip, PLDT Enterprise fortaleció la seguridad de SMS en la red de Smart al reducir el spam, el smishing y los intentos de mensajería fraudulenta, mientras mejoraba la protección de los suscriptores.

**1.300 millones+** intentos de spam y fraude bloqueados en 6 meses

Mejor entrega de SMS y mayor seguridad de red





# Inteligencia de tráfico OTP

```
{
  "messages": [
    {
      "-destinations": [
        {
          "messageId": "MESSAGE-ID-123-xyz",
          "to": "41793026727"
        },
        {
          "to": "41793026834"
        }
      ],
      "from": "InfoSMS",
      "intermediateReport": true,
    },
    {
      "notifyContentType": "application/json",
      "notifyUrl": "https://www.example.com/sms/advanced",
      "text": „Welcom to Infobip Messaging.",
    }
  ]
}
```



Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

## DETECCIÓN DEL FRAUDE & IA

# Convirtiendo Signals en protección

Infobip Signals identificó automáticamente patrones de tráfico asociados con AIT, SMS pumping y explotación de OTP mediante bots, detectando interacciones OTP fraudulentas tanto en 2024 como en 2025.

La tasa global de actividad sospechosa disminuyó y mostró una mejora interanual del 35%. El volumen absoluto de mensajes sospechosos se redujo un 38%.

## Real-time risk scoring and threat intelligence

Infobip Signals monitorea los flujos de mensajes OTP en tiempo real, identificando interacciones que coinciden con patrones asociados al tráfico inflado artificialmente: aumentos repentinos de volumen, concentraciones geográficas inusuales, bajas tasas de conversión de OTP y actividad de bots entre múltiples marcas.

El tráfico inflado artificialmente (también conocido como fraude de SMS pumping) se estima actualmente en un costo de 8.500 millones de USD anuales para las empresas, lo que destaca el impacto financiero del fraude por SMS en organizaciones que dependen de la mensajería y la autenticación basada en SMS. Una empresa que utiliza SMS para la verificación mediante contraseña de un solo uso (OTP) puede encontrarse pagando millones de mensajes enviados a números controlados por bots, sin recibir nada a cambio más que una factura mensual extremadamente elevada.

En lugar de clasificar mensajes individuales, Signals analiza patrones de comportamiento en el tráfico OTP que indican actividad artificial. Ningún mensaje aislado activa la detección; la señal de fraude se encuentra en el patrón general.

## ANÁLISIS REGIONAL

# Donde se intensifican las amenazas

El volumen de mensajes OTP monitoreados por Signals que fueron identificados como sospechosos es la métrica principal de esta sección. Cuando el volumen disminuye, Signals ayudó a interrumpir campañas de fraude que estaban aumentando los costos de SMS para las empresas.

Cuando el volumen aumenta, Signals está detectando una mayor presión de fraude OTP en ese mercado, protegiendo a las empresas antes de que la exposición financiera se incremente. En ambos casos, Signals cumple exactamente con su objetivo: prevenir el AIT para las empresas.



## Europa y LATAM destacan

Europa registró el mayor aumento de actividad sospechosa de AIT en 2025, con un incremento del 86% interanual en el volumen detectado. LATAM también experimentó un aumento significativo, con un crecimiento del 75% en el volumen sospechoso. La magnitud del incremento sugiere un cambio más amplio en la actividad fraudulenta, en lugar de campañas aisladas, con una mayor presión en ambas regiones. Esto hace que la detección temprana de riesgos y los controles de autenticación más sólidos sean aún más importantes, especialmente en mercados donde los patrones de fraude se vuelven cada vez más persistentes.

**cabify**

**Cabify**

La plataforma de transporte enfrentaba pérdidas financieras significativas debido a ataques de AIT en su flujo de OTP. Después de integrar Infobip Signals, obtuvo resultados inmediatos en menos de 10 minutos.

**15.7%** reducción de pérdidas financieras por AIT en un solo trimestre

**NEXT**

**Next**

El minorista de moda abordó el AIT y, al mismo tiempo, mejoró la calidad de la interacción con sus clientes mediante una solución impulsada por IA y aprendizaje automático, transformando un desafío de fraude en una oportunidad de evolución del canal.

**175K** mensajes artificiales bloqueados al mes





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

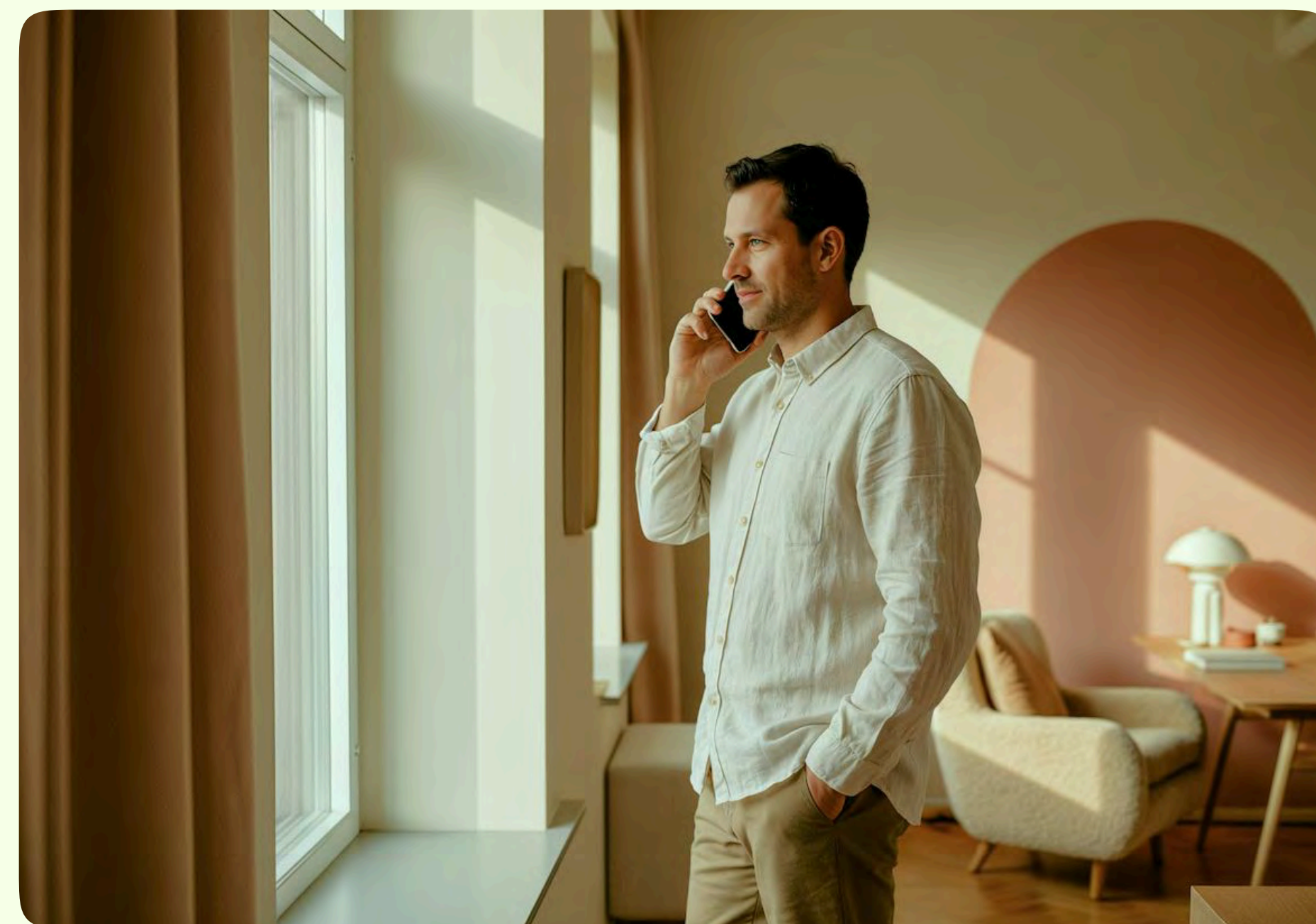
Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad



## OTP y MFA siguen siendo fundamentales para prevenir la toma de control de cuentas

El OTP es un componente clave de la autenticación de dos factores (2FA), que continúa siendo un enfoque común dentro de la autenticación multifactor (MFA). La conclusión es clara: el SMS sigue siendo el canal de OTP más utilizado a nivel mundial debido a su alcance universal y simplicidad, pero ese mismo alcance también genera exposición al fraude.

Como resultado, las empresas están complementando el OTP por SMS no solo con métodos de autenticación alternativos que mejoran la seguridad y la experiencia del cliente, como la verificación de número, sino también con otras señales de red basadas en telecomunicaciones, como la detección de SIM Swap. Esto les permite identificar sesiones riesgosas en etapas más tempranas del proceso de inicio de sesión y mejorar su capacidad general de protección. Infobip Signals ayuda adicionalmente a las empresas a protegerse contra ataques de AIT.

### MÁS ALLÁ DEL SMS

## OTT y verificación de número

Infobip Authenticate refleja este cambio en la estrategia de canales. Permite la entrega de OTP a través de múltiples canales: SMS, voz, WhatsApp, RCS, Viber y otros canales OTT locales predominantes como Kakao y Zalo, con selección inteligente de canales que dirige cada OTP al canal óptimo según la probabilidad de entrega, el costo y la disponibilidad regional. Si el canal principal falla, se activa automáticamente un mecanismo de respaldo. La plataforma permite a las empresas autenticar a sus clientes mediante sus canales preferidos, manteniendo los estándares de seguridad que requieren las industrias reguladas.

La autenticación incluye una amplia variedad de canales además del SMS, entre ellos:

- **RCS** - ofrece una experiencia de mensajería más completa y personalizada, con identidad de remitente verificada y capacidades interactivas para la entrega de OTP.
- **WhatsApp** - proporciona mensajería cifrada y comunicación empresarial verificada en mercados donde es una plataforma de comunicación dominante.
- **OTP vía voz** - garantiza accesibilidad para usuarios sin conexión a internet móvil.
- **Viber** - ofrece una alternativa confiable para la entrega de OTP en regiones donde Viber sigue siendo un canal de comunicación popular entre consumidores.
- **Zalo** - permite la autenticación mediante una de las plataformas de mensajería locales más utilizadas en Vietnam, siendo especialmente relevante para empresas que operan en un mercado con un uso estructuralmente fuerte de canales OTT locales.
- **Kakao** - habilita la entrega de OTP a través de KakaoTalk, una aplicación de mensajería líder en Corea del Sur, donde la relevancia de los canales locales puede mejorar significativamente el alcance y la experiencia del usuario.
- **Telegram** - amplía la autenticación para usuarios de una aplicación de mensajería ampliamente adoptada en múltiples mercados.

Cada canal equilibra seguridad, alcance y disponibilidad, y las estrategias de autenticación más efectivas combinan múltiples canales en lugar de depender de uno solo.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

## Regulación impulsando la estrategia de autenticación

En Filipinas, el Bangko Sentral ng Pilipinas (BSP) está impulsando que los bancos limiten el uso de OTP por SMS para transacciones de alto riesgo, exigiendo métodos de autenticación más sólidos que incluyan biometría, vinculación de dispositivos, señales de comportamiento y claves criptográficas.

En Emiratos Árabes Unidos, el Banco Central está exigiendo a los bancos migrar de los OTP por SMS y correo electrónico hacia métodos de verificación dentro de la aplicación y basados en dispositivos móviles. Ambos reguladores mencionan explícitamente las vulnerabilidades de la autenticación basada en SMS — phishing, fraude por SIM Swap y riesgos de interceptación— como los principales motivos de estas medidas.

Estas no son decisiones regulatorias aisladas. Son los primeros indicadores de un cambio regulatorio más amplio que requerirá que las empresas cuenten con una infraestructura de autenticación multicanal. A medida que más reguladores sigan el camino de Emiratos Árabes Unidos y Filipinas, la dependencia exclusiva del SMS como canal único no solo se convertirá en un riesgo de seguridad, sino también en un riesgo de cumplimiento normativo.

Las empresas que ya han diversificado sus canales de autenticación están adelantándose a esta evolución regulatoria. Al mismo tiempo, métodos alternativos de autenticación, como la verificación de número basada en telecomunicaciones mediante API, ofrecen una forma práctica para que las empresas se adapten a este cambio de cumplimiento.



### NUESTROS CLIENTES EMPLEAN 2FA

 **bukalapak**

#### Bukalapak

Una empresa de comercio electrónico eliminó los problemas de entrega de OTP en toda su plataforma mediante 2FA por SMS. La rápida resolución de problemas técnicos y la entrega confiable a gran escala eliminaron el cuello de botella que estaba bloqueando los registros de usuarios y la finalización de transacciones.

**4-5%** de aumento en las tasas de entrega

 **leanpay**

#### Leanpay

Una empresa fintech necesitaba una solución de 2FA lo suficientemente simple como para no generar fricción en el proceso de aprobación de préstamos, pero lo suficientemente segura para verificar la identidad de los clientes al tomar decisiones crediticias.

**20%** de crecimiento mensual de usuarios registrados





# APIs de Red

```
{  
  "ueId": {  
    "externalId": "123456789@domain.com",  
    "msisdn": "+441134961234",  
    "ipv4Addr": "192.168.1.100",  
    "ipv6Addr": "2001:db8::1"  
  },  
  "uePort": 8080,  
  "latitude": 51.5074,  
  "longitude": -0.1278,  
  "accuracy": 10  
}
```



# Las interacciones con APIs de red aumentaron un 91% en 2025

El crecimiento total de las interacciones con Network APIs en 2025 fue del 91%, lo que refleja una demanda empresarial sostenida de señales de prevención de fraude a nivel de red.

Los datos abarcan interacciones de tres productos: detección de SIM Swap, Know Your Customer (KYC) y verificación de número. Cada uno consulta la infraestructura central del operador móvil para responder en tiempo real una pregunta específica de prevención de fraude: si una tarjeta SIM fue cambiada recientemente, si un usuario realmente posee el número telefónico que declara mediante una conexión de datos silenciosa, y si sus datos de identidad coinciden con los registros de suscriptores verificados por el operador.

Estas son señales que no pueden replicarse en la capa de aplicación. Su valor proviene del hecho de que se originan directamente en la red, independientemente de cualquier sistema empresarial.

En todas las regiones incluidas en los datos, **BFSI es el principal usuario de APIs de Red**, con bancos, fintechs y proveedores de pagos liderando la adopción.

## LAS APIS DE RED CONTINUARON CRECIENDO EN 2025

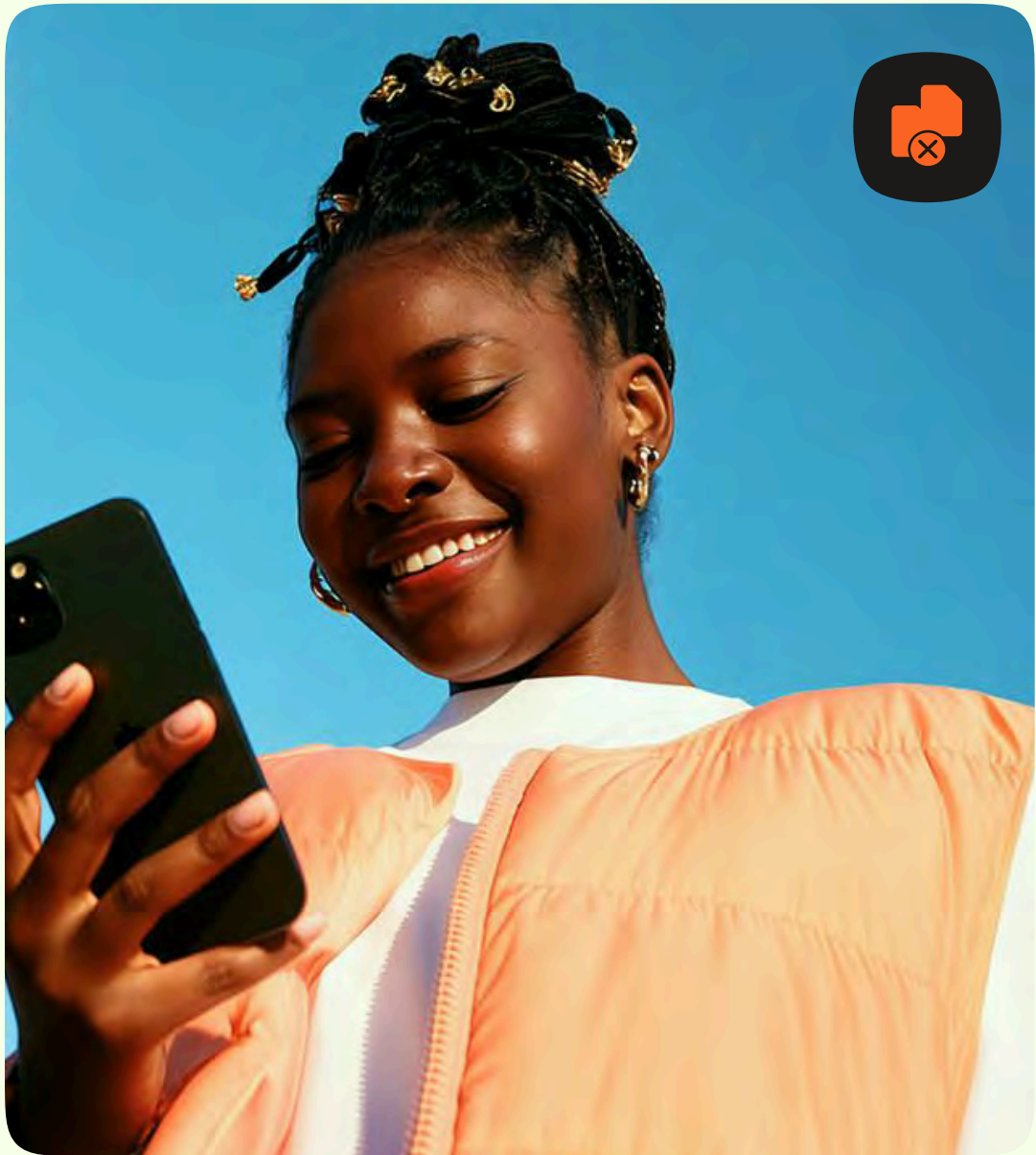
| Producto               | Crecimiento interanual |
|------------------------|------------------------|
| Sim Swap               | 78%                    |
| Verificación de número | 378%                   |
| KYC                    | 88%                    |

## SIM SWAP

### ¿Por qué la detección de SIM Swap lidera los esfuerzos contra el fraude?

SIM Swap representa la mayoría de todas las interacciones de Network APIs en 2025, lo que refleja la mayor adopción entre las empresas. Toda organización que envía códigos de autenticación por SMS a sus clientes debería realizar verificaciones de SIM Swap: si una SIM fue cambiada recientemente, podría significar que un atacante ahora tiene el control de ese número y puede interceptar el OTP.

Aunque la tasa de crecimiento sigue siendo sólida, es la más baja de los tres productos porque SIM Swap ya era la solución más grande y con mayor adopción comercial.



## USO DE SIM SWAP POR INDUSTRIAS

| Industria                              | Crecimiento interanual |
|----------------------------------------|------------------------|
| Finanzas y fintech                     | 73%                    |
| Tecnología y software                  | 92%                    |
| Servicios mayoristas y de comunicación | 47%                    |

El sector de finanzas y fintech creció un 73% en interacciones de SIM Swap durante 2025. Los bancos, las fintech y las plataformas de pago son los principales usuarios de la detección de SIM Swap para protegerse contra la toma de control de cuentas.

El sector de tecnología y software creció un 92%, lo que refleja cómo las empresas de plataformas están integrando la detección de SIM Swap en sus productos y distribuyéndola a clientes empresariales finales.

Nuestros datos muestran que LATAM es, por amplio margen, la región de red dominante, proporcionando la infraestructura para el 90% de todas las interacciones globales de SIM Swap en 2025. Las interacciones relacionadas con LATAM representan la mayor proporción del total, con un crecimiento del 111% frente a 2024, mientras que otras regiones también muestran avances, incluida Europa con un crecimiento del 13%.



## VERIFICACIÓN DE NÚMERO

# 5x de crecimiento global en 2025

Para las empresas que durante años han gestionado fallos en la entrega de OTP, ataques de AIT y costos asociados al SMS pumping, la verificación de número aborda el problema desde la raíz, en lugar de optimizar la entrega de un mecanismo vulnerable. El crecimiento de 5x refleja que las empresas están descubriendo que la alternativa a una mejor entrega de OTP puede ser no necesitar OTP en absoluto. Este crecimiento también demuestra una demanda real del mercado, no solo un interés teórico.

En lugar de enviar un código al teléfono del usuario y esperar a que lo introduzca, la verificación de número confirma silenciosamente que el dispositivo actual del usuario tiene el número telefónico esperado, utilizando la propia red móvil como capa de confianza.

## La verificación de número sigue siendo una opción de autenticación en etapa temprana

La verificación de número continuó siendo una capacidad de nicho en 2025, con una adopción todavía limitada tanto entre empresas como entre operadores móviles. Aun así, la tasa de crecimiento muestra un impulso claro, ya que las empresas comienzan a considerarla una alternativa práctica y no solo una tecnología experimental. Las principales limitaciones son prácticas, más que estratégicas: la cobertura del mercado es desigual y solo funciona mediante conexiones de datos móviles, no a través de Wi-Fi, lo que reduce su alcance en los recorridos habituales de los clientes. El OTP por SMS sigue siendo la opción predeterminada para muchos procesos de clientes porque es conocido, está disponible globalmente y ya se encuentra integrado en flujos existentes. Los factores comerciales también son relevantes, ya que puede ser más difícil justificar la verificación de número

cuando el SMS continúa siendo más económico y sencillo de implementar.

El enfoque de verificación de número basado en SIM confirma el número telefónico mediante la autenticación directa de la tarjeta SIM utilizando los estándares GSMA TS.43, en lugar de depender de datos de red. Este modelo está más alineado con la evolución futura de la categoría, ya que aprovecha mecanismos existentes de autenticación y autorización dentro de las redes de telecomunicaciones para garantizar seguridad y escalabilidad.

También proporciona una alternativa de baja fricción para procesos en los que las empresas desean confirmar la titularidad de un número sin exponer a los usuarios a un paso adicional de ingreso de OTP. Además, ofrece beneficios prácticos y de seguridad adicionales: funciona a través de conexiones de datos móviles incluso en escenarios de roaming y mediante VPN; proporciona una experiencia invisible para el usuario, ya que no necesita introducir un número telefónico ni ingresar un código; ofrece un mayor nivel de seguridad mediante autenticación criptográfica de la SIM; y admite casos de uso con múltiples SIM, permitiendo al usuario seleccionar cuál SIM verificar.

Dicho esto, esta capacidad puede evolucionar a medida que la presión regulatoria impulse a bancos y otras industrias reguladas hacia métodos de autenticación más sólidos. Esta nueva evolución, conocida como verificación de número basada en SIM o Number Verification v2, junto con la estandarización alineada con CAMARA, podría ayudar a ampliar la adopción a medida que la API madure y sus casos de uso sean más prácticos. Por ahora, los datos indican que la verificación de número todavía se encuentra en una etapa temprana de adopción, en lugar de ser un reemplazo generalizado del OTP.

## API DE KNOW YOUR CUSTOMER (KYC)

# Crecimiento sostenido de KYC

Las interacciones de KYC crecieron un 88% interanual, en línea con la tasa general del mercado. KYC valida los datos de identidad proporcionados por el usuario frente a los registros de suscriptores del operador, permitiendo a las empresas confirmar que un cliente es quien afirma ser durante el proceso de registro o solicitud, sin necesidad de verificaciones manuales de documentos.

La API de KYC confirma la información del usuario utilizando datos confiables proporcionados por el operador de telecomunicaciones, ofreciendo una capa de confianza que las aplicaciones OTT tienen dificultades para replicar de forma independiente.

### USO DE LA API KNOW YOUR CUSTOMER POR INDUSTRIA

| Industria                            | Crecimiento interanual |
|--------------------------------------|------------------------|
| Finanzas y fintech                   | 86%                    |
| Tecnología y software                | 14x                    |
| Servicios profesionales y educativos | Nuevo in 2025          |

El sector de **finanzas y fintech** lidera con una participación del **77%**; los bancos y las fintech utilizan la validación de identidad a nivel de red para la incorporación de nuevos clientes.

El sector de **tecnología y software** creció **14x** y ahora representa el **20%** de las interacciones de KYC, lo que indica la distribución de KYC a través de plataformas como un canal emergente.





VOZ Y ENMASCARAMIENTO DE NÚMEROS

# Privacidad desde el diseño

```
{  
  "action": "dial",  
  "from": "41793026727",  
  "to": "41793026731",  
  "transferTo": "41793026785",  
  "duration": 15,  
  "status": "answered",  
  "nmCorrelationId": "7cb72e4b-cf9f-40b6-9fc4-79588d18a666",  
  "ringingTime": "2018-01-01 12:00:00",  
  "answeredTime": "2018-01-01 12:00:10",  
  "correlationId": "0f754338-1aff-4e09-a933-7d205ca7aed4",  
  "inboundDuration": 30,  
  "calculatedDuration": 15,  
  "pricePerSecond": 0.01,  
  "currency": "EUR",  
  "recordingFileId": "7e8d64c0-6c72-4922-aa96-48728753c660",  
  "recordCalleeAnnouncement": true,  
  "recordingStatus": "SFTP",  
  "machineDetectionResult": "HUMAN",  
  "clientReferenceId": "7e8d64c0-6c72-4922-aa96-48728753c660"  
}
```





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

## Protegiendo la privacidad y los datos con la solución Number Masking

Cada día se realizan miles de millones de llamadas entre personas que nunca se han conocido y que nunca necesitarán compartir sus datos de contacto personales. Un conductor coordinando una recogida. Un repartidor llamando antes de una entrega. Un vendedor de un marketplace organizando la entrega de un producto. Un agente de telecomunicaciones dando seguimiento a un cliente. En todos estos casos, la empresa que conecta a ambas partes tiene la responsabilidad de proteger los números telefónicos personales, garantizando al mismo tiempo una forma confiable de que los clientes puedan comunicarse con la persona correcta cuando sea necesario.

Number Masking resuelve este desafío mediante una capacidad de comunicación por voz basada en el principio de privacidad desde el diseño. La solución enruta las llamadas a través de un número virtual en la plataforma de Infobip, ocultando los números telefónicos reales de ambas partes mientras permite una comunicación de voz clara y en tiempo real. Number Masking hace posible una llamada bidireccional sin comprometer el número telefónico de ninguna de las partes; quien recibe la llamada ve un número virtual o enmascarado en lugar del número real del remitente.

Regulaciones como el GDPR, la CCPA y otras normativas regionales de privacidad establecen una fuerte expectativa de que las empresas minimicen los datos personales que recopilan y comparten. En cualquier marketplace de dos lados —como plataformas de transporte, entregas, salud o comercio electrónico— compartir los números telefónicos entre las partes representa una falla en el principio de minimización de datos. Number Masking elimina por completo la necesidad de compartir esa información. La llamada se realiza, pero el número personal nunca sale de la plataforma.

### ADOPCIÓN POR INDUSTRIA

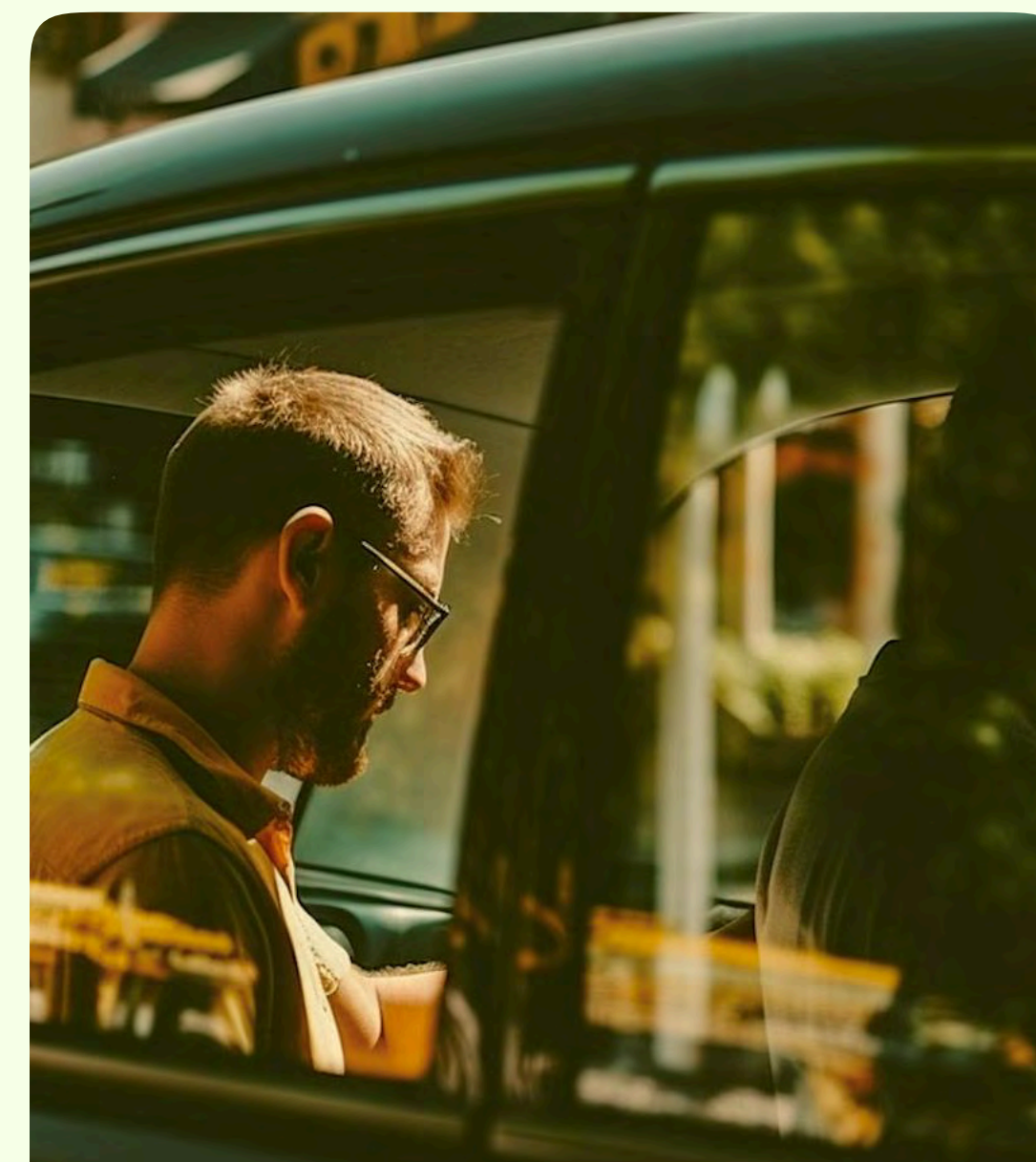
## Las plataformas de domicilios impulsan el crecimiento

Las plataformas de transporte y de entregas bajo demanda representan en conjunto el 97% de todas las interacciones de Number Masking tanto en 2024 como en 2025. Esta concentración refleja una dependencia estructural: para cualquier plataforma que conecte a un conductor o repartidor con un pasajero o cliente, el anonimato en las llamadas es un requisito de seguridad y cumplimiento integrado en la operación del servicio.

## Telecomunicaciones: protegiendo la privacidad de empleados y clientes

El caso de uso en telecomunicaciones es diferente al de las plataformas de transporte. Los operadores utilizan Number Masking en sus propias operaciones de atención al cliente, enrutando las llamadas salientes de agentes de centros de contacto o técnicos de campo a través de números anonimizados, evitando que los clientes conserven y hagan un uso indebido de los datos de contacto personales de los empleados.

Se trata de privacidad desde el diseño aplicada a la propia fuerza laboral del operador. A medida que las empresas de telecomunicaciones gestionan cada vez más las relaciones con sus clientes mediante canales de voz y digitales, exponer los números telefónicos personales de sus empleados representa tanto un riesgo de cumplimiento normativo como un problema de seguridad para el personal. Number Masking aborda ambos desafíos de forma simultánea, y el crecimiento del volumen en este segmento sugiere que cada vez más operadores lo están adoptando como una práctica estándar.



## Uber

**Uber**

La empresa de transporte y entrega de alimentos utiliza Number Masking para proteger la privacidad de sus usuarios durante las llamadas entre conductores y pasajeros, manteniendo ocultos los números telefónicos personales. Esto mejora la confianza y la seguridad, al tiempo que permite una comunicación segura entre ambas partes.

**90%** de anonimización de llamadas a nivel global



# Industrias en las que se está expandiendo Number Masking

La concentración del uso de Number Masking en las plataformas de transporte y entrega refleja los sectores donde este caso de uso es más urgente desde el punto de vista operativo y donde su adopción comercial está más consolidada. Más allá de estos sectores principales, Number Masking continúa expandiéndose a otras industrias.

## Salud

Las plataformas de telesalud y los coordinadores de servicios médicos que conectan a pacientes con profesionales de la salud enfrentan el mismo desafío de arquitectura de privacidad que las plataformas de transporte. Dos personas necesitan comunicarse en tiempo real, pero ninguna debería conservar los datos de contacto personales de la otra; la plataforma debe seguir siendo el intermediario de confianza para la comunicación. En el sector salud, este desafío es aún mayor debido a la sensibilidad de los datos y a los requisitos regulatorios.

El modelo de sesiones temporales de Number Masking resulta especialmente adecuado: el número virtual permanece activo únicamente durante el tiempo de la cita y se desactiva al finalizar, evitando cualquier exposición innecesaria de datos una vez concluida la consulta.

El OTP vía voz también desempeña un papel único en el sector salud que ningún otro canal puede reemplazar por completo. Permite atender a pacientes de edad avanzada, con discapacidad visual o poco familiarizados con aplicaciones móviles, grupos que están sobrerrepresentados en los servicios de salud. Además, contar con un mecanismo de respaldo mediante OTP por voz garantiza que ningún paciente quede sin acceso a su historial médico debido a un fallo en la entrega de un SMS.

## Logística y entregas de última milla

La logística y las entregas de última milla comparten prácticamente el mismo modelo de privacidad que las plataformas de transporte. Un repartidor necesita comunicarse con el destinatario al llegar al punto de entrega; el destinatario no debería conservar el número del repartidor y la plataforma logística debe seguir siendo el canal de comunicación.

A medida que las empresas de logística digitalizan sus operaciones de última milla, Number Masking se implementa cada vez más junto con el seguimiento en tiempo real y la confirmación de entregas como parte de una estrategia integral de comunicación basada en la privacidad desde el diseño, especialmente relevante conforme las entregas el mismo día y bajo demanda continúan expandiéndose a nivel mundial.

## Marketplaces y comercio entre particulares

Las plataformas de anuncios clasificados, marketplaces de alquiler y sitios de comercio entre particulares enfrentan el desafío de permitir la comunicación entre compradores y vendedores antes de que se complete una transacción, cuando todavía no existe la confianza suficiente para compartir información de contacto personal.

Number Masking hace posible esta comunicación sin necesidad de intercambiar números telefónicos, manteniendo a la plataforma como intermediario de confianza y protegiendo a ambas partes durante toda la etapa previa a la transacción.

## Operaciones de campo en servicios financieros

Los asesores financieros, ejecutivos de préstamos y ajustadores de seguros que realizan llamadas salientes a clientes exponen sus números telefónicos personales durante esas comunicaciones.

Number Masking permite a las instituciones financieras enrutar todas las llamadas de campo a través de números anonimizados, protegiendo la privacidad de los empleados, manteniendo registros de llamadas para fines de cumplimiento normativo, evitando el contacto directo que elude los mecanismos de supervisión de la institución y garantizando que todas las interacciones permanezcan dentro del registro de auditoría de la plataforma.

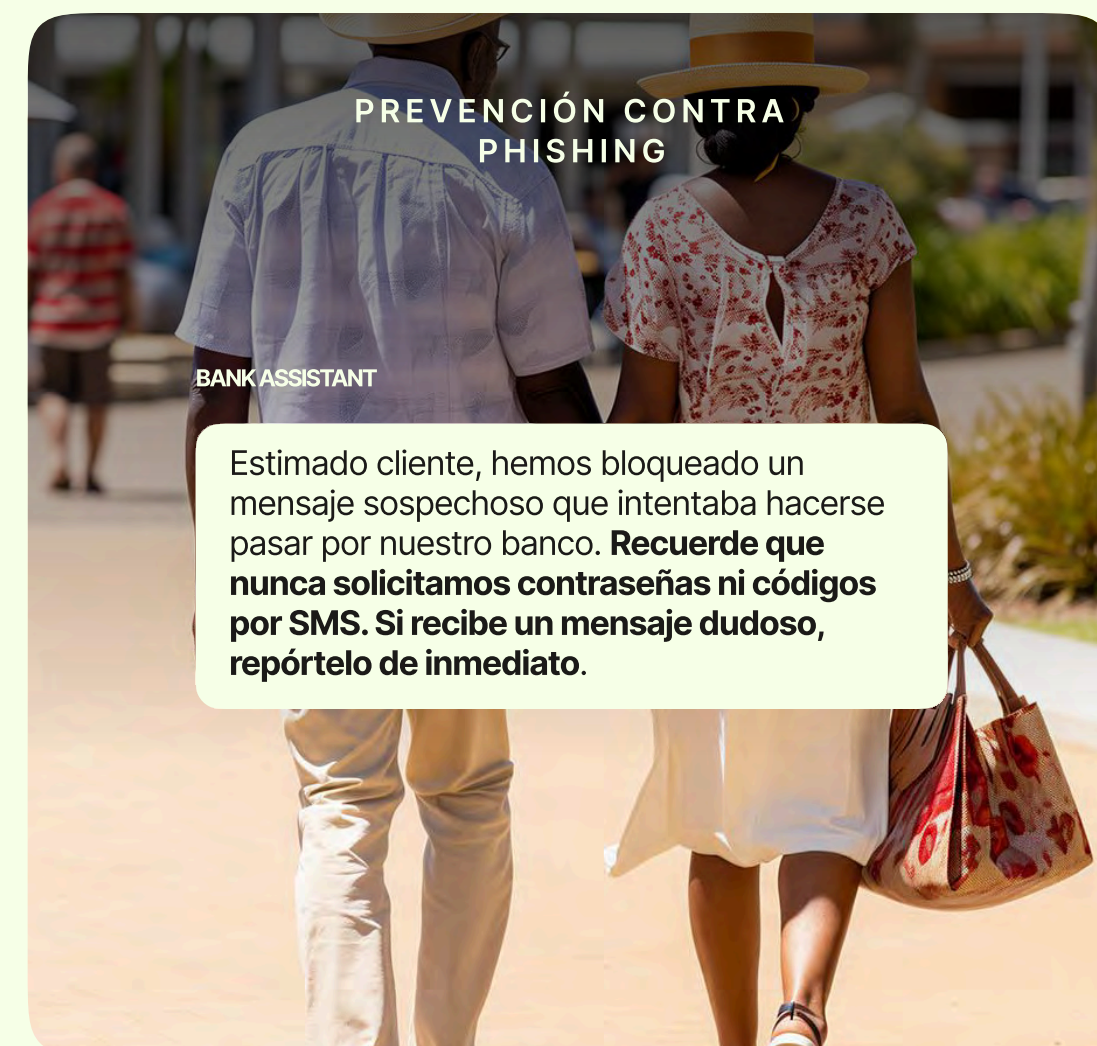




# Tendencias y panoramas regionales



Las tácticas de fraude difieren considerablemente de una región a otra, debido, entre otros factores, a las diferencias en los marcos regulatorios, el nivel de adopción tecnológica y los comportamientos de los consumidores. Así es como se ha visto afectada cada región.



### PREVENCIÓN CONTRA PHISHING

BANK ASSISTANT

Estimado cliente, hemos bloqueado un mensaje sospechoso que intentaba hacerse pasar por nuestro banco. **Recuerde que nunca solicitamos contraseñas ni códigos por SMS. Si recibe un mensaje dudoso, repórtelo de inmediato.**

## LATAM

LATAM se encuentra entre las regiones con mayor incidencia de fraude relacionado con la mensajería. Las operaciones de rutas grises y SIM boxes dirigidas a afectar los ingresos de los operadores de telecomunicaciones son frecuentes, mientras que, a nivel de contenido, el phishing representa la gran mayoría de los mensajes maliciosos bloqueados.

La región también registra un aumento del tráfico OTP sospechoso, lo que refleja cómo los actores maliciosos están siguiendo el crecimiento de la economía digital latinoamericana hacia nuevas superficies de ataque.

Además, LATAM destaca como el mercado más avanzado en la implementación de soluciones de prevención del fraude respaldadas por Network APIs.



### ALERTA DE INTEGRIDAD DE LA AUTENTICACIÓN

金融科技助手

我们注意到您的账户在一台新设备上出现多次 OTP 请求。为了保护您的账户，我们已暂时暂停验证，直到您确认这些请求是由您本人发起的。请在应用程序中点击链接继续操作。您的安全是我们的首要任务。

## APAC

APAC presenta un panorama dual en materia de fraude. A nivel de red, es la región más avanzada tecnológicamente según nuestros datos: los firewalls de los operadores están altamente automatizados y los modelos de detección impulsados por IA han alcanzado un nivel de madurez que permite identificar la mayoría de las amenazas sin intervención humana.

Sin embargo, a nivel empresarial, el fraude basado en OTP sigue siendo persistente en mercados clave. Algunos territorios muestran tasas consistentemente elevadas de autenticaciones sospechosas, lo que apunta a entornos de fraude estructurales y no únicamente a campañas aisladas.

La presión regulatoria también está aumentando. Filipinas ha comenzado a exigir métodos de autenticación más sólidos para transacciones bancarias de alto riesgo, lo que indica que los reguladores financieros de la región consideran las vulnerabilidades del OTP por SMS como un problema de cumplimiento normativo, además de un riesgo de seguridad.



### GARANTÍA DE MENSAJERÍA SEGURA

MOBILE OPERATOR ASSISTANT

Your network is protected by advanced automated security systems that block fraudulent SMS before they reach your phone. **If you ever receive an unexpected OTP or suspicious message, report it through your operator app so we can continue improving your protection.**

## NAM

El principal desafío de fraude en Norteamérica se concentra en la capa de autenticación, especialmente por el tráfico OTP inflado artificialmente y las campañas de smishing. El perfil de fraude de la región está orientado principalmente hacia las empresas, más que hacia los operadores de telecomunicaciones, por lo que el monitoreo de OTP en tiempo real y la selección inteligente del canal de autenticación representan las medidas de protección con mayor impacto comercial.

Los patrones observados también sugieren un potencial creciente para el uso de soluciones antifraude basadas en Network APIs, a medida que se amplía su cobertura en el mercado.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad

## CUMPLIMIENTO NORMATIVO

FINANCIAL SERVICE ASSISTANT

We are strengthening our authentication process to comply with updated European security and data-protection standards. If you receive an OTP you did not request, please report it through your app. **This helps us protect your account and ensure secure communication across all European markets.**

## EUROPA

En Europa estamos observando un deterioro significativo en los indicadores de fraude relacionados con OTP, con un fuerte aumento del tráfico de autenticaciones sospechosas que revierte la percepción anterior de Europa como una región de riesgo relativamente bajo. Al mismo tiempo, estamos viendo una adopción inicial de Network APIs como parte de las soluciones antifraude, lo que sugiere que las empresas están dispuestas a fortalecer sus controles actuales con nuevas capacidades a medida que estas se vuelven más accesibles.

El entorno regulatorio añade una dimensión particular: requisitos más estrictos de protección de datos regulan la forma en que las empresas pueden comunicarse con sus clientes, haciendo que una mensajería segura y conforme a la normativa sea una obligación legal, además de una prioridad comercial para las organizaciones que operan en múltiples mercados europeos.

## ENTREGA POR ENRUTAMIENTO NO AUTORIZADO

E-COMMERCE ASSISTANT

We're processing your verification code, but delivery may take longer than usual due to unauthorized routing attempts detected on the network. Please request a new code through your account if you don't receive it shortly. Your security is important to us.

## ÁFRICA

La gran cantidad de operadores presentes en numerosos mercados del continente, junto con los distintos niveles de aplicación de las regulaciones, crea condiciones estructurales en las que el enrutamiento no autorizado de SMS sigue siendo una práctica extendida.

A pesar de ello, el modelo de detección impulsado por IA que protege las redes de los operadores africanos registró la mayor mejora de cualquier región en 2025, demostrando que la detección inteligente y automatizada puede ser efectiva incluso frente a volúmenes muy elevados de fraude.

Es importante señalar que la cobertura de Infobip se concentra en los principales mercados económicos del continente, por lo que la magnitud real del fraude por SMS en África probablemente sea mayor que la reflejada en este conjunto de datos.

## CONFIRMACIÓN FINAL Y ACCESO SEGURO

مساعد خدمات حكومية

تم تأمين حسابك الآن. يمكنك متابعة استخدام خدماتنا بعد تفعيل طريقة المصادقة الجديدة. شكرًا لمساعدتك لنا في الحفاظ على أمان معلوماتك.

## MENA

MENA está experimentando un aumento de la presión del fraude tanto a nivel de red como en la capa de autenticación de forma simultánea.

Las tasas de OTP sospechosos están creciendo por encima del promedio global, están surgiendo nuevos mercados de alto riesgo y el firewall SMS registró en 2025 el crecimiento más acelerado del volumen de tráfico bloqueado entre todas las regiones.

El entorno regulatorio también está evolucionando. El Banco Central de Emiratos Árabes Unidos ha ordenado la eliminación gradual de los OTP enviados por SMS y correo electrónico, sustituyéndolos por métodos de autenticación más sólidos, debido a los riesgos asociados con el phishing, el fraude por SIM Swap y la interceptación de comunicaciones. Para las empresas que operan en MENA, esta combinación de mayor actividad fraudulenta y regulaciones más estrictas convierte la modernización de la infraestructura de autenticación en una prioridad operativa inmediata, y no en una iniciativa para el futuro.





# Tendencias de fraude por industria

La exposición al fraude varía significativamente entre industrias, impulsada por diferencias en el volumen de transacciones, los requisitos de autenticación, la presencia regional y el valor económico que los datos o las cuentas representan para los atacantes.

Comprender estos perfiles de riesgo específicos por industria es fundamental para desarrollar estrategias de seguridad que respondan a las amenazas reales de cada sector, en lugar de aplicar un enfoque único para un problema que, por naturaleza, presenta características distintas según la industria.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

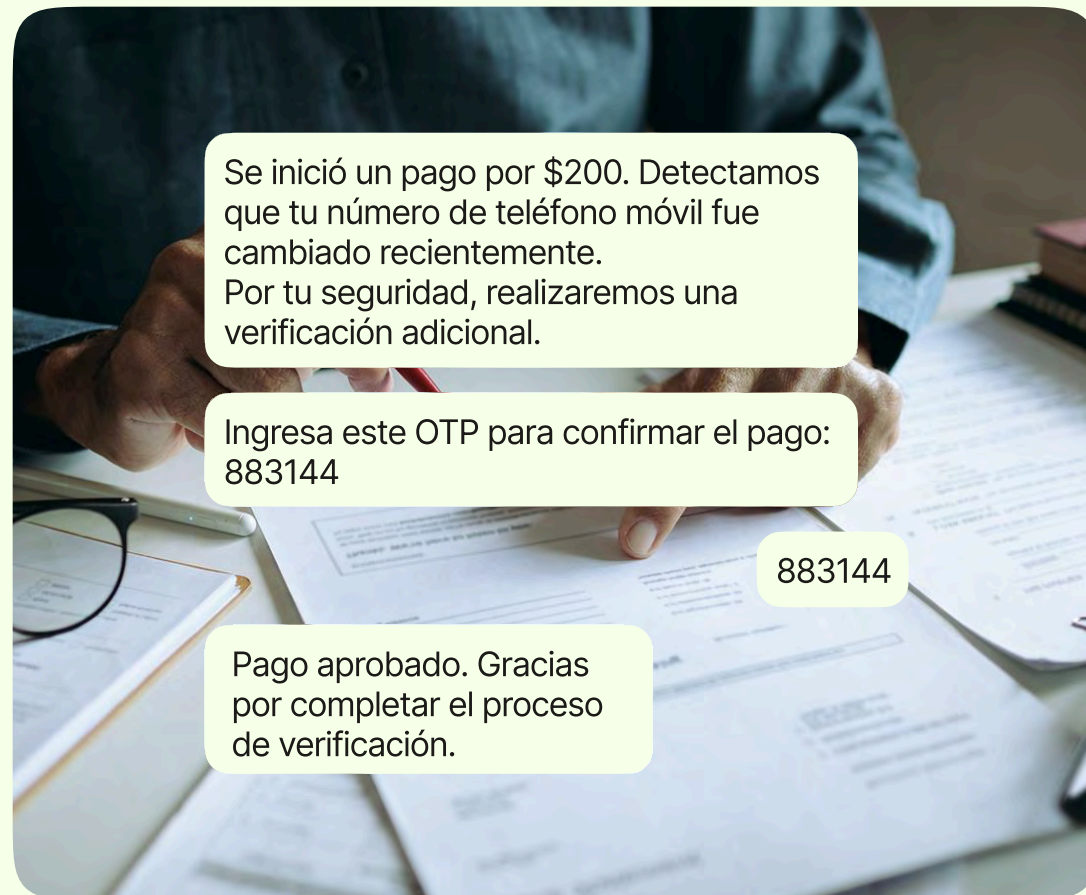
Enmascaramiento de números

Tendencias de fraude por regiones

**Tendencias de fraude por industria**

Recomendaciones futuras para las empresas

El futuro de la confianza y la seguridad



## Banca, servicios financieros y seguros

Las organizaciones del sector financiero enfrentan algunos de los vectores de fraude más sofisticados. La toma de control de cuentas mediante SIM Swap, donde un atacante convence a un operador móvil de transferir el número de la víctima a una nueva tarjeta SIM, representa una vía casi directa para comprometer las credenciales bancarias, ya que la mayoría de los bancos utiliza OTP por SMS como principal método de autenticación de dos factores (2FA). La exposición al fraude en este sector abarca la verificación de identidad durante el registro de clientes, el inicio de sesión en cuentas, la autorización de pagos, la confirmación de préstamos y el procesamiento de reclamaciones de seguros; cada uno de estos procesos requiere mecanismos de autenticación adecuados según el valor de la transacción y el nivel de riesgo.

La detección de SIM Swap y la verificación de número mediante Network APIs se encuentran entre los casos de uso más importantes para aprovechar inteligencia antifraude a nivel de operador.

El interés del sector por implementar estrategias de seguridad en múltiples capas también continúa creciendo a medida que los intentos de fraude se vuelven cada vez más sofisticados.



## Telecomunicaciones

Los operadores de telecomunicaciones ocupan una posición única en el panorama del fraude: son, al mismo tiempo, la infraestructura que hace posible la autenticación basada en SMS y las organizaciones más directamente afectadas cuando esa infraestructura es explotada. Cada mensaje que evade las rutas oficiales mediante rutas grises representa una pérdida de ingresos por facturación para los operadores.

En 2025, los operadores están respondiendo de dos maneras complementarias: utilizando firewalls como Anam Protect para proteger y monetizar el tráfico SMS, y ofreciendo Network APIs como SIM Swap, Verificación de número y KYC, que permiten a las empresas fortalecer sus propios controles antifraude. En este modelo, las empresas de telecomunicaciones se posicionan principalmente como proveedoras dentro del mercado de Network APIs, mientras que el sector de banca, servicios financieros y seguros (BFSI) sigue siendo la principal industria que utiliza estas APIs en casos de uso relacionados con la prevención del fraude.

Algunos operadores también emplean estas capacidades internamente para la gestión de suscriptores y la seguridad de las cuentas, aunque el crecimiento del mercado continúa siendo impulsado principalmente por la demanda empresarial.



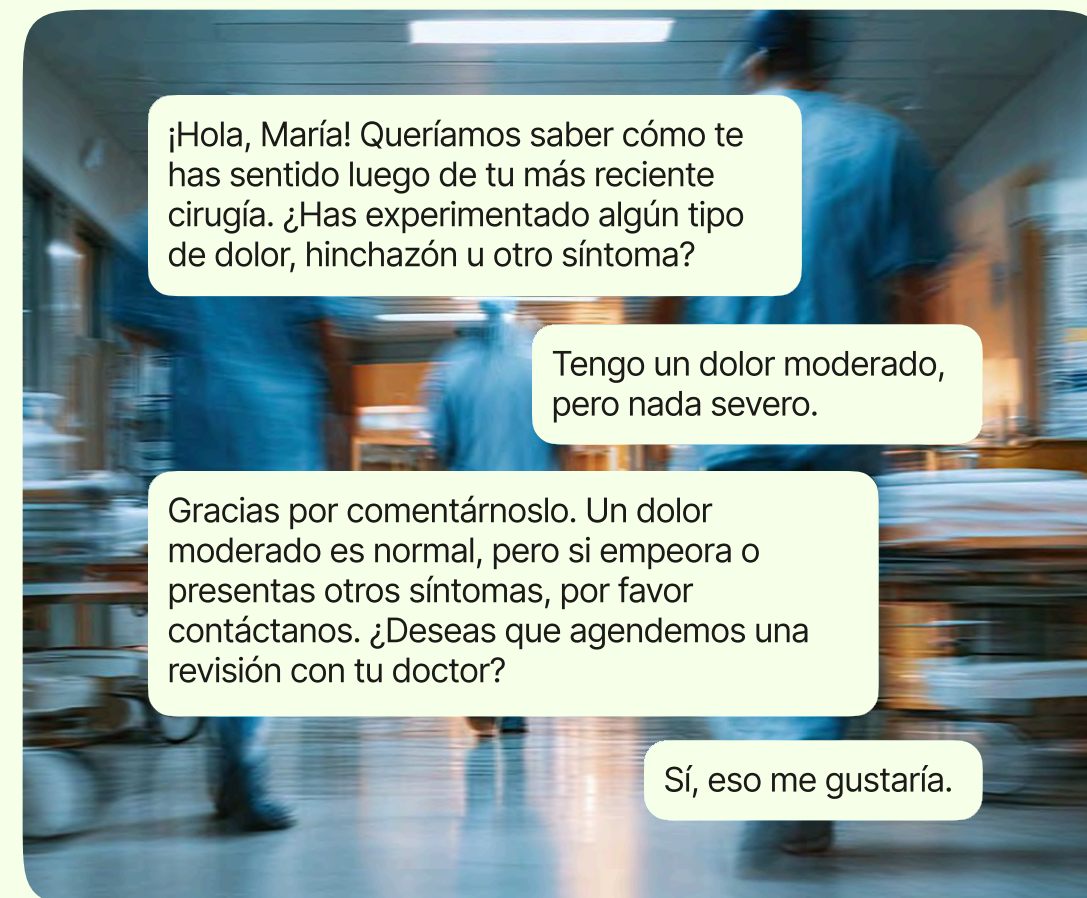
## Retail y comercio electrónico

El fraude en el sector retail y de comercio electrónico abarca todo el ciclo de vida del cliente: bots que crean cuentas falsas durante el registro, ataques de toma de control de cuentas dirigidos a credenciales de pago almacenadas, interceptación de OTP y confirmaciones de transacciones fraudulentas diseñadas para facilitar contracargos. El desafío de la autenticación se ve agravado por la escala: los grandes comercios procesan millones de transacciones diarias y cualquier fricción en el proceso de autenticación tiene un impacto directo en las tasas de conversión.

La creciente adopción de Signals para la protección contra AIT refleja una realidad comercial: los ataques de AIT dirigidos a los puntos de envío de OTP en plataformas de comercio electrónico generan cargos elevados e inesperados por SMS que aparecen en las cuentas de las empresas antes de que el ataque sea detectado. La detección en tiempo real de Signals evita que esos costos se acumulen desde el inicio.

De manera más amplia, este mismo entorno de fraude está impulsando el interés por las Network APIs, que proporcionan señales adicionales para fortalecer los controles antifraude en los procesos de registro, inicio de sesión y pagos.





## Salud

El fraude en el sector salud se encuentra en la intersección entre la sensibilidad de los datos, el cumplimiento regulatorio y la seguridad de los pacientes.

Los portales de pacientes, las plataformas de telesalud, los sistemas de gestión de recetas y los historiales clínicos electrónicos requieren un acceso seguro. En este sector, las consecuencias de una falla en la autenticación van más allá de las pérdidas financieras, ya que pueden afectar la seguridad del paciente y generar responsabilidades regulatorias. En este contexto, Number Masking también desempeña un papel importante al ayudar a proteger los datos de contacto de los pacientes en los flujos de comunicación donde la privacidad y la confianza son fundamentales.



## Gobierno y sector público

Los servicios gubernamentales enfrentan los mismos desafíos de autenticación y confianza que otros servicios digitales de alto riesgo, pero las consecuencias son mayores porque los fallos pueden afectar a grandes poblaciones de ciudadanos y datos personales sensibles. Los servicios orientados a los ciudadanos, como los portales de impuestos, las solicitudes de beneficios, las renovaciones de documentos de identidad y los registros de licencias, suelen depender de códigos OTP (contraseñas de un solo uso) para el acceso y la confirmación de transacciones, lo que los hace vulnerables tanto a la toma de control de cuentas como a ataques de tráfico automatizado.

El sector también enfrenta una presión creciente para reforzar la autenticación, ya que los reguladores y las instituciones públicas ponen mayor énfasis en una identidad digital segura y resiliente. La supervisión en tiempo real puede ayudar a los equipos gubernamentales a distinguir la actividad legítima de los usuarios de los patrones de fraude a gran escala, especialmente cuando los altos volúmenes de mensajes dificultan separar el acceso válido del uso indebido.



## Logística y servicios de transporte bajo demanda

Los servicios bajo demanda, como la logística, el transporte con conductor y la entrega de alimentos, comparten un desafío común en su arquitectura de seguridad: necesitan conectar a dos partes (el conductor y el pasajero, el repartidor y el destinatario) en tiempo real, sin que ninguna de las partes tenga que conocer los datos de contacto personales de la otra, y sin que los conductores tengan que manipular sus teléfonos mientras conducen un vehículo.

El enmascaramiento de números (Number Masking) aborda este problema directamente, y su adopción en estos sectores ha crecido significativamente en 2025. Las API de red (Network APIs) también tienen un papel importante, especialmente en los procesos de registro e inicio de sesión de conductores y repartidores, donde pueden ayudar a verificar que la persona que accede a la cuenta sea el usuario legítimo y reducir los riesgos de phishing y toma de control de cuentas.





# Recomendaciones para las empresas en los próximos años

Recomendaciones clave para que las empresas fortalezcan sus estrategias de prevención del fraude.





Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

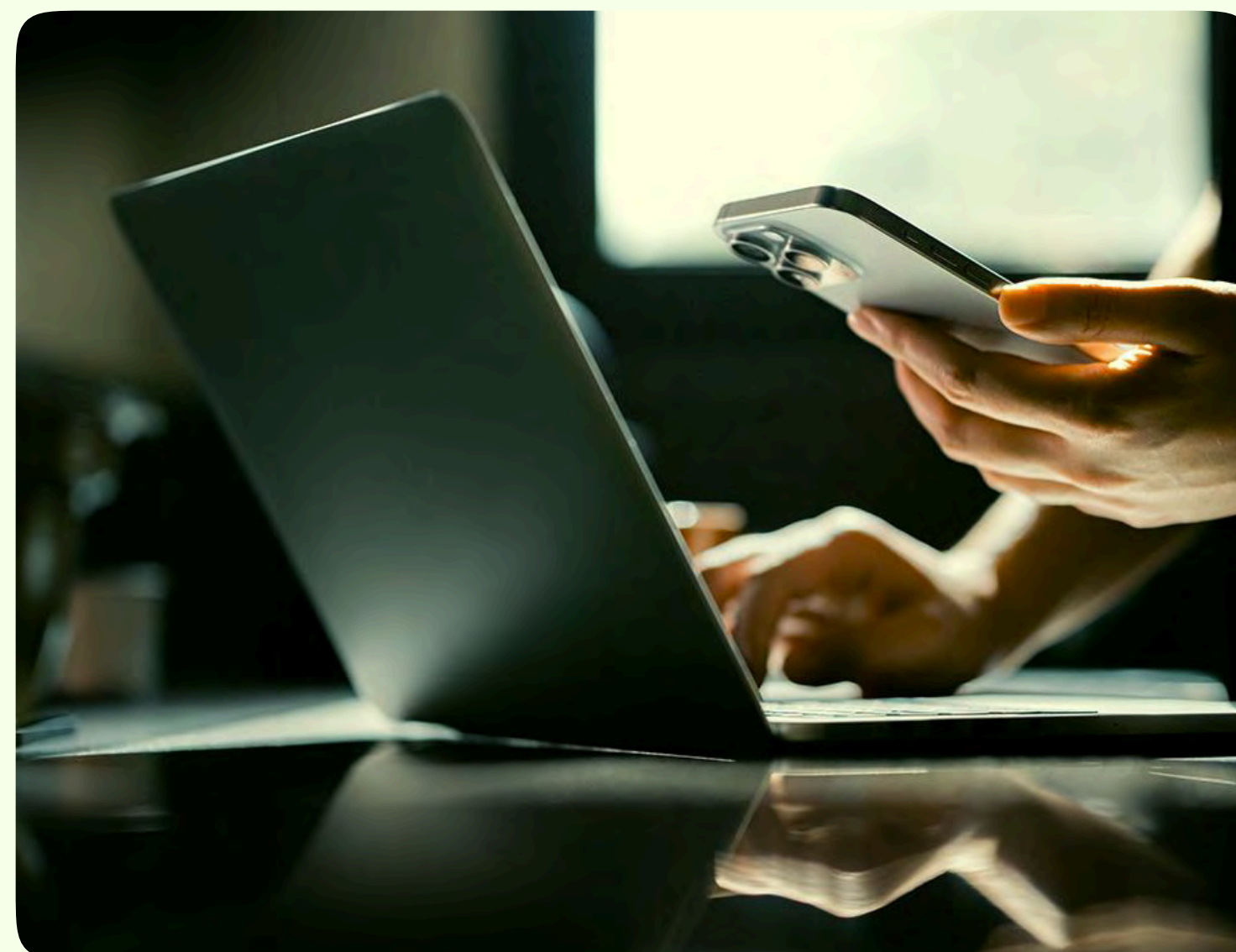
Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

**Recomendaciones futuras para las empresas**

El futuro de la confianza y la seguridad



Inserta el código de 6 dígitos  
que te enviamos vía SMS

6 3 5 6 0 6

Verificar

1

## Invertir en IA y aprendizaje automático

La inteligencia artificial es la base para una detección eficaz del fraude a gran escala. Las empresas deben priorizar las inversiones en sistemas de detección de fraude basados en IA que puedan analizar patrones de tráfico en tiempo real, identificar anomalías antes de que se conviertan en pérdidas y adaptarse continuamente a nuevas técnicas de fraude sin requerir actualizaciones manuales de reglas.

Los datos de 2025 muestran que las organizaciones que han implementado sistemas de detección impulsados por IA están identificando amenazas que los sistemas tradicionales basados en reglas no logran detectar, incluyendo técnicas de evasión mediante imágenes, campañas de bots que afectan a múltiples marcas y nuevos patrones de phishing nunca antes observados. Según lo aprendido, la IA no reemplaza la supervisión humana. Gestiona el volumen de información para que la experiencia humana pueda centrarse en las excepciones más importantes.

2

## Mejorar la autenticación multifactor

Implementar la autenticación multifactor para transacciones de alto riesgo permitirá mitigar la mayoría de los intentos de fraude desde el punto de entrada. Sin embargo, el canal a través del cual se entrega la autenticación es tan importante como la propia autenticación. Los códigos OTP por SMS, aunque son una solución universal, presentan vulnerabilidades relacionadas con el intercambio fraudulento de SIM (SIM swap) y la exposición a ataques de tráfico artificial (AIT).

Las empresas que operan en mercados de alto riesgo o que enfrentan niveles elevados de OTP sospechosos deberían evaluar la diversificación de canales como una estrategia de seguridad, no únicamente como una mejora de experiencia de usuario. Las señales a nivel de red, como la detección de intercambio de SIM (SIM Swap Detection), pueden ayudar a identificar riesgos antes de enviar un OTP, mientras que la verificación del número (Number Verification) puede añadir una capa adicional de seguridad cuando esté disponible, al confirmar la titularidad del número sin depender de un código visible. Las arquitecturas de autenticación más resistentes combinan múltiples capas: detección de señales de fraude y mecanismos automáticos de respaldo cuando los canales principales fallan.





3

## Mejorar la seguridad de las comunicaciones

Los operadores móviles deberían adoptar firewalls de SMS para proteger el tráfico sensible a nivel de infraestructura. Un firewall de SMS correctamente implementado funciona tanto como una herramienta de protección para los suscriptores como un mecanismo de recuperación de ingresos, al bloquear el tráfico de rutas grises (grey routes) que evita la facturación legítima y mantener el contenido malicioso alejado de los usuarios finales.

Los canales cifrados de extremo a extremo para las comunicaciones orientadas al cliente, especialmente para la autenticación y las notificaciones sensibles, reducen aún más la superficie de ataque disponible para los defraudadores.

Cuando está disponible, la verificación de números (Number Verification) representa una mejora significativa del proceso de OTP, ya que es resistente al phishing. Con las mejoras previstas a corto plazo en la verificación de números, se convertirá en una opción aún más sólida para las empresas y sus clientes. El enmascaramiento de números (Number Masking) protege tanto a clientes como a empleados en cualquier escenario donde personas desconocidas deban comunicarse: transporte bajo demanda, entregas, atención sanitaria y transacciones en marketplaces. La privacidad desde el diseño (Privacy by Design) es tanto un requisito regulatorio como un mecanismo estructural de prevención del fraude.



4

## Educar a los clientes sobre las amenazas

La tecnología por sí sola no puede cerrar la brecha del fraude; el comportamiento humano sigue siendo una de las vulnerabilidades más explotadas dentro de la cadena de seguridad.

La educación proactiva de los clientes genera el nivel de concienciación necesario para que los ataques de phishing, smishing e ingeniería social sean menos efectivos. Las campañas que ayudan a los clientes a identificar mensajes fraudulentos, comprender cuándo desconfiar de situaciones de urgencia y saber cómo reportar interacciones sospechosas reducen las tasas de éxito de los ataques y fortalecen la confianza en la marca, un valor que el fraude deteriora directamente.

Los datos de este informe muestran que el phishing relacionado con entregas es la única categoría que presenta una disminución año tras año, lo que indica que una mayor concienciación de los consumidores mantenida en el tiempo sí genera resultados. El mismo resultado puede alcanzarse en otras categorías de fraude mediante programas constantes de educación adaptados a cada canal de comunicación.

Hemos incorporado nuevas medidas de protección para mantener tu cuenta y tus compras más seguras. Las tácticas de fraude evolucionan rápidamente, y los métodos que funcionaban el año pasado no siempre son suficientes hoy.

Entonces, ¿qué está cambiando?

Es posible que veas elementos como códigos de acceso de un solo uso, verificaciones del dispositivo o confirmaciones rápidas de identidad. Estas medidas nos ayudan a asegurarnos de que realmente eres tú y no alguien que intenta utilizar tu cuenta o tus datos de pago.

5

## Adaptarse a la evolución de las tácticas de fraude

La prevención del fraude no debe basarse en la suposición de que los controles actuales serán suficientes en el futuro. Las tácticas de fraude evolucionan rápidamente, y las empresas que permanecen ancladas en la mentalidad de “siempre lo hemos hecho así” están más expuestas a nuevos métodos de ataque, nuevos canales y cambios en el comportamiento de los clientes.

Las organizaciones más resilientes mantienen la apertura hacia nuevas señales, nuevas tecnologías y nuevas formas de detectar riesgos con mayor anticipación.

Utiliza las herramientas disponibles actualmente, pero también planifica las capacidades que estarán disponibles en el futuro. Trabaja con socios de confianza para evaluar, desarrollar e implementar nuevas soluciones a medida que cambia el panorama de amenazas, incluyendo enfoques de inteligencia en tiempo real como Number Risk Score de Infobip, que evalúa el riesgo asociado a un número de teléfono móvil y ayuda a identificar posibles riesgos antes dentro del flujo de comunicación. Mantenerse alerta y ser adaptable suele ser el factor que diferencia a las organizaciones que evolucionan rápidamente de aquellas que se quedan atrás.





# El futuro de la confianza y la seguridad







Resumen

Introducción

El panorama global del fraude y el spam en 2026

Firewall para SMS

Inteligencia de tráfico de OTP

APIs de red

Enmascaramiento de números

Tendencias de fraude por regiones

Tendencias de fraude por industria

Recomendaciones futuras para las empresas

**El futuro de la confianza y la seguridad**

## CONCLUSIÓN

# Hacia un futuro digital seguro y confiable

Los hallazgos de este informe muestran que el fraude se está volviendo más sofisticado, más automatizado y más difícil de detectar. A medida que evolucionan los ataques impulsados por inteligencia artificial y continúan creciendo las interacciones digitales, las empresas deben adaptarse continuamente para mantenerse un paso adelante. Sin embargo, los datos también cuentan una historia más alentadora.

Las organizaciones que invierten en prevención moderna del fraude, automatización e inteligencia están mejor preparadas para proteger a sus clientes y, al mismo tiempo, ofrecer las experiencias digitales confiables que esperan. En los próximos años, la confianza será una ventaja competitiva clave, haciendo que la seguridad no sea solo una necesidad, sino un elemento diferenciador para las empresas.



Los datos de este informe confirman que el fraude es una realidad presente que evoluciona más rápido de lo que las defensas tradicionales pueden responder. Las organizaciones líderes están integrando la seguridad directamente en su infraestructura de comunicación, en lugar de tratarla como una medida secundaria.

Para las empresas de todos los sectores, la oportunidad está en proteger la confianza de los clientes y generar valor comercial mediante una mayor visibilidad, un control de tráfico más inteligente y las soluciones antifraude y de seguridad de Infobip.

A medida que los defraudadores utilizan cada vez más la inteligencia artificial para automatizar y escalar sus ataques, las organizaciones están respondiendo con detección basada en IA y protección en tiempo real que evolucionan con la misma rapidez.



**Matija Ražem**

Chief Commercial  
Telecom Officer en Infobip

## Unificar la seguridad y la interacción con los clientes mediante IA

El futuro de la comunicación digital segura pertenece a las organizaciones que consideran la seguridad como parte de su infraestructura, no como un elemento extra.

Estas organizaciones incorporan la detección de fraude en cada etapa del recorrido del cliente, autentican de forma inteligente a través de múltiples canales y métodos, protegen los datos personales desde el diseño y garantizan a sus clientes que cada interacción sea lo más segura posible. A medida que la inteligencia artificial continúa transformando las interacciones con los clientes, plataformas de orquestación como [Infobip AgentOS](#) pueden ampliar aún más este modelo.





# La ventaja de Infobip

## ALCANCE GLOBAL Y PRESENCIA LOCAL

- ✓ Conecta con +7 mil millones de personas y dispositivos
- ✓ +800 conexiones directas con operadores
- ✓ +75 oficinas en 6 continentes
- ✓ +15 canales compatibles de forma nativa

AgentOS es una plataforma nativa de inteligencia artificial (IA). Sin embargo, lo que la hace estar preparada para entornos empresariales es la base sobre la que está construida: 20 años de infraestructura que ha gestionado miles de millones de las comunicaciones con clientes más críticas del mundo.

## EXPERIENCIA EXCEPCIONAL DEL CLIENTE

- ✓ Experiencia técnica especializada
- ✓ Soluciones y consultoría de experiencia del cliente (CX)
- ✓ Gestión del éxito del cliente
- ✓ Soporte 24/7 y monitoreo de red

Una verdadera alianza. Soporte durante la implementación, gestión dedicada del éxito del cliente y capacidades de servicios profesionales que te ayudan a pasar de la compra a la puesta en producción sin los retrasos que normalmente acompañan al software empresarial.

## SOLUCIONES ESCALABLES, RÁPIDAS Y FLEXIBLES

- ✓ Tasas de entrega líderes en el mercado
- ✓ Alta velocidad y confiabilidad
- ✓ Baja latencia
- ✓ Plataforma desarrollada internamente

Cumplimiento integrado desde el diseño, no añadido posteriormente. Residencia regional de datos, plantillas de cumplimiento preconfiguradas para sectores regulados y una postura de seguridad que cumple con los requisitos de adquisición de las grandes empresas desde el primer día.

## INFRAESTRUCTURA PROPIA

- ✓ Servicios disponibles a nivel local
- ✓ Cumplimiento de las normativas locales
- ✓ Más de 40 centros de datos en todo el mundo
- ✓ SLA de disponibilidad del 99,99% (acuerdo de nivel de servicio)

Nuestra infraestructura global escala horizontalmente con facilidad, aprovechando un modelo de nube híbrida para garantizar que nunca nos quedemos sin recursos. Nuestro motor global de cumplimiento integrado se actualiza constantemente con las normativas locales más recientes de cada país y los requisitos de los operadores.



Líder en prevención del fraude en mensajería móvil 2025  
Líder consolidado en prevención de AIT 2024  
Líder consolidado en mensajería empresarial RCS 2024  
Líder consolidado en CPaaS 2024



Gartner® Magic Quadrant™  
para CPaaS 2026  
Infobip es reconocido como un líder  
POR CUARTO AÑO CONSECUTIVO



Top 25 de las empresas más  
innovadoras de Europa según  
Fortune 2026



Metrigy CPaaS MetriRank  
Infobip es nombrado como uno  
de los principales proveedores  
de CPaaS en 2023 y 2024



IDC MarketScape  
Líder CPaaS 2021, 2023 y 2025



Omdia Universe  
Líder CPaaS 2022, 2023 y 2025





One communication platform.  
Billions of conversations.