Ostorlab

Informe 2026 de seguridad de aplicaciones de banca móvil

Lo que incluyen 2686 apps bancarias de los 500 principales bancos de 64 países en Android, iOS y HarmonyOS, y lo que eso significa para el fraude.

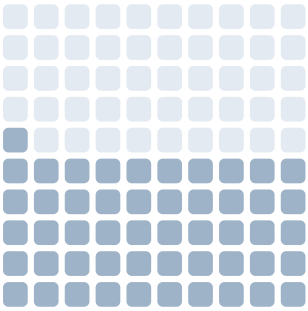


CONCLUSIÓN CLAVE

Los neobancos independientes acumulan los hallazgos más graves.

Los análisis de las apps de neobancos reciben una calificación de riesgo alto o crítico con más frecuencia que los de las apps de bancos tradicionales, 61,1 % frente a 51,2 %, y toda la diferencia procede de los neobancos independientes. Los neobancos filiales de un banco tradicional se parecen a los bancos a los que pertenecen.

51,2%

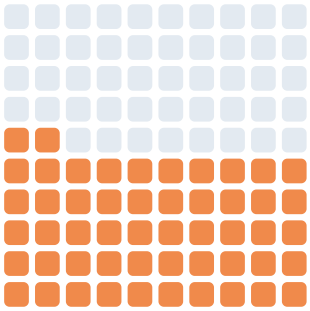


Bancos tradicionales

Banca con oficinas, minorista y corporativa

2596 APPS

52,5%

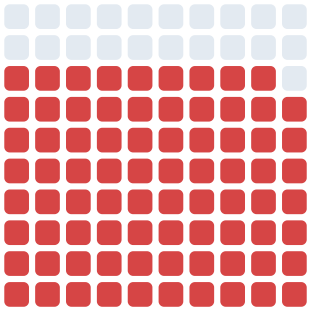


Neobancos filiales

Marcas digitales de un banco tradicional

61 APPS

79,3%



Neobancos independientes

Bancos solo digitales sin matriz tradicional

29 APPS

Qué explica la diferencia



Pero lideran en defensas modernas



FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

ÍNDICE

2686 apps, once capítulos.

Cada línea enlaza con su página.

Conclusión clave: neobancos independientes 02

Resumen 04

El informe en nueve cifras 05

01 Cómo medimos 06

2686 apps de todas las regiones 07

Tres tipos de evidencia, cinco reglas para cada cifra 08

02 Cómo se construyen las apps bancarias 09

Las apps web híbridas son las de mayor riesgo 10

Una plataforma, muchos bancos 11

Actualizadas a menudo, pensadas para teléfonos antiguos 12

Una nueva versión cada 6 a 9 semanas 13

03 Qué llevan dentro 14

Analítica en todas partes, SDK antifraude en pocas apps 15

La banca con IA aún no está en la app 16

04 Qué encontraron los análisis 17

La mitad de las apps tiene un hallazgo grave 18

Los hallazgos de código y privacidad afectan a la mayoría de las apps 19

Una de cada cinco apps embebe una credencial que debería ser secreta 20

Cuatro de cada diez apps incluyen una vulnerabilidad conocida 21

Cada plataforma falla a su manera 22

05 Autenticación y pagos 23

El código de llaves de acceso llega; las llaves de acceso, no 24

¿Menciona la web del banco a la app? 25

La biometría suele ir vinculada a una clave, pero un tercio puede eludirse 26

06 Blindaje: lo que incluyen las apps 27

Protecciones halladas en el código 28

Los SDK aportan muchos de los controles 29

Pocas apps combinan sus defensas en capas 30

07 Más allá de la app 31

Dominios bancarios: listos para lo cuántico, difíciles de alertar 32

Etiquetas de privacidad que no coinciden con la app 33

Algunos servidores bancarios responden más allá de la web 34

Uno de cada seis bancos tiene un registro público de brechas 35

Las normas que rigen a los bancos y lo que estos declaran 36

08 El panorama de amenazas 37

Cuatro de cada diez bancos están en la lista de un troyano 38

2026: los atacantes vuelven la propia app del banco en su contra 39

¿Notaría un banco que su app ha sido sustituida? 40

Adónde va el dinero 41

09 Por región, tipo de banco y país 42

Ninguna región lo tiene todo 43

Resultados por país 44

Las apps bancarias más seguras por región 45

10 Casos de estudio 46

CyberDakait: siete troyanos, una llamada 47

WindRelay: un préstamo desde la propia app de la víctima 48

Hirudo: el troyano que sustituye su app bancaria 49

Dentro de la copia, cualquier control puede falsearse 50

La clave de API de Google que se convirtió en una credencial de IA 51

11 Próximos pasos 52

Qué deben hacer los bancos en 2026: las 10 prioridades 52

A Definiciones y notas sobre los datos 53

Los controles que frenan el fraude moderno siguen siendo los menos frecuentes.

Este año analizamos 2686 apps de banca móvil de los 500 principales bancos de 64 países. Los bancos actualizan a menudo y la mayoría de las apps incluye lo básico. Las protecciones que importan frente a los ataques actuales, como las llaves de acceso, la atestación y el blindaje en tiempo de ejecución, siguen presentes solo en una minoría de apps.

La mitad de las apps tiene un hallazgo grave

El 51,5 % de las apps tiene al menos un hallazgo alto o crítico en nuestro análisis automatizado. Solo el 11,8 % no tiene nada por encima de bajo. Las causas más frecuentes son las credenciales embebidas en la app (20,3 % sin contar las claves de API de Google) y los componentes con vulnerabilidades conocidas (41,1 %).

La autenticación fuerte aún es incipiente

Solo el 4,9 % de las apps integra una API de llaves de acceso, y el 20,2 % usa atestación de app o de dispositivo. En Android, el 35,1 % tiene un flujo biométrico que nuestro escáner pudo eludir, aunque la mayoría de las apps que vinculan la biometría lo hacen a una clave.

Los atacantes apuntan ya a la propia app

Las apps de 192 de los 500 principales bancos figuran en listas públicas de objetivos de troyanos bancarios. En 2026, campañas como Hirudo y Gigabud fueron más allá y sustituyeron o clonaron apps bancarias auténticas en el teléfono de la víctima. En el Reino Unido, la banca móvil concentró el 52 % de las pérdidas por estafas de transferencia autorizada en 2025.

El blindaje es frecuente por partes, raro en conjunto

En Android, el 69,9 % de las apps detecta el root, pero solo el 26,9 % incluye un producto de blindaje comercial o de plataforma. Nuestros datos muestran lo que contienen las apps, no cómo resisten; eso exige pruebas en dispositivos.

TRES CONCLUSIONES DE LOS ANÁLISIS

51,5%



de las apps tienen al menos un hallazgo alto o crítico

1384 de 2686 apps

35,1%



de las apps Android tienen un flujo biométrico que nuestro escáner pudo eludir

apps Android

4,9%



de las apps integran una API de llaves de acceso, el control que inutiliza las contraseñas robadas por phishing

El informe en nueve cifras.

COMPONENTES 01

41,1%

de las apps incluyen un componente con una vulnerabilidad conocida

1103 de 2686 apps

Capítulo 04 · página 17 →

CLAVES SECRETAS 02

20,3%

de las apps embeben secretos como claves de API, tokens de acceso o claves privadas

544 de 2686 apps; sin contar las claves de API de Google

Capítulo 04 · página 17 →

TELÉFONOS ANTIGUOS 03

96%

de las apps se instalan en versiones que ya no reciben parches de seguridad

Android 99 % · HarmonyOS 100 % · iOS 72 %

Capítulo 02 · página 12 →

ATESTACIÓN 04

20,2%

de las apps usan atestación de app o de dispositivo

525 de 2602 apps con código legible

Capítulo 05 · página 23 →

BLINDAJE 05

26,9%

de las apps Android incluyen un producto de blindaje en tiempo de ejecución

Productos comerciales o de plataforma, apps Android

Capítulo 06 · página 27 →

IA 06

2 apps

hacen referencia a una API de modelo de lenguaje (LLM); ninguna incluye un SDK de LLM, mientras que el 28,3 % usa ML en el propio dispositivo

De 2686 apps; destacan los modelos de códigos de barras, texto y rostros

Capítulo 03 · página 14 →

TROYANOS 07

38%

de los bancos tienen apps en listas públicas de objetivos de troyanos bancarios

192 de los 500 principales bancos; listas publicadas sobre todo de 2021 a 2023

Capítulo 08 · página 37 →

POSCUÁNTICO 08

71%

de los hosts web bancarios accesibles negocian TLS poscuántico

732 de 1038 negociaciones TLS completadas

Capítulo 07 · página 31 →

PÉRDIDAS POR ESTAFAS 09

52%

de las pérdidas por estafas en el Reino Unido en 2025 pasaron por la banca móvil

301,8 M£ de 576,4 M£ en estafas de transferencia autorizada (UK Finance)

Capítulo 08 · página 37 →

CAPÍTULO 01

01

Cómo medimos

Descargamos 2686 apps bancarias de los 500 principales bancos de 64 países y sometimos cada una al análisis de seguridad automatizado de Ostorlab, en Android, iOS y HarmonyOS.



En pantalla: la muestra por país y región.

2686

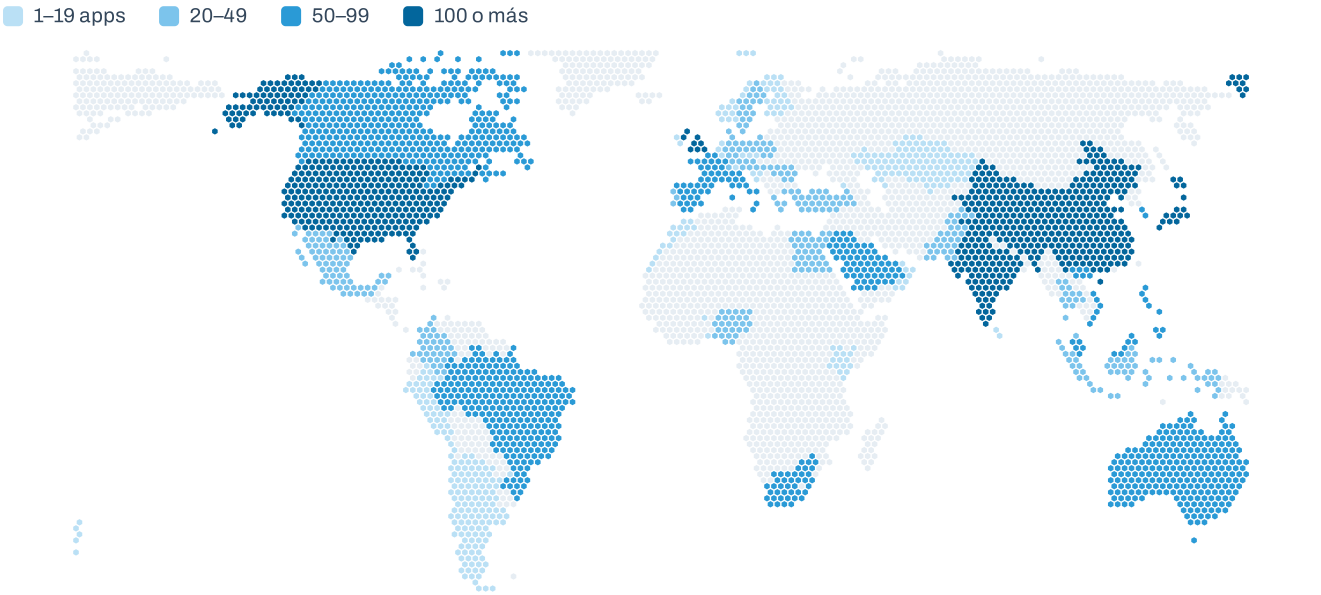
apps de los 500 principales bancos de 64 países

2686 apps de todas las regiones.

La muestra abarca 2686 apps de los 500 principales bancos, incluidos 29 de los bancos de importancia sistémica mundial, en Android, iOS y HarmonyOS.

Bancos de 64 países, en todos los continentes

FIG. 1,1

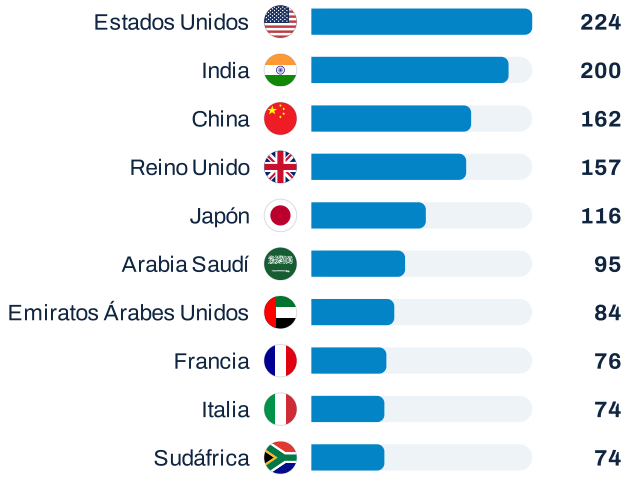


Apps analizadas por país, según el mercado de origen del banco. Se recopilaron 2841 fichas de tienda; 155 no pudieron descargarse.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Los diez mayores mercados

FIG. 1,2

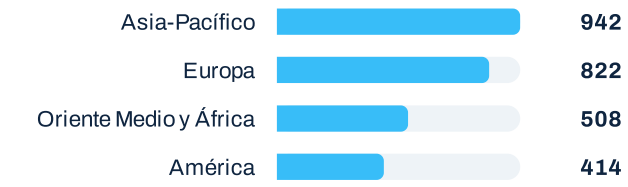


Número de apps, por país de origen del banco.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Asia-Pacífico es la mayor región

FIG. 1,3



Número de apps, por región de origen del banco.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Tres tipos de evidencia, cinco reglas para cada cifra.

Cada cifra de este informe procede del análisis de las apps realizado por Ostorlab, y todas siguen las mismas cinco reglas, para que los gráficos, el texto y los pies de figura concuerden.

Inventario de la app

Recoge con qué está construida cada app: framework, SDK, permisos, protecciones y los hosts con los que se comunica. Las 2686 apps.

Análisis de seguridad automatizado

Las reglas del escáner de Ostorlab detectan vulnerabilidades, califican su severidad y las asocian a OWASP MASVS. Las reglas varían según la plataforma. Las 2686 apps.

Señales de controles

Dieciséis comprobaciones de controles de autenticación, pago y privacidad, cada una con la evidencia de código que la activó. Las 2686 apps.

CÓMO LEER CADA CIFRA

01 **Cada porcentaje indica su denominador**

Cada porcentaje indica sobre qué apps se midió, en el pie bajo el gráfico.

02 **Las reglas de una plataforma se quedan en su plataforma**

Una regla que solo existe en Android se expresa como porcentaje de las apps Android, nunca del total de apps.

03 **Lo desconocido se cuenta, no se supone**

El código empaquetado o ilegible se excluye del denominador de cada control, y se indica cuánto se ha excluido.

04 **Las claves de API de Google se tratan aparte**

Google prevé que vayan en las apps, así que la cifra principal de credenciales las excluye.

05 **No se nombra a ningún banco**

La evidencia procede de apps reales, mostradas sin el nombre del banco y con todos los secretos enmascarados.

Cómo interpretar las cifras

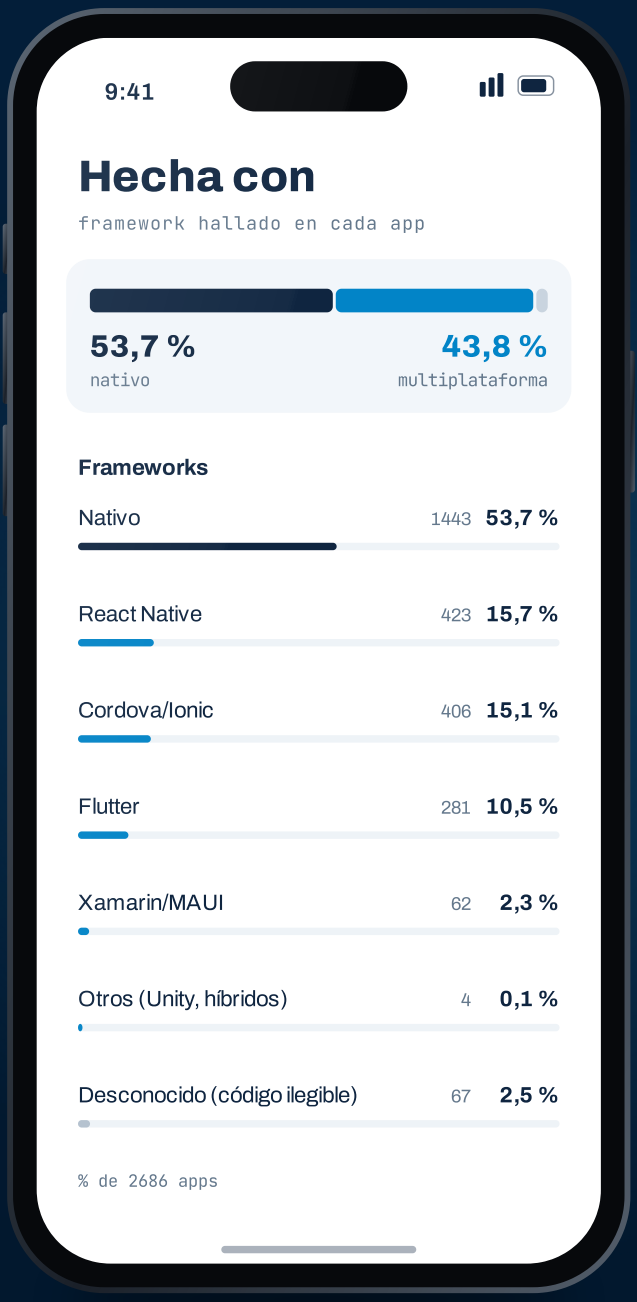
Un hallazgo significa que nuestro escáner encontró una coincidencia con una regla en el paquete publicado. Es evidencia de que existe un problema, no prueba de que sea explotable en producción. La severidad sigue las calificaciones del escáner: crítico, alto, medio y bajo. El escáner usa además dos calificaciones inferiores. «Potencial» señala un patrón que puede ser un fallo real pero que debe confirmar una persona, como una cadena con forma de clave. «Refuerzo» señala una salvaguarda ausente. Cada app se califica por su hallazgo crítico, alto, medio o bajo más grave; los hallazgos «potencial» y «refuerzo» no cambian esa calificación. Cuando un gráfico los cuenta, lo indica.

CAPÍTULO 02

02

Cómo se construyen las apps bancarias

La mayoría de los bancos sigue desarrollando en nativo, pero cuatro de cada diez apps funcionan ya sobre un framework multiplataforma. La elección se refleja en los resultados de seguridad.



En pantalla: el framework hallado en cada app.

43,8%

de las apps están construidas sobre un framework multiplataforma

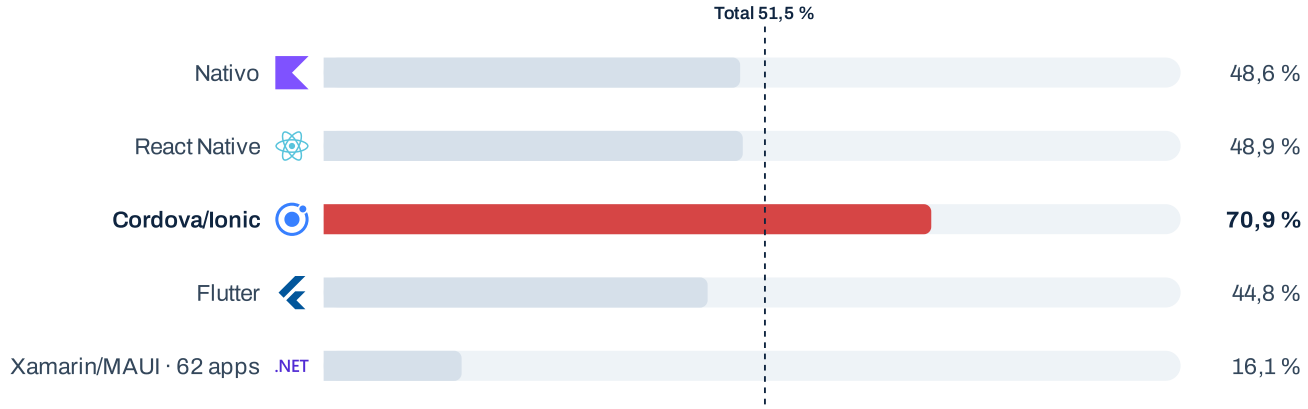
1176 de 2686 apps

Las apps web híbridas son las de mayor riesgo.

Las apps Cordova e Ionic empaquetan una app web dentro de un contenedor nativo. Suponen el 15,1 % de la muestra, y el 70,9 % de ellas tiene un hallazgo alto o crítico, frente al 48,6 % de las apps nativas.

El 70,9 % de las apps Cordova e Ionic tiene un hallazgo grave

FIG. 2,1

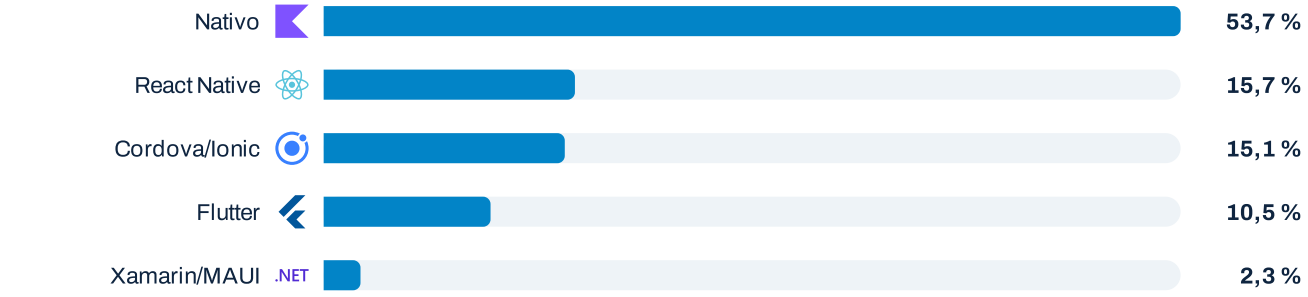


Porcentaje de apps de cada framework con al menos un hallazgo alto o crítico. Línea discontinua: las 2686 apps.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

La mayoría de las apps bancarias sigue siendo nativa

FIG. 2,2



Porcentaje de 2686 apps por framework; no se muestran 67 con código ilegible.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Las apps Cordova e Ionic también encabezan los componentes vulnerables (72,2 %), sobre todo bibliotecas JavaScript obsoletas incluidas en la capa web.

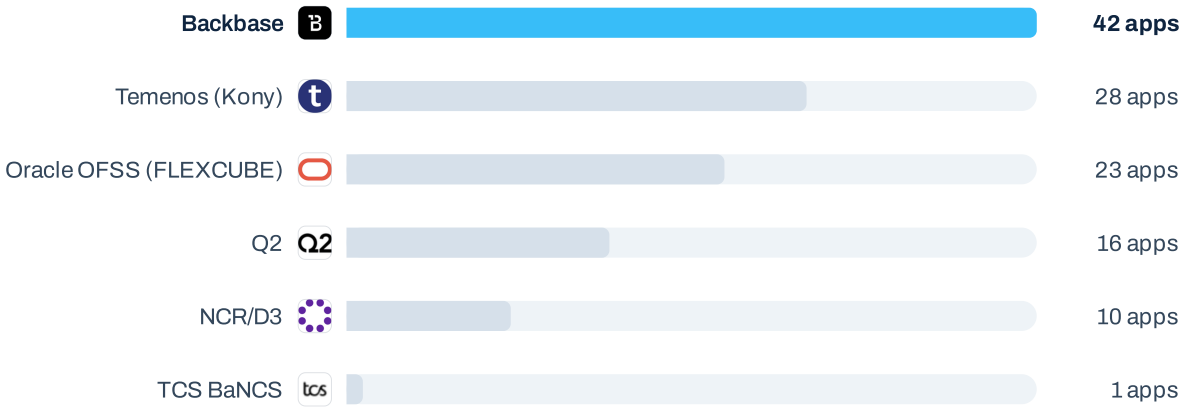
No hay una diferencia clara entre las apps nativas (48,6 %), React Native (48,9 %) y Flutter (44,8 %). Las apps Xamarin y MAUI salen mejor paradas, pero son un grupo pequeño de 62 apps y son las que más a menudo embeben credenciales (43,5 %).

Una plataforma, muchos bancos.

Muchos bancos no escriben su app desde cero: licencian una plataforma de banca digital y le ponen su marca. 120 apps de la muestra llevan la firma de código de una de 6 plataformas de este tipo.

Backbase es la plataforma bancaria más detectada

FIG. 2,3



Número de apps. 120 de 2602 apps coinciden con una firma de plataforma conocida. Una coincidencia requiere código de plataforma reconocible, por lo que estas cifras son un mínimo.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

> **Cuando una plataforma es compartida, una vulnerabilidad en ella puede alcanzar a todos los bancos que la usan.**

Por qué importa

Un fallo en el código compartido de una plataforma es un fallo en todas las apps construidas sobre ella, y la corrección depende de la versión del proveedor y, después, de que cada banco la publique. Una sola divulgación puede exponer a muchos bancos a la vez.

Buenas prácticas

Pida al proveedor de la plataforma una lista de materiales de software, los resultados de sus pruebas de seguridad y un plazo de parcheo acordado. Siga los avisos del proveedor tan de cerca como los suyos propios.

Actualizadas a menudo, pensadas para teléfonos antiguos.

Los bancos mantienen sus apps al día con la plataforma: el 72,1 % de las apps Android apunta a la API de Android más reciente. Pero en todas las plataformas, la mayoría de las apps sigue instalándose en versiones del sistema operativo que ya no reciben parches de seguridad.

En todas las plataformas, la mayoría de las apps se instala en versiones sin parches

FIG. 2,4



Porcentaje de apps de cada plataforma con una versión mínima de SO legible. Una app cuenta cuando la versión mínima de SO que declara es anterior a la versión más antigua que aún recibe parches de seguridad (Android 14, iOS 18; las apps HarmonyOS declaran una versión de Android). Esto muestra lo que la app permite, no lo que usan los clientes.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Dar soporte a teléfonos antiguos es una decisión de negocio: los clientes los conservan. El riesgo es que la app se ejecute en un sistema con fallos conocidos sin parchear. Solo el 0,5 % de las apps Android rechaza las versiones sin parches; en iOS, el 28,5 % exige iOS 18 o posterior. Los bancos pueden comprobar el nivel de parches al iniciar sesión y limitar las acciones de alto riesgo en los dispositivos que ya no reciben actualizaciones.

Versión más antigua en la que puede instalarse cada app

FIG. 2,5

Android y HarmonyOS · versión de Android

	Android	HarmonyOS
4 o anterior	0,8 %	4,0 %
5	4,4 %	12,8 %
6	5,3 %	7,8 %
7	17,4 %	24,3 %
8	19,5 %	19,5 %
9	13,1 %	13,0 %
10	16,5 %	12,4 %
11	7,0 %	3,4 %
12	12,8 %	2,9 %
13	2,7 %	0,0 %
14 o posterior	0,5 %	0,0 %

iOS · versión de iOS

	iOS
11 o anterior	1,8 %
12	2,1 %
13	5,0 %
14	6,5 %
15	27,0 %
16	23,1 %
17	5,9 %
18 o posterior	28,5 %

Porcentaje de apps de cada plataforma según la versión más antigua en la que se instalan. Cada barra corresponde exactamente a esa versión; una app así se instala también en todas las posteriores. Android 14 e iOS 18 son las versiones más antiguas que aún reciben parches.

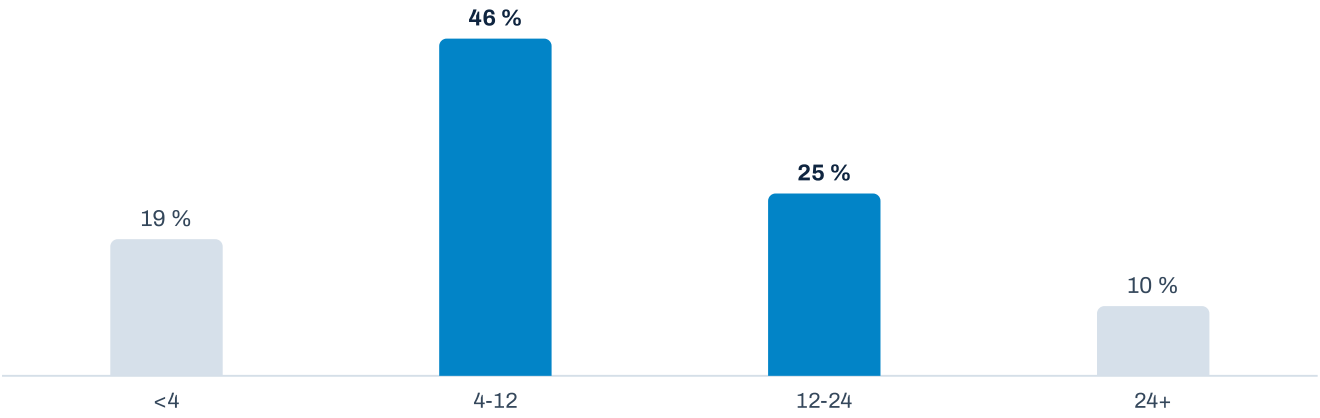
FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Una nueva versión cada 6 a 9 semanas.

La app Android mediana publica al menos 8,9 versiones al año (reconstruidas a partir de las reseñas de Google Play) y la app iOS mediana, 6,0 (historial de versiones de App Store). La tienda de HarmonyOS solo muestra la versión actual, por lo que HarmonyOS no pudo medirse. Publicar a menudo es una fortaleza: así llegan a los clientes las correcciones de los hallazgos de este informe.

La mayoría de las apps publica entre 4 y 24 versiones al año

FIG. 2,6



Porcentaje de apps Android con un historial de versiones reconstruido a partir de las reseñas de Google Play, por versiones al año; mediana 8,9, un mínimo, porque se pierden las versiones que nadie reseñó. iOS: mediana 6,0, según el historial de versiones de App Store.

FUENTE Fichas y reseñas de Google Play y App Store, recopiladas para este informe.

75,1 %
de las apps Android con fecha de actualización en Google Play se actualizaron en los últimos 90 días

6,8 %
no se actualizaron en un año

3,8 mil M
instalaciones en Google Play del conjunto de apps Android, como mínimo

Tamaño

El tamaño de descarga mediano es de 68 MB en Android, 38 MB en iOS y 129 MB en HarmonyOS. La mitad de las bibliotecas nativas de estas apps procede de SDK de terceros conocidos, y solo el 4 % puede atribuirse al propio banco. El código de terceros es el tema del siguiente capítulo.

Versiones frecuentes, componentes antiguos

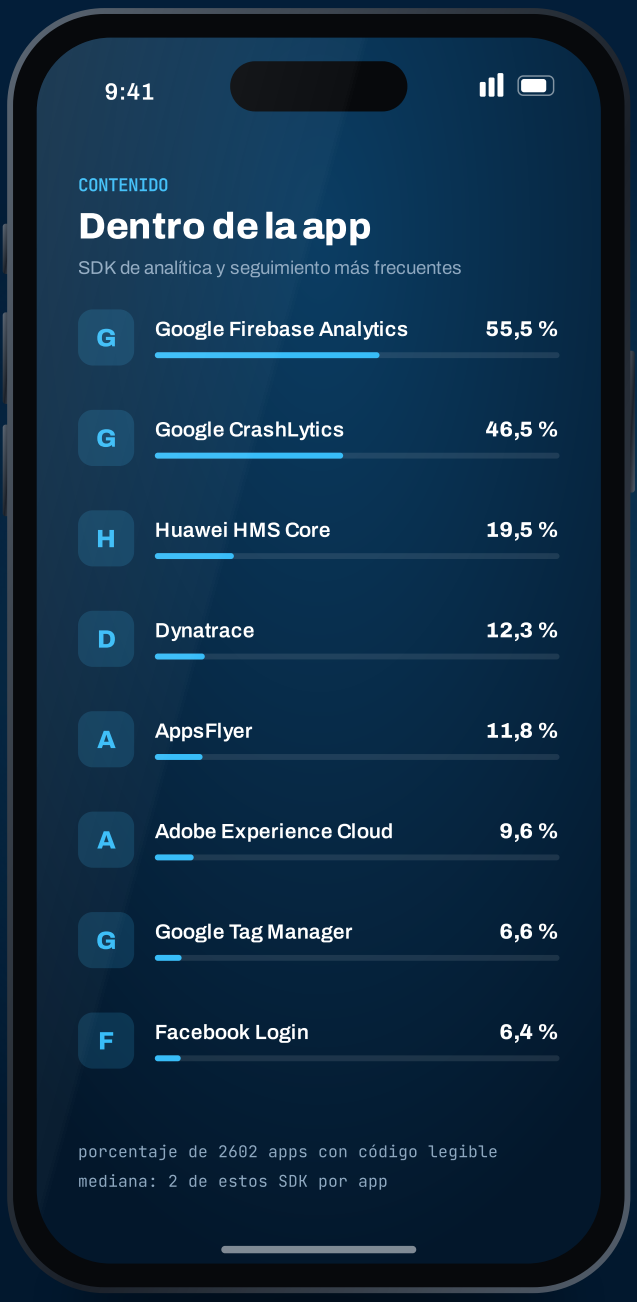
Publicar a menudo no mantiene al día todas las piezas. Como muestra el capítulo 4, el 41,1 % de las apps sigue incluyendo un componente con una vulnerabilidad conocida.

CAPÍTULO 03

03

Qué llevan dentro

Una app bancaria es, en su mayor parte, código ajeno: analítica, informes de fallos, detección de fraude, mapas, escáneres. Cada SDK trae sus propios flujos de datos y sus propias vulnerabilidades.



En pantalla: los SDK de analítica y seguimiento más frecuentes.

80,6%

de las apps con código legible incluyen al menos un SDK de analítica o seguimiento

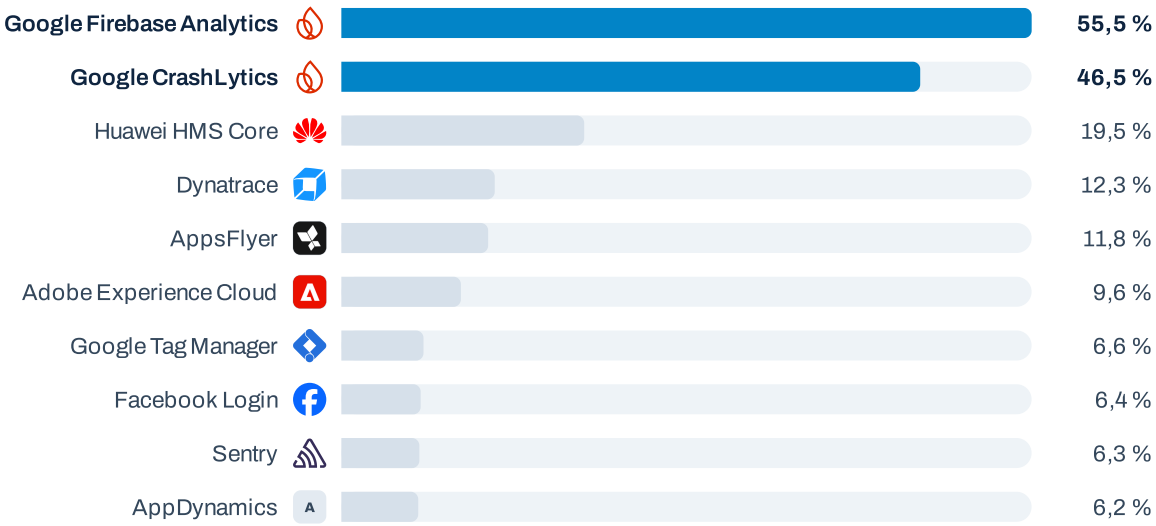
2096 de 2602 apps

Analítica en todas partes, SDK antifraude en pocas apps.

Firebase Analytics de Google aparece en el 55,5 % de las apps. Los SDK especializados en fraude y riesgo del dispositivo, que los bancos usan para detectar en tiempo real el robo de cuentas, aparecen en el 12,1 %.

Firebase Analytics y Crashlytics de Google encabezan los rastreadores

FIG. 3,1

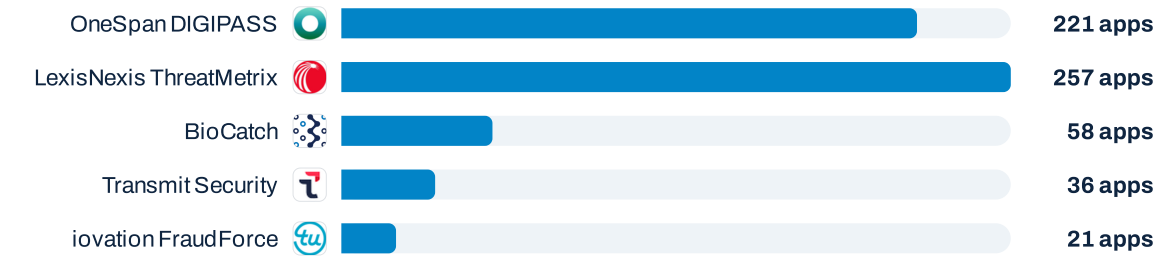


Porcentaje de 2602 apps con código legible. Firmas de rastreadores de la base de datos de Exodus Privacy. Huawei HMS Core aparece en el 64 % de las apps HarmonyOS; abarca los servicios de notificaciones push, ubicación y analítica de Huawei.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Los SDK de seguridad especializados llegan a pocas apps

FIG. 3,2



Número de apps. SDK de autenticación: 9,3 % de las apps. SDK de fraude y riesgo del dispositivo: 12,1 %.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

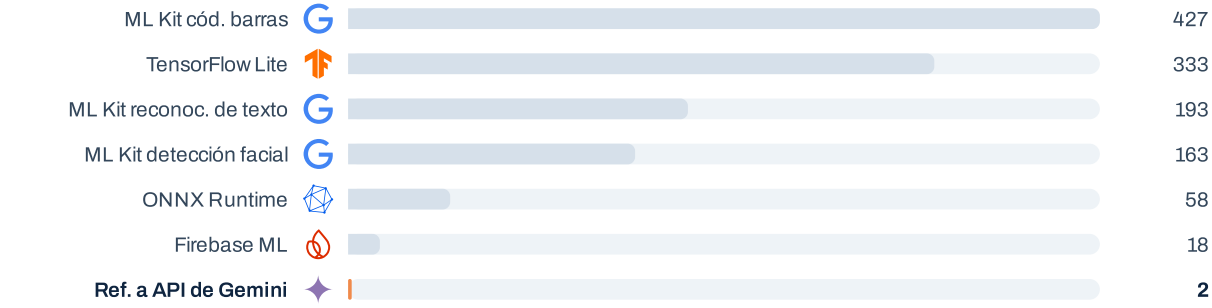
Los SDK especializados se concentran en las apps iOS: el 35,3 % de las apps iOS incluye un SDK de fraude o de riesgo del dispositivo, frente al 8,8 % en Android. Varios proveedores dan servicio a muchos bancos, así que su seguridad importa mucho más allá de una sola app.

La banca con IA aún no está en la app.

El 28,3 % de las apps incluye aprendizaje automático en el dispositivo, casi siempre para leer códigos de barras, documentos y rostros. Ninguna app incluye un SDK de modelo de lenguaje de gran tamaño: 2 de 2686 apps hacen referencia a una API de LLM, y no encontramos claves de proveedores de IA embebidas en ninguna app.

El ML en el dispositivo lee códigos de barras, texto y rostros

FIG. 3,3

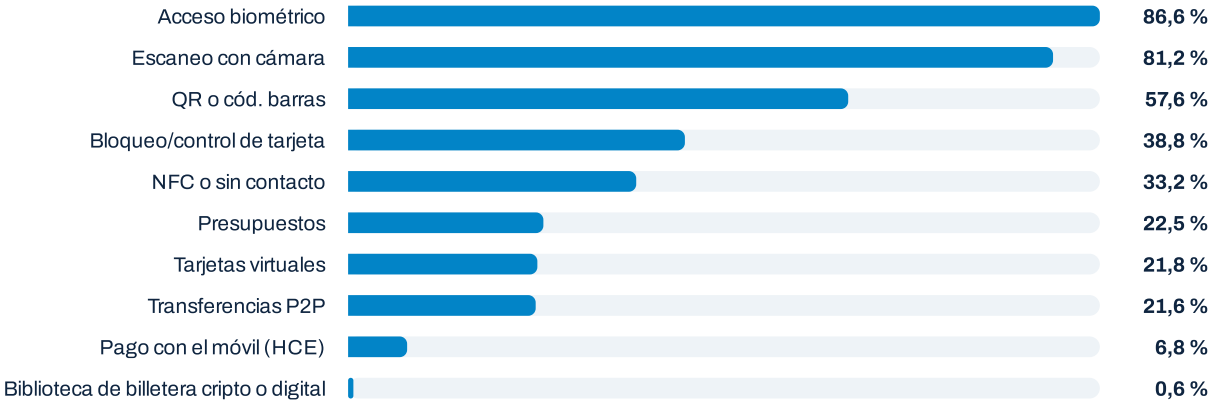


Número de apps. Referencia a la API de Gemini: la app nombra el endpoint de la API de Gemini; ninguna app incluye un SDK de LLM. Las funciones de LLM pueden ejecutarse por completo en los servidores del banco y no aparecerían en la app.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

El acceso biométrico y el escaneo con cámara son casi universales

FIG. 3,4



Porcentaje de 2686 apps. Detectado a partir del código, los recursos y los permisos; una función presente en el código puede estar desactivada. Biblioteca de billetera cripto o de moneda digital: se cuenta cuando el código de la app incluye una biblioteca de billetera o de blockchain; no indica que la app ofrezca compraventa de criptomonedas.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Las apps con un SDK de chatbot o asistente virtual embeben credenciales con más frecuencia

FIG. 3,5



Porcentaje de apps con al menos una credencial embebida, sin contar las claves de API de Google. Un SDK de chatbot es una biblioteca de chatbot o asistente virtual de un proveedor, como Dialogflow, Kore.ai, Kasisto o Watson Assistant, no un modelo de lenguaje de gran tamaño; solo 2 apps nombran la API de Gemini, y ninguna de ellas incluye un SDK de chatbot. Los bancos más grandes suelen tener uno e incluyen más SDK: una correlación, no una causa.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

CAPÍTULO 04

04

Qué encontraron los análisis

El análisis automatizado de Ostorlab encontró al menos un problema alto o crítico en la mitad de las apps. Encabezan la lista las credenciales embebidas y los componentes obsoletos, seguidos de problemas propios de cada plataforma.



En pantalla: el informe de análisis de una app real de la muestra.

18,4%

de las apps tienen al menos un hallazgo crítico

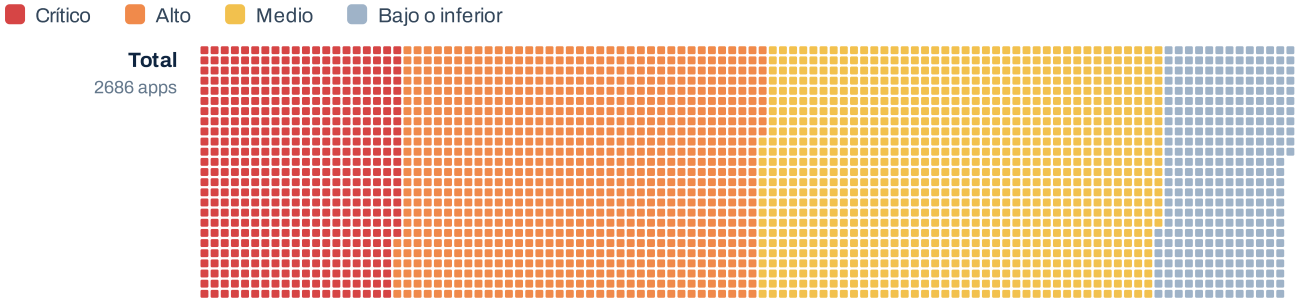
494 de 2686 apps

La mitad de las apps tiene un hallazgo grave.

Calificamos cada app por su hallazgo más grave. En Android, el 54,2 % tiene al menos un problema alto o crítico; en iOS, el 36,2 %. Las apps HarmonyOS son las que más hallazgos críticos tienen, un 31,6 %, debido a los componentes obsoletos.

Cada una de las 2686 apps, por su hallazgo más grave

FIG. 4,1

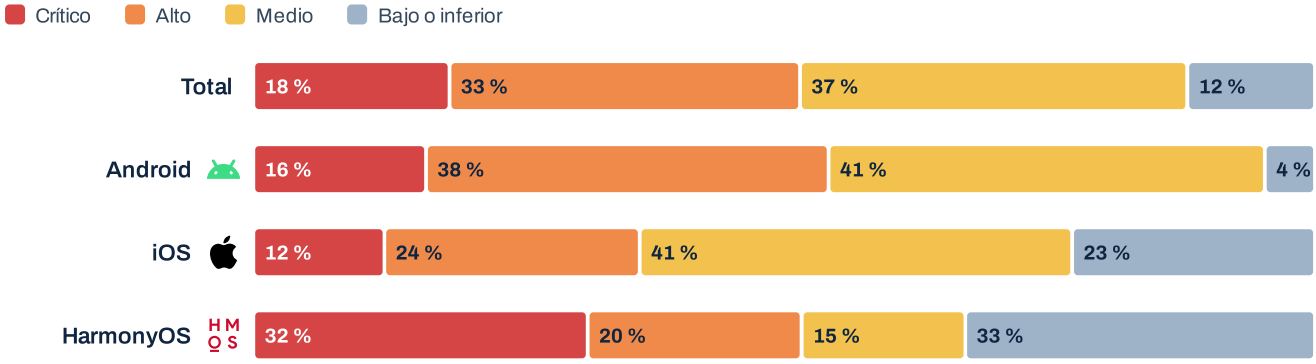


Un cuadrado por app, ordenados por severidad. «Bajo o inferior» incluye las apps cuyo peor hallazgo es bajo, «potencial» o «refuerzo», y las apps sin hallazgos.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Las apps HarmonyOS tienen más hallazgos críticos

FIG. 4,2



Porcentaje de apps según su hallazgo más grave. Las 2686 apps. «Bajo o inferior» incluye las apps cuyo peor hallazgo es bajo, «potencial» o «refuerzo», y las apps sin hallazgos. La mayor proporción de «bajo o inferior» en iOS y HarmonyOS se debe en parte a que el escáner tiene menos reglas en esas plataformas.

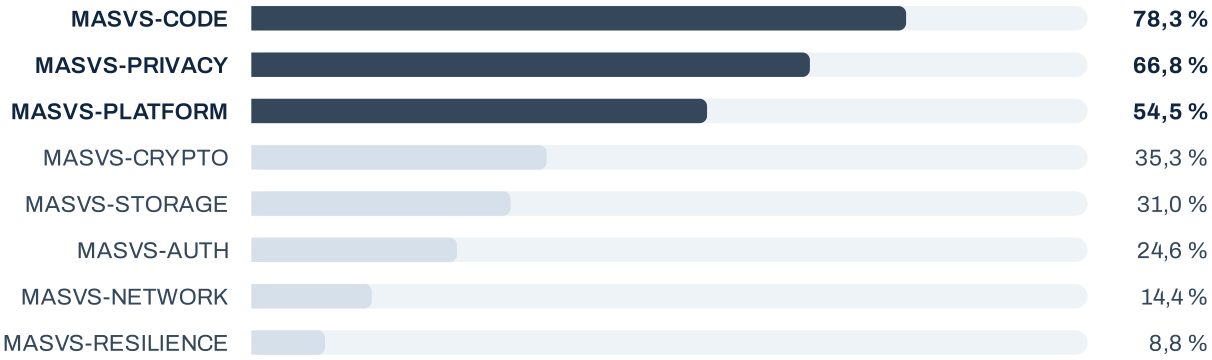
FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Los hallazgos de código y privacidad afectan a la mayoría de las apps.

La mayoría de los hallazgos se asocia a un grupo de controles de OWASP MASVS, el estándar del sector para la seguridad de apps móviles. Contando los hallazgos críticos, altos, medios y bajos, los de código aparecen en el 78,3 % de las apps y los de privacidad en el 66,8 %. Las apps iOS y HarmonyOS no presentan hallazgos de criptografía ni de autenticación, lo que reduce las cifras de esos grupos.

Porcentaje de apps con un hallazgo en cada grupo de controles de OWASP MASVS

FIG. 4,3



Porcentaje de 2686 apps con al menos un hallazgo crítico, alto, medio o bajo en cada grupo. Se excluyen los hallazgos «potencial» y «refuerzo». El 15 % de los hallazgos de Android no se asocia a ningún grupo.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.



Análisis real de una app de la muestra

UNA APP, TAL COMO LA PRESENTA EL ESCÁNER

766 hallazgos, una calificación

Esta app Android de la muestra tiene 2 hallazgos críticos, 2 altos, 757 medios y 5 bajos. Como todas las apps de este informe, se califica por su peor hallazgo: **crítico**.

Una regla puede activarse muchas veces en una misma app. La cifra de hallazgos medios es alta porque una sola regla de serialización coincidió con cientos de puntos de llamada; sigue siendo un único problema que corregir.

El escáner también notificó 98 elementos «potencial» y 2 «refuerzo». «Potencial» señala un patrón que puede ser un fallo real pero que debe confirmar una persona; «refuerzo» señala una salvaguarda ausente. Ninguno de los dos cambia la calificación de la app.

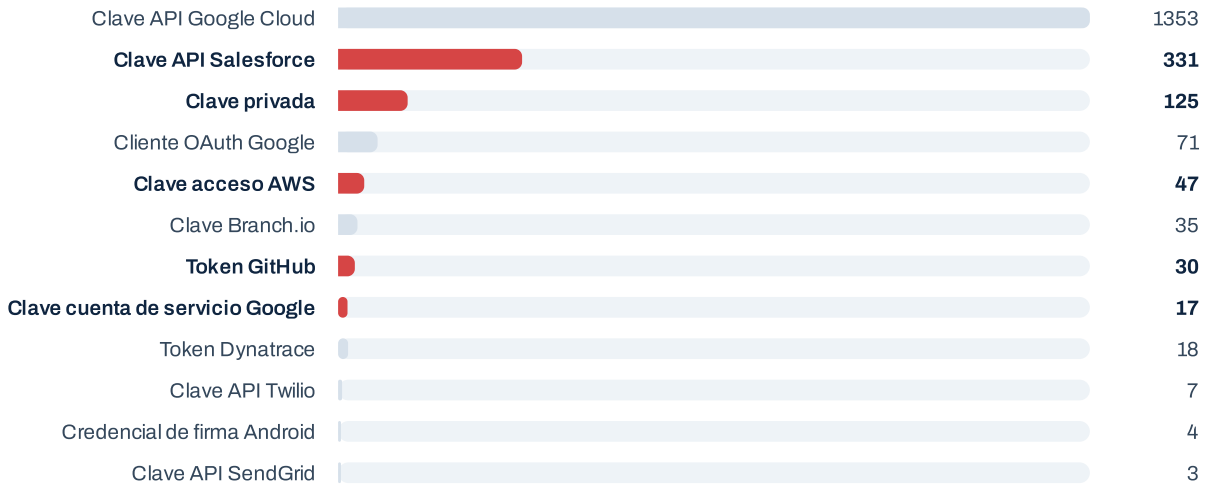
MASVS-AUTH-2 · MASVS-CODE-1 · MASVS-CODE-3 · MASVS-CODE-4 · MASVS-NETWORK-1 · MASVS-PRIVACY-1 · MASVS-PRIVACY-3 · MASVS-PRIVACY-4 · MASVS-STORAGE-1 · MASVS-STORAGE-2

Una de cada cinco apps embebe una credencial que debería ser secreta.

El 59,8 % de las apps contiene al menos una credencial con un formato reconocible. La mayoría son claves de API de Google, que Google concibe para ir dentro de las apps: identifican un proyecto para servicios como Maps y Firebase, y las protegen las restricciones configuradas en el proyecto en la nube (la firma de la app, las API autorizadas), no el secreto. No comprobamos si alguna clave está restringida. Dejándolas aparte, el 20,3 % de las apps sigue incluyendo claves privadas, claves de servicios en la nube y tokens de acceso (Android 18 %, iOS 21 %, HarmonyOS 28 %).

Tras las claves de API de Google, destacan las de Salesforce y las claves privadas

FIG. 4,4



Número de apps en las que las reglas de credenciales del escáner señalaron cada tipo; una app puede contener varios. Una búsqueda en todo el paquete, un método distinto, encuentra una clave de API de Google en el 80 % de las apps Android, el 71 % de las apps HarmonyOS y el 31 % de las apps iOS (página 51).

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.



De un análisis real de una app de la muestra; valores enmascarados

Cualquiera puede descargar una app bancaria y leer lo que contiene.

EL PAQUETE DE UNA APP

Esta app Android incluye 4 tipos de posibles secretos, entre ellos una clave de API de Google, un DSN de Sentry, una dirección de base de datos de Firebase y tokens firmados. Cualquiera que descargue la app puede leerlos.

Una clave de API de Google puede obtener nuevos accesos después de publicada la app: véase el caso de estudio de la página 51.

Buenas prácticas

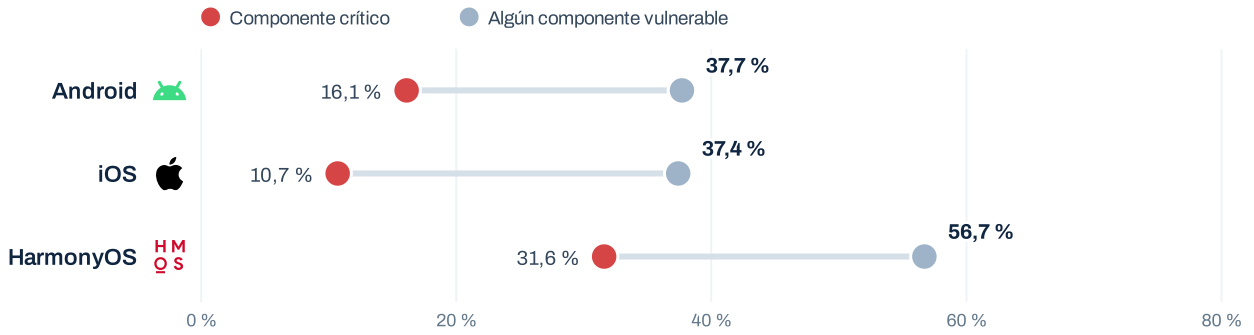
Mantenga los secretos en el servidor y emita tokens de corta duración para la app. Cuando una clave deba ir en la app, como en el caso de Google Maps, restrínjala a la firma de la app y a las API que necesita, y supervise su uso.

Cuatro de cada diez apps incluyen una vulnerabilidad conocida.

El 41,1 % de las apps incluye un componente de terceros con una vulnerabilidad publicada, y el 18,2 % uno calificado como crítico. Las apps HarmonyOS salen peor paradas.

Las apps HarmonyOS incluyen más componentes vulnerables

FIG. 4,5

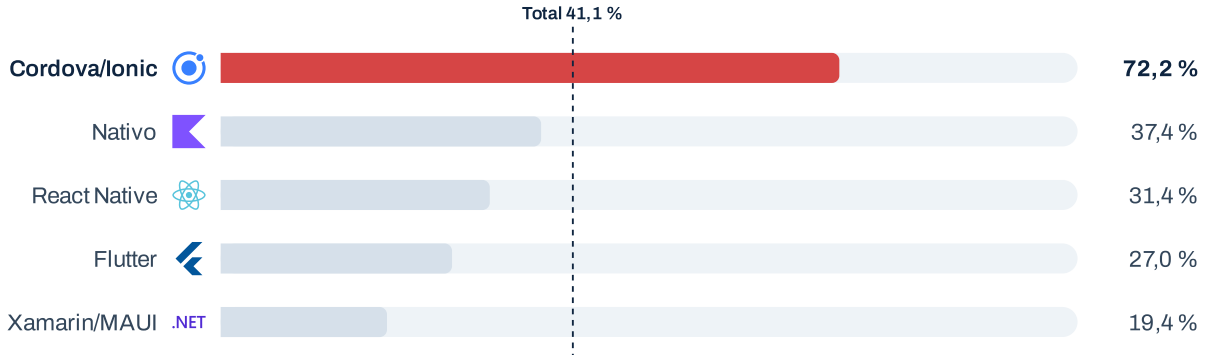


Porcentaje de apps de cada plataforma. La etiqueta indica el porcentaje con algún componente vulnerable.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

El 72,2 % de las apps Cordova e Ionic incluye un componente vulnerable

FIG. 4,6



Porcentaje de apps de cada framework. Línea discontinua: las 2686 apps.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Por qué persiste

Unos componentes arrastran a otros. Un banco puede actualizar su propio código cada mes y seguir publicando una biblioteca de hace años dentro de un SDK que no controla.

Buenas prácticas

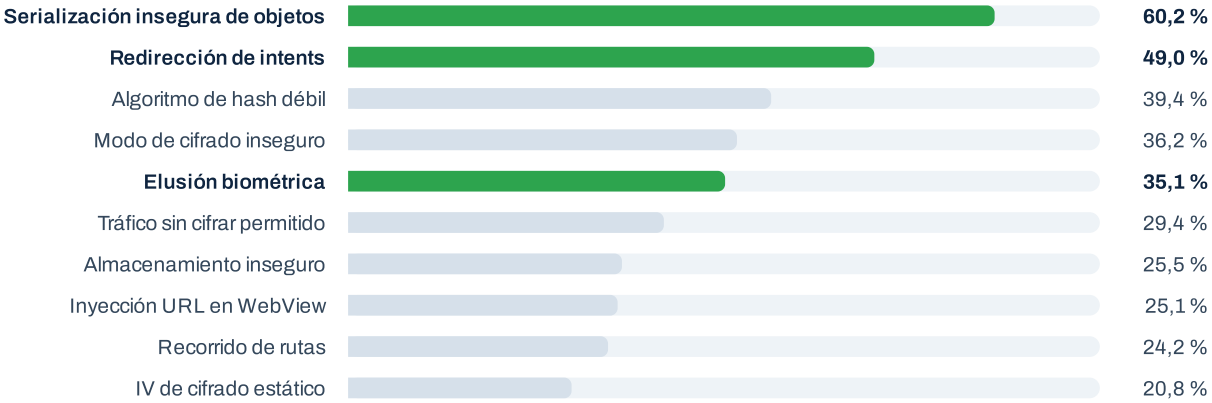
Mantenga una lista de materiales de software para cada versión, contraste con ella los avisos de seguridad y fije un plazo para corregir los componentes críticos. Exija lo mismo a los proveedores de SDK.

Cada plataforma falla a su manera.

Muchas reglas de análisis existen solo para una plataforma, así que comparamos las apps dentro de cada plataforma. En Android dominan los problemas a nivel de código. En iOS, los principales problemas son de configuración. En HarmonyOS, destacan los componentes antiguos y el código web.

Android: destacan la serialización y la redirección de intents

FIG. 4,7



Porcentaje de apps Android. Reglas solo de Android.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

iOS: destacan los problemas de configuración

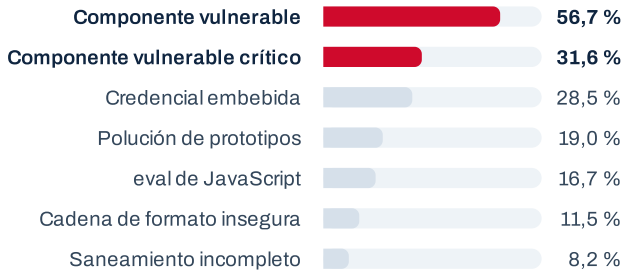
FIG. 4,8



Porcentaje de apps iOS. Los enlaces universales evitan el robo de cuenta OAuth, en el que otra app se apropia de la redirección del inicio de sesión.

HarmonyOS: destacan los componentes antiguos y el código web

FIG. 4,9



Porcentaje de apps HarmonyOS.

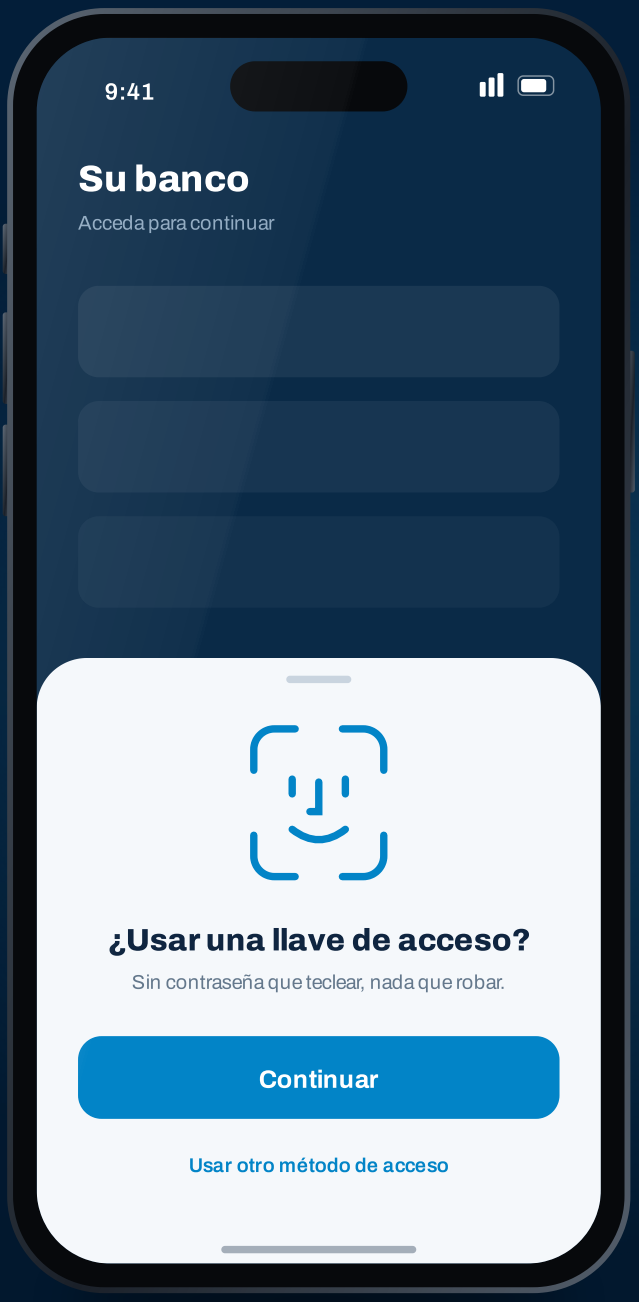
FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

CAPÍTULO 05

05

Autenticación y pagos

Las llaves de acceso, la atestación y la biometría vinculada a claves restan mucha utilidad a las contraseñas robadas y a las apps manipuladas. Se están extendiendo, despacio.



En pantalla: ilustración de una solicitud de llave de acceso, no una app real.

4,9%

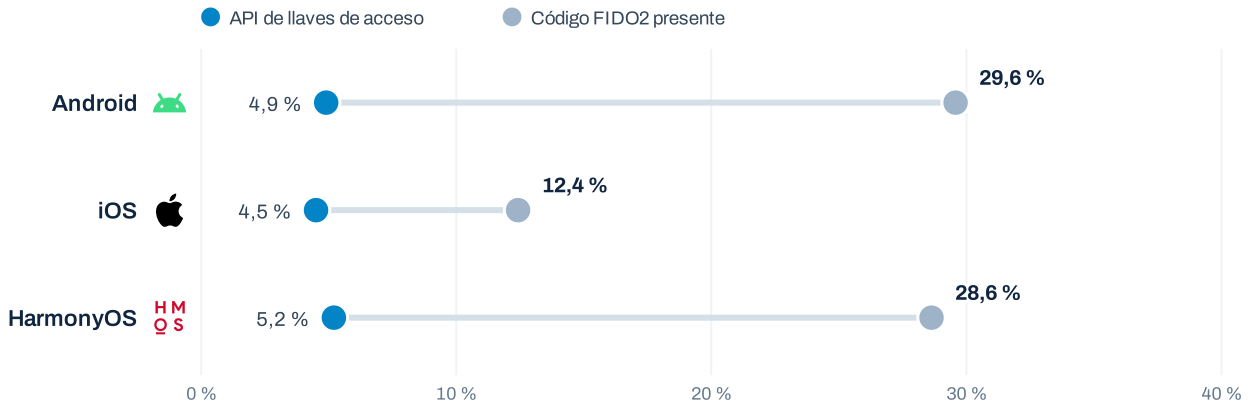
de las apps integran una API de llaves de acceso

El código de llaves de acceso llega; las llaves de acceso, no.

Casi un tercio de las apps Android contiene código FIDO2 o WebAuthn, pero solo el 4,9 % llama a una API de llaves de acceso. En iOS, lo hace el 4,5 %. El código puede llegar dentro de otras bibliotecas sin que la función esté activada.

El código FIDO2 es frecuente; las API de llaves de acceso, raras

FIG. 5,1



Porcentaje de apps de cada plataforma. API de llaves de acceso integrada: la app llama a Credential Manager, a la API FIDO2 de Google o a las API de llaves de acceso de Apple.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

El 79,8 % de las apps no usa ninguna atestación

FIG. 5,2

	Fuerte	Solo débil	Ninguna
Android	16,0 %	2,8 %	81,2 %
Fuerte: Play Integrity · Débil: solo SafetyNet (obsoleto)			
iOS	3,6 %	17,2 %	79,2 %
Fuerte: App Attest · Débil: DeviceCheck, sin App Attest confirmado			
HarmonyOS	20,9 %	4,5 %	74,5 %
Fuerte: Play Integrity 13,4 %, HMS Safety Detect 7,5 % · Débil: solo SafetyNet (obsoleto)			

Porcentaje de apps de cada plataforma con código legible. Fuerte: el servidor del banco puede verificar la app y el dispositivo. Solo débil: una comprobación más antigua o solo del dispositivo, sin ninguna fuerte junto a ella. App Attest y DeviceCheck son servicios de Apple; Play Integrity y SafetyNet, de Google; HMS Safety Detect, de Huawei.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

La atestación permite al servidor del banco comprobar que una solicitud procede de su app auténtica en un dispositivo auténtico. Es la principal defensa contra apps reempaquetadas como Hirudo y, sin embargo, el 79,8 % de las apps no la usa. Desde la app no puede verse si los servidores aplican el resultado.

¿Menciona la web del banco a la app?

Las llaves de acceso y los enlaces a la app solo funcionan si la web del banco menciona la app. Leímos el archivo de asociación público de cada banco y comprobamos si incluye la app.

Pocas webs bancarias mencionan su app para credenciales guardadas y llaves de acceso

FIG. 5,3



Porcentaje de apps de cada plataforma cuya web bancaria declara la app como autorizada para compartir credenciales guardadas y llaves de acceso. Leído de los archivos apple-app-site-association y assetlinks.json de los dominios de los bancos.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

16%

de las apps iOS pertenecen a un banco cuyo archivo también incluye identificadores de app de compilaciones de prueba

92

de 226 dominios bancarios con archivo de asociación de Apple incluyen identificadores de app que no son de producción

88

de 217 dominios bancarios con archivo asset-links de Android incluyen paquetes que no son de producción



El archivo de un banco, tal como lo leyó nuestra comprobación

EL ARCHIVO DE ASOCIACIÓN DE UN BANCO

El archivo del banco declara su app iOS para enlaces universales, así que los enlaces a la web del banco abren la app. No declara la app para credenciales web, así que la app no puede ofrecer las llaves de acceso del banco. Además, incluye 4 identificadores de app de compilaciones de prueba junto a la app de producción.

Higiene, no una vulnerabilidad

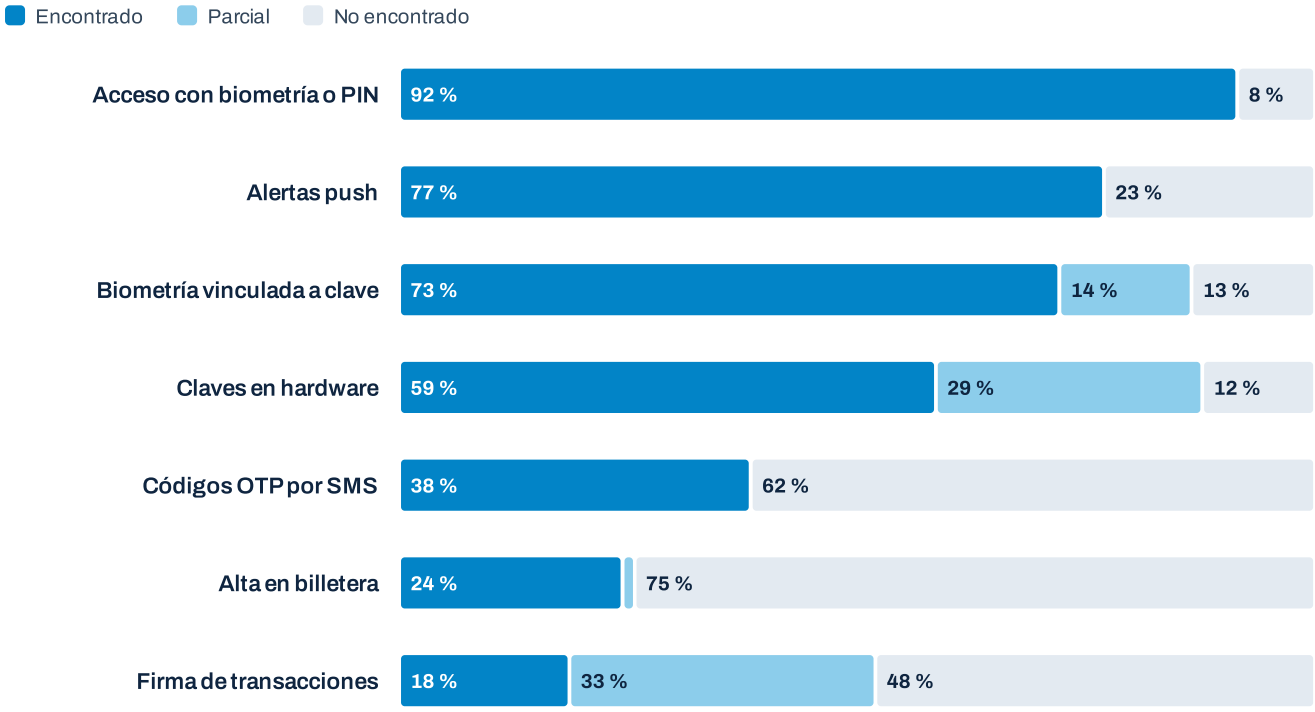
Solo las apps firmadas por el banco pueden usar estas entradas. Pero un archivo de producción que nombra compilaciones de prueba revela a cualquiera los identificadores internos de compilación del banco, y mantiene operativos enlaces y credenciales para compilaciones que los clientes nunca deberían ejecutar. La carencia más grave es la entrada que falta: sin ella, una app no puede ofrecer llaves de acceso en absoluto.

La biometría suele ir vinculada a una clave, pero un tercio puede eludirse.

Cuando pudimos determinar cómo usa la biometría una app Android, el 73,2 % vincula la comprobación a una clave criptográfica, y el 11,4 % la trata como una respuesta de sí o no que el malware puede falsificar. Nuestro escáner también encontró un flujo biométrico eludible en el 35,1 % de las apps Android. Mientras tanto, un tercio de las apps Android y la mayoría de las apps iOS admiten códigos de un solo uso por SMS, el objetivo de los ataques de duplicado de SIM.

Cómo identifican las apps a los usuarios y aprueban los pagos

FIG. 5,4



Porcentaje de 2686 apps de todas las plataformas. Encontrado: evidencia clara en el código. Parcial: parte de la evidencia, pero no toda. La atestación y los SDK antifraude se tratan en las páginas 24 y 15.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Biometría eludible

Un flujo eludible puede estar en una app que usa biometría vinculada a claves en otros puntos. Toda acción sensible debería pasar por la ruta vinculada a una clave, de modo que un «sí» falsificado no desbloquee nada.

Códigos SMS y duplicado de SIM

En un ataque de duplicado de SIM, un estafador convence al operador móvil de que traslade el número de la víctima a una SIM que él controla. A partir de ahí, cada código de un solo uso por SMS llega al atacante, no al cliente. Los códigos vinculados al dispositivo y a la transacción no viajan por SMS.

CAPÍTULO 06

06

Blindaje: lo que incluyen las apps

El blindaje en tiempo de ejecución detecta teléfonos rooteados, depuradores, herramientas de hooking y copias manipuladas de la app. Buscamos estas protecciones en el código de todas las apps, en las tres plataformas.



En pantalla: ilustración de una app blindada en un teléfono rooteado.

26,9%

de las apps Android incluyen un producto de blindaje comercial o de plataforma

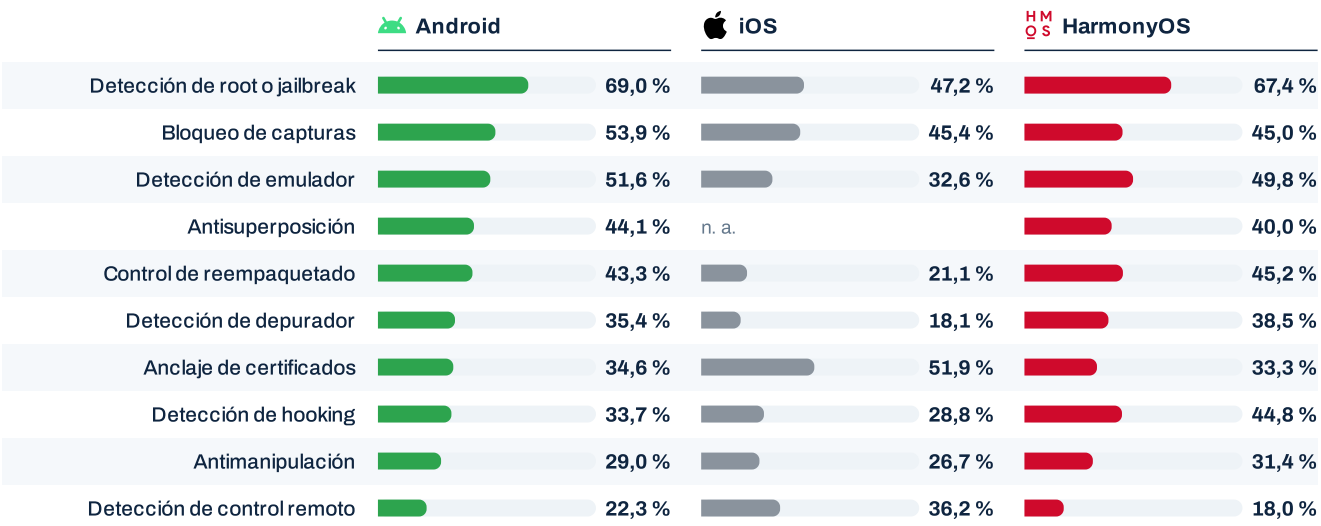
apps Android

Protecciones halladas en el código.

La mayoría de las apps de todas las plataformas comprueba al menos si el teléfono está rooteado o tiene jailbreak. Muchas menos detectan herramientas de hooking, manipulación o control remoto: el 22,3 % de las apps Android y el 36,2 % de las apps iOS muestran código que detecta la pantalla compartida o el control remoto, que los troyanos usan para cometer fraude desde el propio teléfono de la víctima.

Las comprobaciones de root son habituales; las de hooking y control remoto, no

FIG. 6,1



Porcentaje de apps con el control invocado desde el código propio del banco o no atribuido, en cada plataforma. Ordenado por el porcentaje de Android. n. a.: la protección contra superposiciones no se aplica en iOS, donde ninguna app puede dibujar encima de otra.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Presente no equivale a eficaz

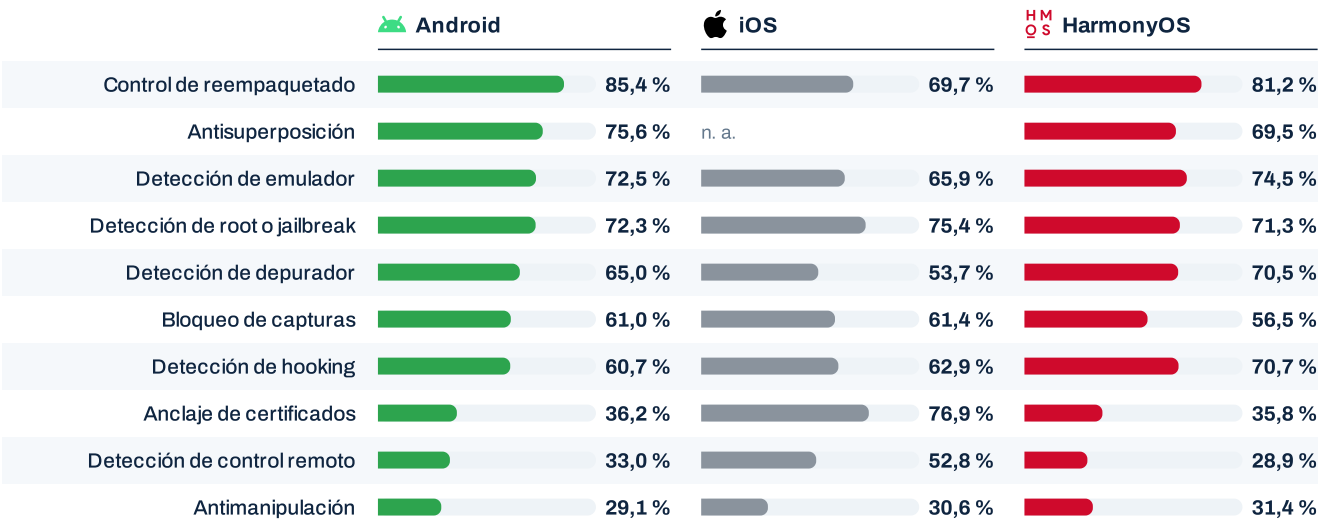
Estos resultados muestran que una protección existe en la app. No muestran que resista a un atacante que sabe que está ahí. Comprobarlo requiere dispositivos reales y está previsto para una edición posterior. Considere estas cifras como un límite superior de la protección.

Los SDK aportan muchos de los controles.

Si se cuentan los controles incluidos en un SDK integrado además del código propio del banco, el 85,4 % de las apps Android incorpora controles de reempaquetado, pero solo el 33 % incorpora detección de control remoto, el control más importante frente a los troyanos de acceso remoto.

Los controles de reempaquetado están muy extendidos; los antimanipulación son raros en todas las plataformas

FIG. 6,2



Porcentaje de apps de cada plataforma. Encontrado: el control está en la app, en el código propio del banco o dentro de un SDK integrado. n. a.: los ataques de superposición no se aplican en iOS. Un control dentro de un SDK solo protege la app si el banco lo activa.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Pocas apps combinan sus defensas en capas.

El blindaje funciona mejor por capas, de modo que eludir un control no desactive el resto. La app Android mediana muestra evidencia clara de 4 de las 10 protecciones que buscamos; el 10,7 % muestra 8 o más.

Las 10 protecciones que buscamos

01 **Detección de root**
Detecta un teléfono rooteado, en el que los datos de la app quedan expuestos.

02 **Detección de emuladores**
Detecta que la app se ejecuta en un emulador y no en un teléfono real.

03 **Detección de depuradores**
Detecta un depurador conectado a la app en ejecución.

04 **Detección de hooking**
Detecta herramientas como Frida que modifican la app mientras se ejecuta.

05 **Control de reempaquetado**
Detecta una copia modificada de la app firmada por otra persona.

06 **Antimanipulación**
Comprueba que el propio código de la app no se ha modificado.

07 **Anclaje de certificados**
Solo acepta el certificado del propio servidor del banco.

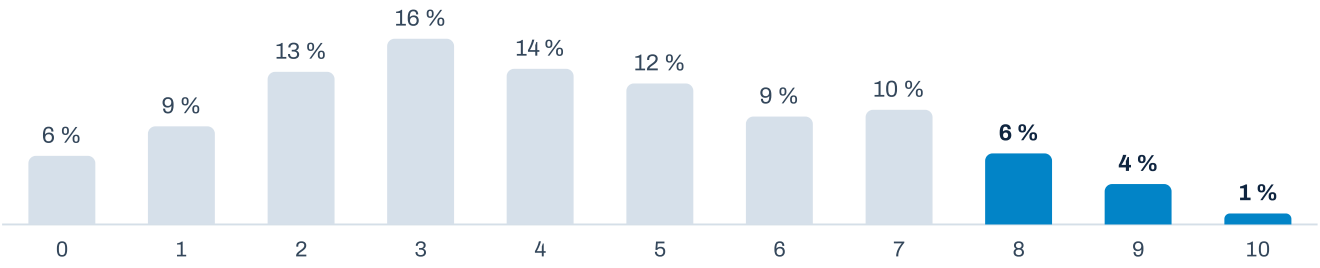
08 **Protección contra superposiciones**
Impide que otra app dibuje una pantalla falsa sobre la app del banco.

09 **Bloqueo de capturas**
Impide las capturas y grabaciones de las pantallas sensibles.

10 **Detección de control remoto**
Detecta la pantalla compartida o una herramienta de acceso remoto.

La app Android mediana muestra 4 de 10 protecciones

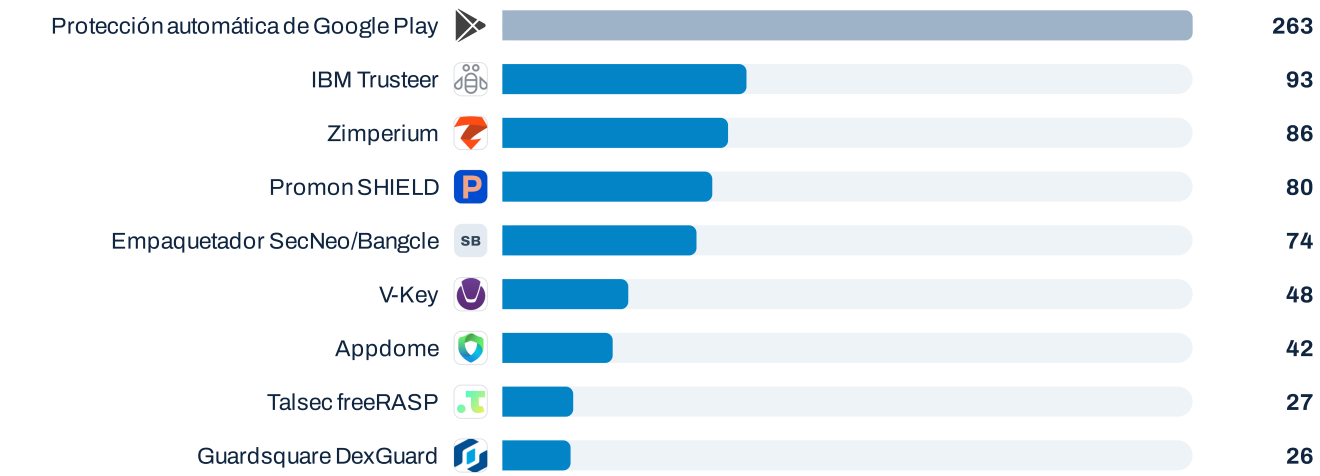
FIG. 6,3



Porcentaje de apps Android según el número de protecciones con evidencia clara, de 10. Resaltado: 8 o más.

La protección automática de Google Play es el blindaje más frecuente

FIG. 6,4



Número de apps que usan cada producto, todas las plataformas. La protección automática de Google Play (pairip) la aplica la tienda; no se elige en el código.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

CAPÍTULO 07

07

Más allá de la app

Una app solo es tan fiable como los dominios, los servidores y la entidad que hay detrás. Revisamos los dominios web y de correo de los bancos, los servidores con los que se comunican las apps, las etiquetas de privacidad, los registros públicos de brechas y las normas a las que está sujeto cada banco.



En pantalla: una etiqueta típica y las discrepancias que nuestro análisis encontró con más frecuencia.

67%

de las apps Android tienen una etiqueta de privacidad de Google Play que contradice sus propios permisos o SDK

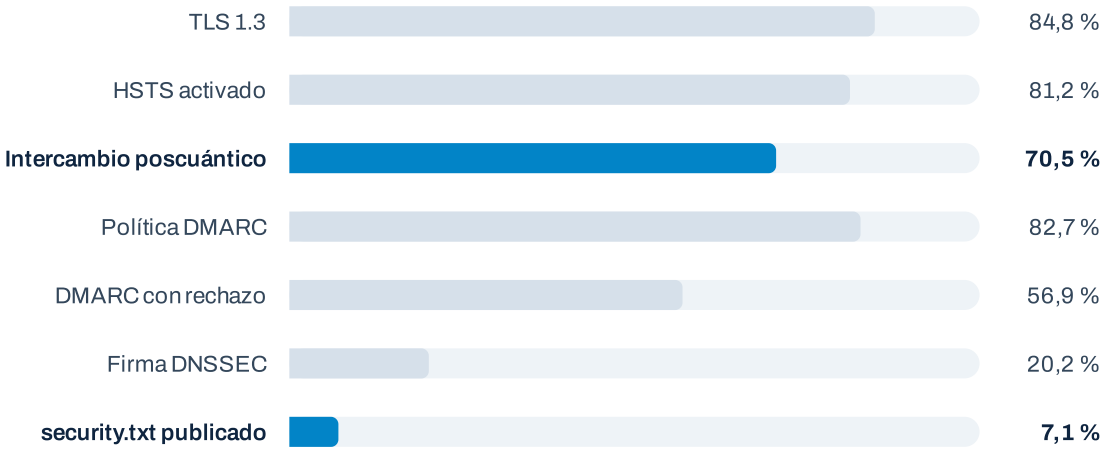
apps Android con etiqueta de privacidad de Google Play

Dominios bancarios: listos para lo cuántico, difíciles de alertar.

El 70,5 % de los hosts web bancarios a los que llegamos ya negocia un intercambio de claves poscuántico. La higiene básica va por detrás: solo el 7,1 % de los dominios publica un archivo security.txt que indique a los investigadores dónde notificar un fallo.

El TLS poscuántico va por delante de security.txt

FIG. 7,1

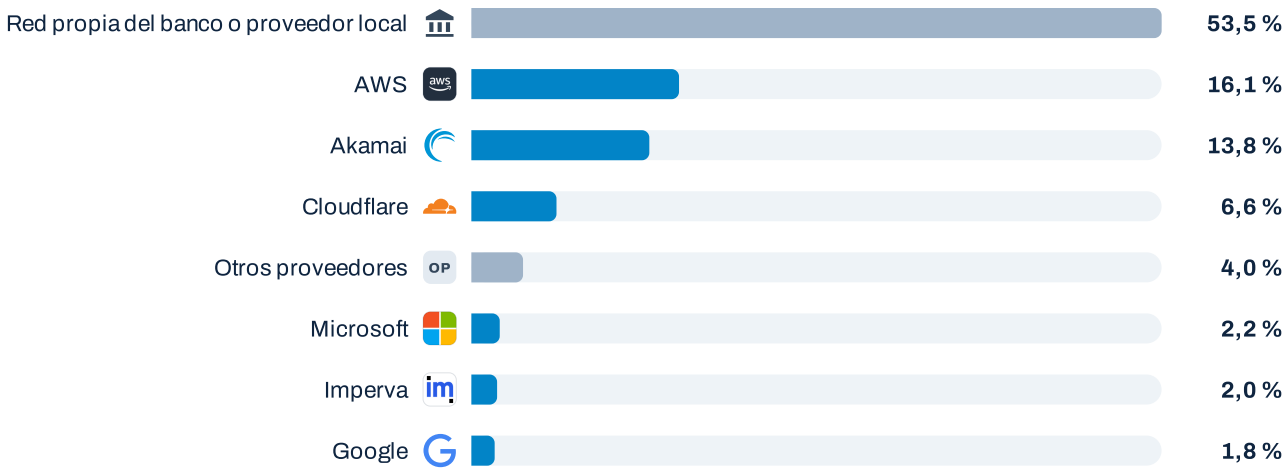


TLS y HSTS: porcentaje de 1140 hosts web accesibles. Poscuántico: 1038 negociaciones completadas. Comprobaciones DNS: 1252 dominios.

FUENTE Negociaciones TLS de Ostorlab y registros DNS públicos de los dominios de los bancos.

La mayoría de los backends funciona en la red propia del banco; AWS encabeza las nubes

FIG. 7,2



Porcentaje de 5101 direcciones IP de backend propiedad de los bancos a las que hacen referencia las apps en las tres plataformas, resueltas mediante DNS público.

FUENTE Hosts referenciados en las apps, resueltos mediante DNS público; registros de titularidad de direcciones IP.

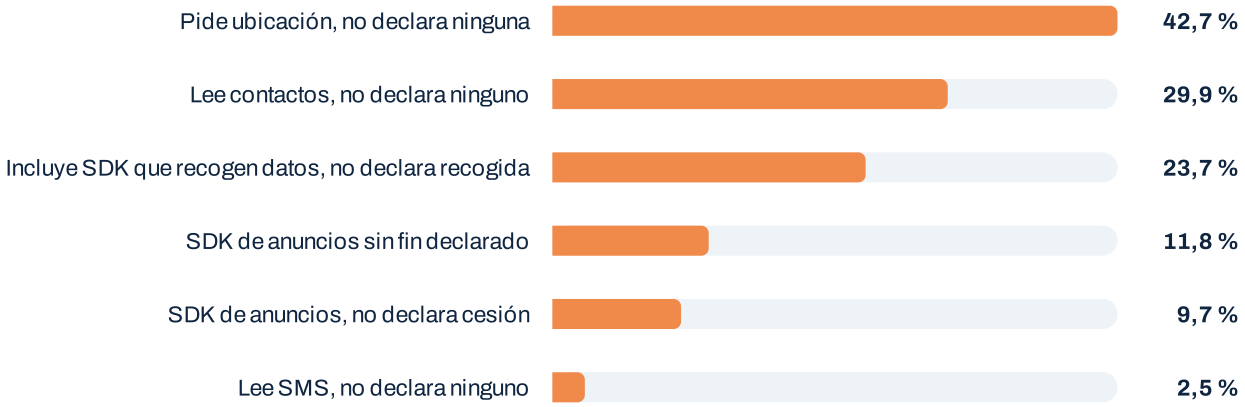
AWS, Akamai, Cloudflare y Microsoft concentran el 38,7 % de las direcciones de backend. Una caída o una brecha en cualquiera de ellos afecta a muchos bancos a la vez. El Reglamento DORA de la UE pide a los bancos que sopesen precisamente esto antes de firmar, incluido si supondría «la celebración de un contrato con un proveedor tercero de servicios de TIC que no sea fácilmente sustituible» (Reglamento (UE) 2022/2554, artículo 29, apartado 1).

Etiquetas de privacidad que no coinciden con la app.

Las tiendas de apps piden a los desarrolladores que declaren qué datos recoge su app. En el 67 % de las apps bancarias Android, la declaración contradice lo que muestran los propios permisos o SDK de la app.

La ubicación no declarada es la discrepancia más frecuente

FIG. 7,3



Porcentaje de apps Android con etiqueta «Seguridad de los datos» de Google Play. Una app puede tener varias discrepancias.

FUENTE Etiquetas «Seguridad de los datos» de Google Play, comparadas con los permisos y SDK de las apps.

Por qué importa

Un permiso en el manifiesto no prueba que la app lo use, así que algunas discrepancias se deben a manifiestos excesivamente prudentes. Pero los reguladores leen las etiquetas como compromisos. Una etiqueta que infravalora la recogida de datos es un riesgo de cumplimiento normativo y confunde a los clientes que comparan apps.

Etiquetas de iOS

De las apps bancarias iOS con etiqueta de privacidad, el 19 % declara datos usados para rastrear a los usuarios en apps de otras empresas, sobre todo identificadores y datos de uso.

Algunos servidores bancarios responden más allá de la web.

De las 5101 direcciones de servidor propiedad de los bancos a las que apuntan las apps, 4113 aparecen en datos públicos de observación de todo internet. 251 de ellas responden en puertos distintos de los de tráfico web y CDN, en 113 bancos, y 79 ejecutan software cuya versión coincide con una vulnerabilidad conocida.

251

IP bancarias con puertos abiertos además de los web y CDN, en 113 bancos

79

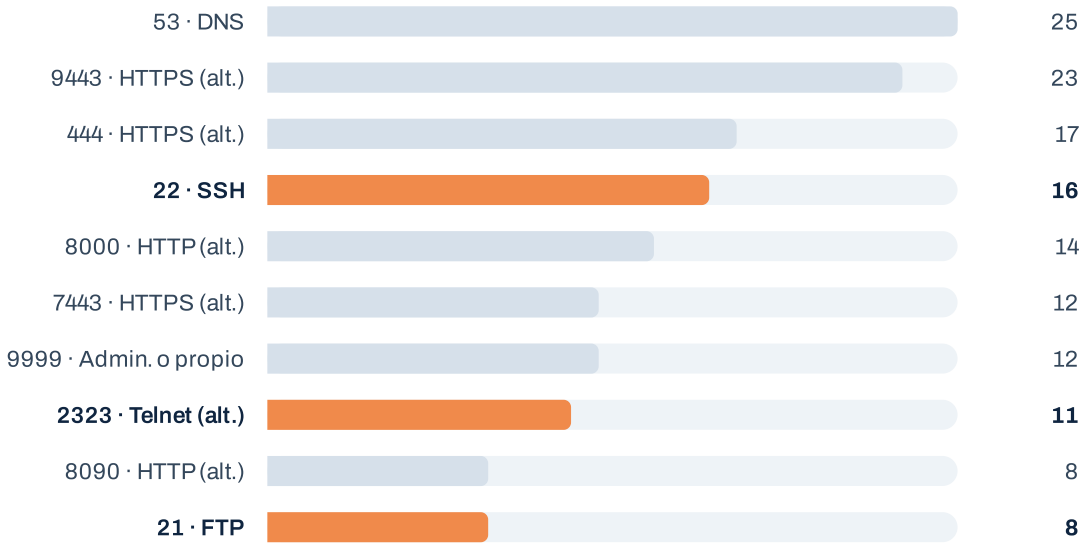
IP bancarias con CVE deducidas de las versiones de software, en 74 bancos

25

IP bancarias que ejecutan un producto al final de su vida útil

DNS y los puertos HTTPS alternativos encabezan los puertos abiertos adicionales

FIG. 7,4



Número de IP propiedad de los bancos que responden en cada puerto, de 4113 indexadas por Shodan InternetDB. Se excluyen los puertos 80 y 443 y los puertos de proxy de CDN; no se cuentan 151 IP que responden en más de 40 puertos, algo típico de cortafuegos y tarpits.

FUENTE Shodan InternetDB, índice pasivo; no se envió ninguna solicitud a ningún servidor bancario.

No escaneamos ningún servidor bancario

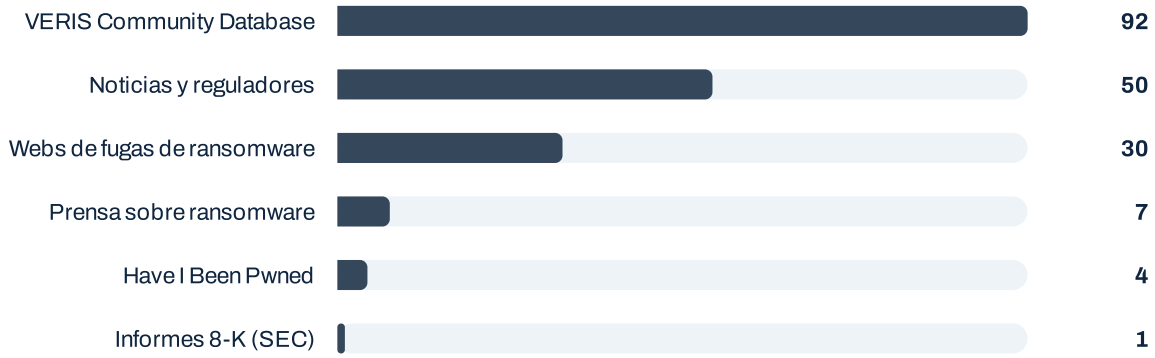
Los puertos abiertos y las versiones de software proceden de datos públicos de observación de todo internet (Shodan InternetDB), así que no se tocó ningún sistema bancario. Las otras 988 direcciones no figuran en esos datos: estado desconocido, no cerradas. Las CVE se asocian a partir de la versión de software observada, así que cada una es una pista que el banco debe confirmar.

Uno de cada seis bancos tiene un registro público de brechas.

En bases de datos de brechas, sitios de filtraciones de ransomware, avisos de reguladores y registros ante la SEC, encontramos al menos un registro público de brecha para 83 de los 500 principales bancos (16,6 %). 55 de ellos tienen un registro de 2020 o posterior.

La mayoría de los registros de brechas procede de la base de datos VERIS

FIG. 7,5



Número de registros de los 500 principales bancos; un banco puede tener varios. Cada coincidencia se revisó a mano. Las comprobaciones de noticias y reguladores solo cubrieron los 29 G-SIB.

FUENTE VCDB, Have I Been Pwned, ransomware.live, informes 8-K de la SEC, noticias y avisos de reguladores.

Qué es un registro

Un registro es un incidente comunicado públicamente: un ataque, un empleado que abusa de su acceso, un error que expuso datos o la reivindicación de un grupo de ransomware. No es un hallazgo sobre la app del banco, y muchos registros son antiguos: la base de datos VERIS se remonta a más de una década.

CVE que nombran a un banco

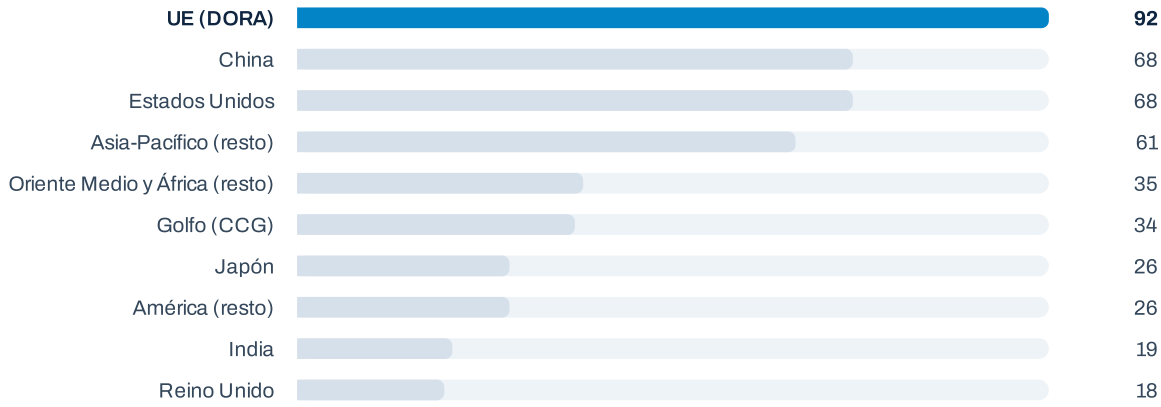
51 registros CVE publicados coinciden con la marca de 37 bancos, 14 de ellos desde 2025. La mayoría describe versiones antiguas de apps móviles, y la coincidencia por marca incluye falsos positivos, así que los tratamos como pistas, no como hallazgos.

Las normas que rigen a los bancos y lo que estos declaran.

Todos los bancos de la muestra están sujetos a un régimen nacional o regional de riesgo TIC. 95 de los 500 principales bancos están sujetos al Reglamento de Resiliencia Operativa Digital (DORA) de la UE, que se aplica desde enero de 2025 y convierte dependencias como los proveedores de alojamiento de la página 32 en una responsabilidad de la dirección.

El Reglamento DORA de la UE cubre el mayor grupo de bancos

FIG. 7,6



Número de los 500 principales bancos, según el régimen de su país de origen. Se muestran los diez grupos mayores; otros 40 bancos están en grupos más pequeños.

FUENTE Registros de los reguladores y mercados de origen de los bancos.

332

de los 500 principales bancos son emisores de Apple Pay

44

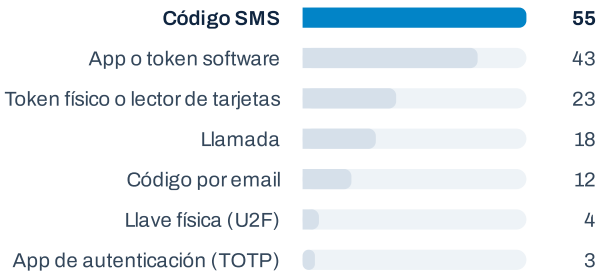
bancos declaran en su web que tienen una certificación, sobre todo ISO 27001

19

bancos tienen un programa público de divulgación de vulnerabilidades, 5 con bug bounty

El SMS es el segundo factor más anunciado

FIG. 7,7



Número de los 73 bancos cuyas webs describen sus métodos de acceso; un banco puede indicar varios. 8 anuncian llaves de acceso.

FUENTE Webs de los bancos y la lista 2fa.directory.

Declaraciones, no certificados

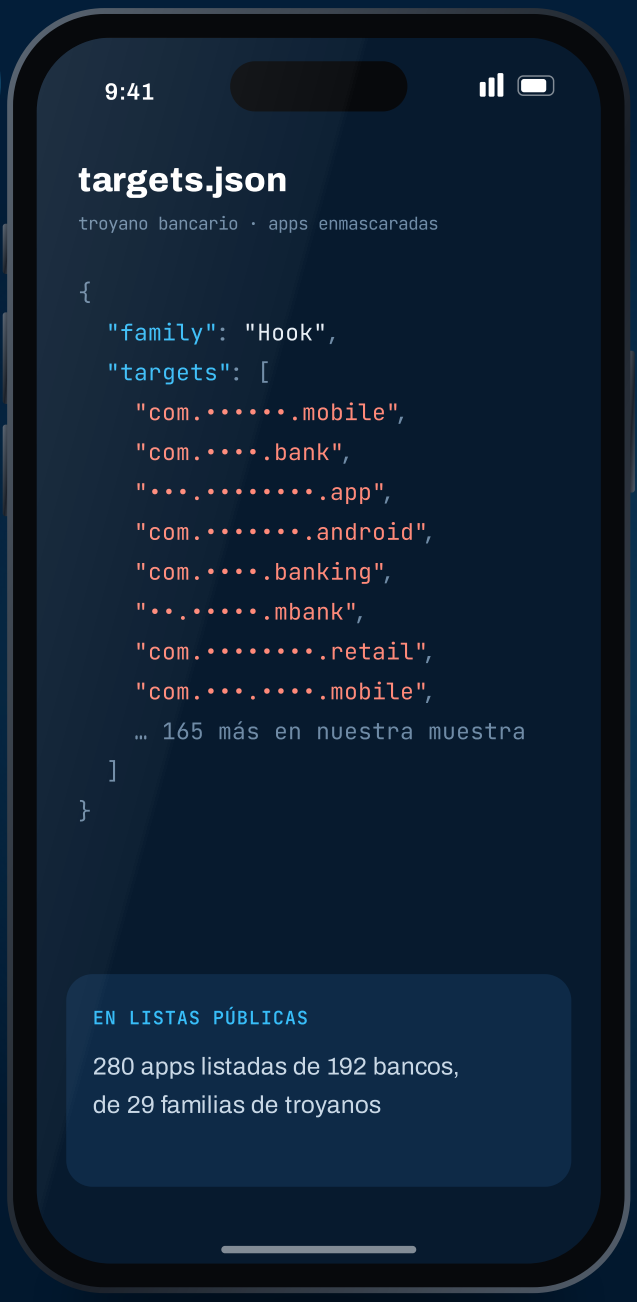
Las certificaciones son lo que dice la web de un banco, no certificados verificados. 62 bancos publican un archivo security.txt en al menos un dominio, y 19 mencionan un programa de divulgación. El SMS sigue siendo el segundo factor más anunciado, aun cuando reguladores como el banco central de los Emiratos Árabes Unidos están retirando los códigos de un solo uso por SMS.

CAPÍTULO 08

08

El panorama de amenazas

Los troyanos bancarios mantienen listas de las apps que atacan. Los kits de phishing copian las páginas de acceso de los bancos. En el último año, los atacantes también han sustituido apps bancarias auténticas por copias parcheadas.



En pantalla: la estructura de una lista de objetivos publicada, con los nombres de las apps enmascarados.

15%

de las apps Android analizadas figuran en al menos una lista pública de objetivos de troyanos bancarios

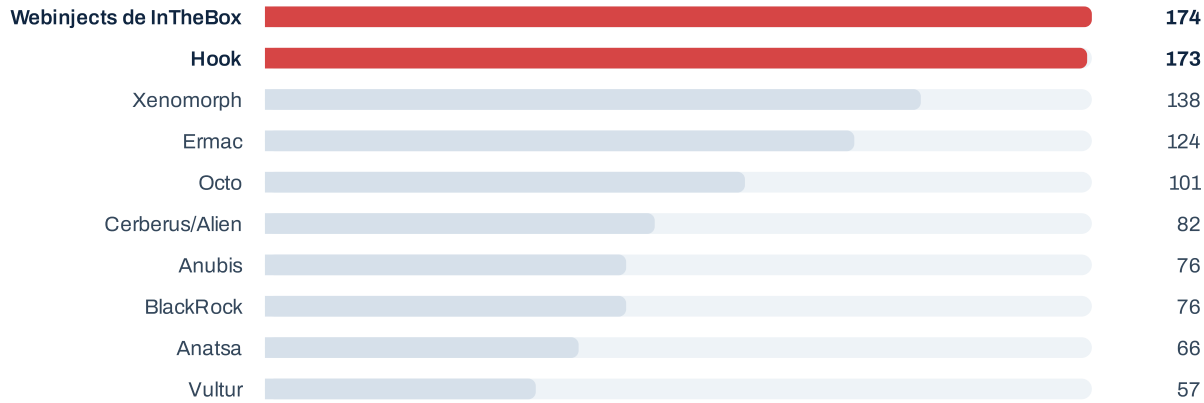
apps Android

Cuatro de cada diez bancos están en la lista de un troyano.

Los investigadores publican las listas de objetivos halladas dentro de los troyanos bancarios. Al cruzarlas con las apps Android de nuestra muestra, 280 apps de 192 bancos (38,4 %) aparecen citadas por al menos una de 29 familias.

Hook e InTheBox apuntan a más apps de la muestra

FIG. 8,1



Número de apps de nuestra muestra en las listas de objetivos publicadas de cada familia: 47 listas, publicadas en su mayoría de 2021 a 2023 por ThreatFabric, Cleafy, Zimperium y otros. Solo Android, porque las listas nombran paquetes Android.

FUENTE Listas publicadas de objetivos de troyanos bancarios (ThreatFabric, Cleafy, Zimperium y otros), 2021–2023.

Europa y América concentran el 93 % de los hosts de phishing y los nueve bancos más atacados

FIG. 8,2

54%
Europa
5 de los 9 bancos más atacados

39%
América
4 de los 9 bancos más atacados

5%
Asia-Pacífico
ninguno de los 9 bancos más atacados

1%
Oriente Medio y África
ninguno de los 9 bancos más atacados



Color: porcentaje de cada región sobre los hosts de phishing activos que nombran a un banco. Chinchetas: número de los nueve bancos más atacados con sede en ese país; en conjunto, esos nueve concentran el 57 % de todos los hosts. Gris: fuera de la muestra. No se nombra a los bancos.

FUENTE PhishTank, OpenPhish, Phishing.Database y URLhaus.

2026: los atacantes vuelven la propia app del banco en su contra.

Durante diez años, los troyanos bancarios dibujaron pantallas falsas sobre la app real. Las campañas del último año van más allá: parchean, clonan o sustituyen la app auténtica, de modo que el propio código del banco acaba trabajando para el atacante.

DESDE 2016

Superposición

Dibujar encima

Un troyano dibuja una pantalla falsa de acceso o de pago sobre la app real y lee lo que escribe el cliente.

POR QUÉ FUNCIONA

La app auténtica no se toca; el troyano solo necesita el permiso de accesibilidad.

QUÉ LO DETIENE

Protección contra superposiciones, comprobación de servicios de accesibilidad

GOLDFACTORY, 2025

Parcheo

Modificar la app

El atacante toma la app auténtica, inyecta código de hooking y la vuelve a firmar, de modo que las propias pantallas del banco ejecutan el código del atacante.

POR QUÉ FUNCIONA

La copia tiene el aspecto y el comportamiento de la app real, incluidos sus controles de integridad, que el hook desactiva.

QUÉ LO DETIENE

Verificación de la firma con la clave del banco, atestación en el servidor

GIGABUD, 2026

Clonado

Ejecutar una segunda copia

El atacante ejecuta la app auténtica dentro de un perfil de trabajo oculto o de un espacio virtual que controla.

POR QUÉ FUNCIONA

Las herramientas antifraude ven la app real en un dispositivo conocido, así que la sesión parece normal.

QUÉ LO DETIENE

Detección de perfiles de trabajo y espacios virtuales, vinculación al dispositivo

HIRUDO, 2026

Sustitución

Cambiar la app

Un dropper desinstala la app auténtica e instala una copia parcheada con el mismo nombre, icono y número de versión.

POR QUÉ FUNCIONA

El cliente no ve ningún cambio. Solo difiere la clave de firma, y solo el servidor del banco puede comprobarla.

QUÉ LO DETIENE

Atestación en el servidor que compruebe la clave de firma

Cómo funciona una sustitución de app, paso a paso

1. Una falsa actualización

La víctima instala un dropper desde un enlace o una página de tienda falsa.

2. La app real desaparece

El dropper desinstala la app bancaria auténtica.

3. Vuelve una copia

Instala una copia parcheada: mismo nombre, icono y versión, distinta clave de firma.

4. Se filtran las credenciales

La copia captura contraseñas y códigos de un solo uso mientras aparenta normalidad.

5. El servidor decide

Solo la atestación en el servidor del banco puede distinguir la copia de la app.

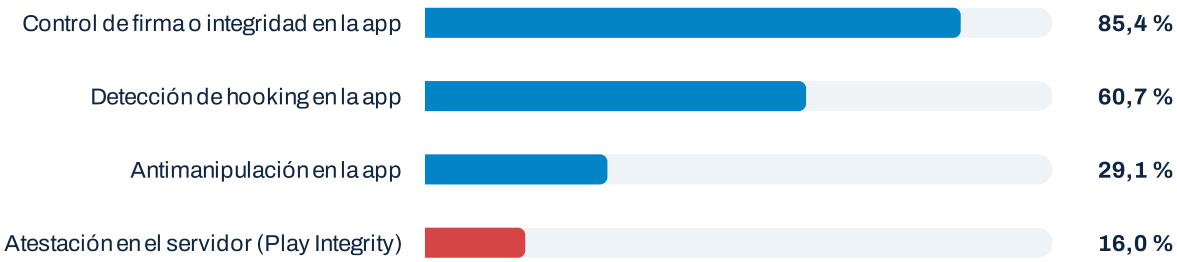
FUENTE Group-IB (GoldFactory, Gigabud), ThreatFabric (Hirudo); análisis de Ostorlab.

¿Notaría un banco que su app ha sido sustituida?

Una copia parcheada puede desactivar cualquier control que se ejecute en el teléfono. El servidor puede hacerlo mejor: puede rechazar las solicitudes que no incluyan una prueba reciente, firmada por Google o Apple, de que la app es la compilación auténtica del banco. Solo el 16 % de las apps Android contiene el código para solicitar esa prueba, y no podemos ver si sus servidores la exigen.

Los controles en la app son habituales; los controles en el servidor, raros

FIG. 8,3



Porcentaje de apps Android. En la app: hallado en el código propio del banco o dentro de un SDK integrado. Atestación en el servidor: la app contiene el código para solicitar la prueba; desde la app no puede verse si el servidor la exige, y un dispositivo auténtico pero comprometido puede superarla igualmente.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Las campañas de 2026

Cuándo	Campaña	Tipo	Qué ocurrió	Publicado por
Dic. 2025	**GoldFactory**	Parcheo	Apps bancarias auténticas de Tailandia, Vietnam e Indonesia a las que se inyectó código de hooking que elude sus controles de integridad: 27 apps modificadas y más de 11000 infecciones comunicadas.	Group-IB
Feb.–jul. 2026	**Gigabud**	Clonado	Apps bancarias ejecutadas dentro de un perfil de trabajo de Android para eludir la detección de fraude; unos 1469 dispositivos comprometidos comunicados.	Group-IB
Mayo 2026	**Prueba de laboratorio**	Parcheo	El 58 % de las apps bancarias probadas en ocho mercados podía reempaquetarse.	Promon
2026	**Familias de superposición**	Superposición	34 familias activas de malware bancario dirigidas a 1243 marcas financieras de 90 países.	Zimperium
Ago.–oct. 2026	**Hirudo**	Sustitución	Un dropper cambia una app bancaria indonesia real por una copia parcheada firmada con una clave de prueba pública; ocho apps de siete bancos tenían ya una sustituta lista. Caso de estudio, página 49.	ThreatFabric

Qué hacer

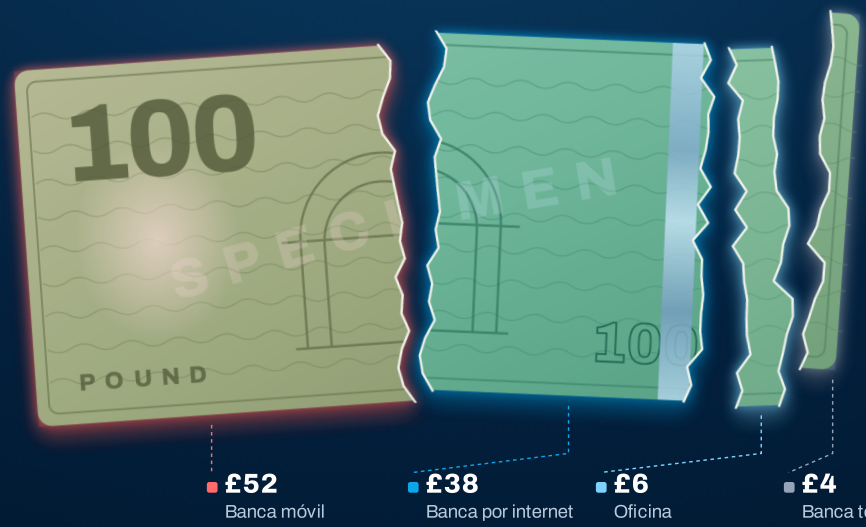
Trate cualquier control que se ejecute en el teléfono como un simple obstáculo. Haga que decida el servidor: exija atestación para el acceso y los pagos, rechace las solicitudes de apps firmadas con cualquier clave que no sea la del banco y vincule la sesión del cliente al dispositivo en que se inició.

Adónde va el dinero.

Los datos publicados sobre fraude son irregulares: de 101 mercados revisados, 83 publican alguna cifra comparable. Donde hay datos, apuntan en la misma dirección: el fraude se ha desplazado a los pagos que el cliente hace engañado, y al teléfono.

FIG. 8.4

De cada 100 £ perdidas por estafas en el Reino Unido, 52 £ salieron a través de una app de banca móvil



576,4 M£
perdidos por estafas de transferencia autorizada en el Reino Unido en 2025

79 %
de los pagos por estafa, en número, se hicieron en banca móvil

88 %
de las pérdidas por estafa notificadas se reembolsaron según la norma de reembolso del Reino Unido

Un billete de 100 £ rasgado según el canal en el que se hizo el pago de la estafa; cada trozo es tan ancho como la proporción del valor perdido en su canal. En las estafas de transferencia autorizada (APP), se engaña al cliente para que envíe el dinero. Las pérdidas autorizadas subieron un 19 % en el año, mientras que las no autorizadas bajaron un 5 %.

Fuente: UK Finance, Annual Fraud Report 2026; Payment Systems Regulator del Reino Unido

Europa

En 2024, el 74 % del valor fraudulento de las transferencias en la UE se debió a la manipulación del ordenante para que autorizara el pago. El fraude con tarjeta es 13 veces más frecuente, en valor, cuando la tarjeta no está presente. Fuente: informe de fraude en pagos del BCE y la ABE, datos de 2024.

El reembolso funciona

Desde que el reembolso pasó a ser obligatorio en el Reino Unido en octubre de 2024, los bancos devolvieron el 88 % del valor de las pérdidas por estafas APPnotificadas en los 18 meses siguientes. La responsabilidad se desplaza hacia los bancos, lo que aumenta el valor de los controles que frenan las estafas en la app. Fuente: Payment Systems Regulator del Reino Unido.

Contexto, no causa

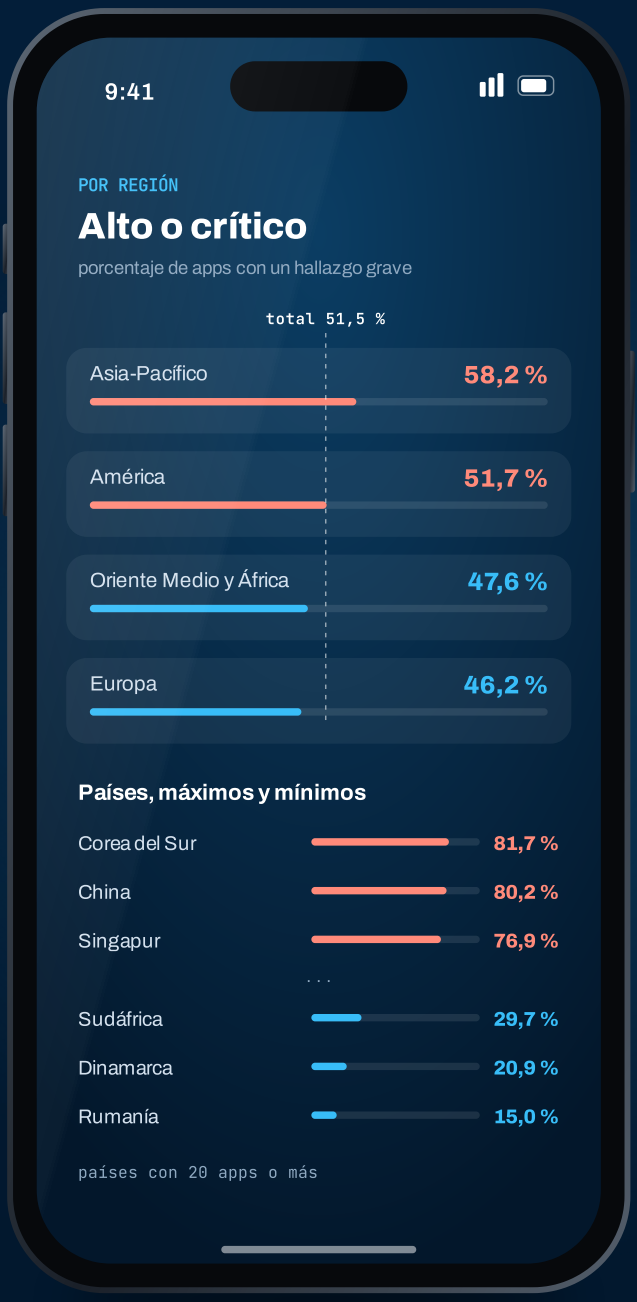
Estas estadísticas describen el fraude en cada mercado. No demuestran que las debilidades de las apps recogidas en este informe causaran las pérdidas.

CAPÍTULO 09

09

Por región, tipo de banco y país

Los resultados varían más por país que por plataforma. Algunos mercados lideran en blindaje, otros en atestación, y ninguno lidera en todo.



En pantalla: apps con un hallazgo alto o crítico, por región y país.

64

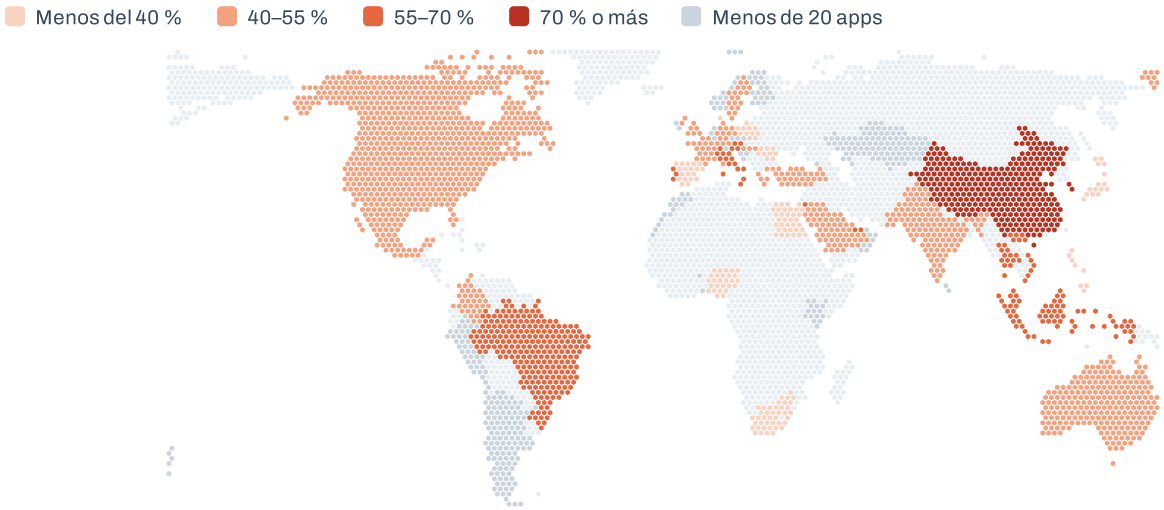
países en la muestra, de Estados Unidos y China a Togo y Liechtenstein

Ninguna región lo tiene todo.

Las apps de Asia-Pacífico tienen a la vez los hallazgos más graves y el mayor blindaje. Las apps europeas son las que menos hallazgos altos o críticos tienen. Las apps de América lideran en llaves de acceso, con un 9,9 %.

Los hallazgos graves varían mucho de un país a otro

FIG. 9,1



Porcentaje de apps de cada país, para los 40 países con al menos 20 apps; gris: en la muestra con menos de 20 apps.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Ninguna región ni tipo de banco lidera en todas las medidas

FIG. 9,2

Grupo	Apps	Alto o crítico	Componente vulnerable	Credenciales embebidas	Producto de blindaje	Atestación	Llaves de acceso
Asia-Pacífico	942	58,2 %	46,3 %	24,5 %	33,7 %	20,0 %	2,8 %
Europa	822	46,2 %	40,0 %	15,7 %	21,3 %	16,9 %	4,7 %
Oriente Medio y África	508	47,6 %	39,0 %	23,0 %	19,9 %	19,9 %	4,3 %
América	414	51,7 %	33,8 %	16,2 %	29,5 %	23,4 %	9,9 %
Por tipo de banco							
Tradicional	2596	51,2 %	40,9 %	19,8 %	26,4 %	19,3 %	4,4 %
Neobanco filial	61	52,5 %	47,5 %	24,6 %	37,7 %	16,4 %	4,9 %
Neobanco independiente	29	**79,3 %**	44,8 %	**48,3 %**	24,1 %	**48,3 %**	**37,9 %**
Total	*2686*	*51,5 %*	*41,1 %*	*20,2 %*	*26,6 %*	*19,6 %*	*4,8 %*

Porcentaje de apps de cada grupo. Los neobancos independientes tienen un hallazgo alto o crítico con mucha más frecuencia que las demás apps (79,3 % frente a 51,2 %; prueba exacta de Fisher, p = 0,002), mientras que los neobancos filiales se parecen al resto. Los neobancos independientes también lideran en atestación y en API de llaves de acceso. Son solo 29 apps, un tercio de un mismo banco, así que la magnitud de la diferencia es orientativa. Celdas sombreadas como en la página siguiente. Las credenciales embebidas excluyen las claves de API de Google. Solo se comparan reglas multiplataforma, porque la combinación de plataformas varía según la región.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Resultados por país.

Los 18 países con más apps en la muestra. Cada celda se sombrea según cuánto supera el porcentaje del conjunto de apps: rojo para un riesgo, azul para una defensa. Las celdas sin sombrear están en ese porcentaje o por debajo.

Cada país tiene su propio patrón de riesgos y defensas

FIG. 9,3

Por encima del total de apps: Riesgo +5 p. p. +12 +20 Defensa +5 p. p. +12 +20

País	Apps	Alto o crítico	Componente vulnerable	Credenciales embebidas	Producto de blindaje	Atestación	Llaves de acceso
Estados Unidos	224	52,2 %	35,3 %	12,9 %	33,9 %	28,1 %	12,9 %
India	200	50,0 %	30,5 %	21,0 %	**43,0 %**	**32,5 %**	0,5 %
China	162	**80,2 %**	**77,8 %**	**43,8 %**	**51,9 %**	15,4 %	5,6 %
Reino Unido	157	47,1 %	**57,3 %**	31,2 %	**43,9 %**	18,5 %	14,0 %
Japón	116	38,8 %	33,6 %	13,8 %	6,9 %	4,3 %	3,4 %
Arabia Saudí	95	47,4 %	32,6 %	31,6 %	17,9 %	13,7 %	6,3 %
Emiratos Árabes Unidos	84	**64,3 %**	**59,5 %**	25,0 %	23,8 %	28,6 %	0,0 %
Francia	76	43,4 %	35,5 %	3,9 %	21,1 %	9,2 %	0,0 %
Italia	74	58,1 %	**58,1 %**	21,6 %	5,4 %	29,7 %	2,7 %
Sudáfrica	74	29,7 %	17,6 %	**37,8 %**	20,3 %	**54,1 %**	9,5 %
Malasia	71	57,7 %	42,3 %	25,4 %	31,0 %	25,4 %	1,4 %
España	69	37,7 %	24,6 %	8,7 %	**42,0 %**	27,5 %	7,2 %
Brasil	66	60,6 %	31,8 %	22,7 %	27,3 %	21,2 %	10,6 %
Australia	63	54,0 %	33,3 %	19,0 %	4,8 %	23,8 %	3,2 %
Corea del Sur	60	**81,7 %**	**71,7 %**	21,7 %	3,3 %	3,3 %	0,0 %
Vietnam	56	**64,3 %**	51,8 %	**33,9 %**	**41,1 %**	25,0 %	3,6 %
Catar	55	41,8 %	40,0 %	21,8 %	10,9 %	25,5 %	0,0 %
Canadá	50	48,0 %	26,0 %	14,0 %	12,0 %	14,0 %	4,0 %
Total	*2686*	*51,5 %*	*41,1 %*	*20,2 %*	*26,6 %*	*19,6 %*	*4,8 %*

Porcentaje de apps de cada país. Sombreado: 5, 12 y 20 puntos porcentuales o más por encima del porcentaje del conjunto de apps. Las apps de China incluyen muchas apps HarmonyOS, que elevan sus cifras de componentes y de hallazgos críticos.

FUENTE Análisis de seguridad automatizado de Ostorlab de 2686 apps bancarias.

Las apps bancarias más seguras por región.

Tres bancos por región cuyas apps tienen menos debilidades, y menos graves, que las de sus homólogos, por orden alfabético. No se muestran puntuaciones.

Norteamérica

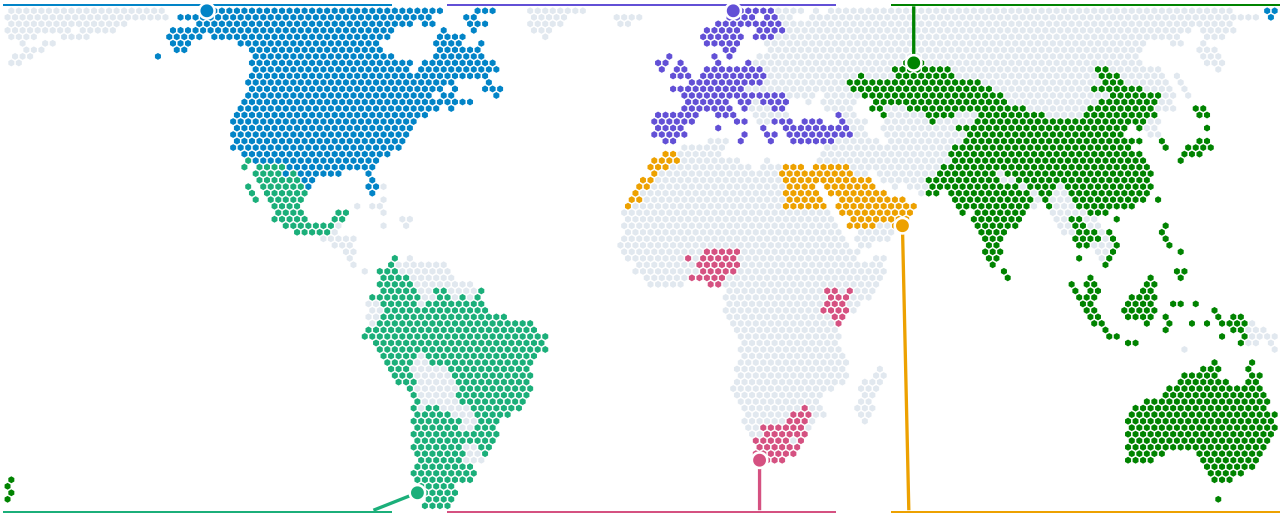
- **Scotiabank** — Canadá
- **WaFD Bank** — Estados Unidos
- **Zions Bancorporation** — Estados Unidos

Europa

- **Ibercaja** — España
- **Komerční banka** — Chequia
- **TSB** — Reino Unido

Asia-Pacífico

- **Bandhan Bank** — India
- **HBL** — Pakistán
- **RCBC** — Filipinas



América Latina

- **Banorte** — México
- **BCP** — Perú
- **Itaú** — Brasil

África subsahariana

- **Absa** — Sudáfrica
- **Co-Operative Bank of Kenya** — Kenia
- **Rand Merchant Bank** — Sudáfrica

Oriente Medio y Norte de África

- **Gulf Bank** — Kuwait
- **Qatar Islamic Bank** — Catar
- **Saudi Investment Bank** — Arabia Saudí

Color: países cuyos bancos se compararon, un color por región Gris: no comparados

Cómo se compararon los bancos

Se comparan bancos, no apps individuales. Cada app analizada obtiene un valor a partir de la calificación de su análisis (70 %) y de las defensas y debilidades halladas en su código (30 %), y se sitúa entre las apps de su propia tienda. La puntuación de las apps de un banco es la media de todas sus apps analizadas, ajustada hacia el centro cuando tiene pocas.

El historial de seguridad cuenta

A continuación, la puntuación se reduce por cada incidente de seguridad del banco comunicado públicamente en los últimos tres años: más si el incidente es grave, menos si es leve. Las estafas dirigidas a los clientes no cuentan. Un historial vacío significa que no se encontró nada, no que no ocurriera nada.

Qué significa una posición

Los tres bancos mejor situados de cada región, entre los bancos con al menos dos apps analizadas. Una posición significa hallazgos menos numerosos y menos graves que los de sus homólogos. No significa que las apps estén libres de hallazgos.

FUENTE Calificaciones de análisis y controles de seguridad de Ostorlab para las apps de los 500 principales bancos; informes públicos de incidentes. Los logotipos son los iconos de las webs de los bancos y marcas de sus titulares, mostrados solo a efectos de identificación.

CAPÍTULO 10

10

Casos de estudio

Cuatro ataques públicos de 2026, cada uno contrastado con lo que nuestro análisis encontró en las apps a las que apuntan. Van de una app falsa instalada durante una llamada telefónica a la sustitución de la app auténtica y a una clave en la nube que gana nuevos permisos después de publicada la app.



En pantalla: los cuatro casos y la página en la que empieza cada uno.

4

ataques públicos de 2026, cada uno contrastado con lo que nuestro análisis encontró en las apps a las que apuntan

CASO DE ESTUDIO 1 DE 4 · LA APP FALSA

CyberDakait: siete troyanos, una llamada.

Siete familias de troyanos para Android dirigidas a clientes de bancos indios. El malware es corriente. Lo que lo hace funcionar es la llamada previa: un estafador que se hace pasar por el banco convence a la víctima de que lo instale.

7
familias de troyanos en el grupo

17 960+
dispositivos infectados, contados en los propios servidores de los operadores

7,6 M
de SMS interceptados en los teléfonos de las víctimas

Publicado por Group-IB, 28 de octubre de 2026

Cómo funciona el ataque

1

La llamada

Alguien que se hace pasar por el banco ofrece un «plan de protección de la tarjeta de crédito» o una recompensa.

Avise a los clientes de que el banco nunca envía una app durante una llamada

2

El enlace

La víctima recibe un archivo de app que se hace pasar por uno de 11 bancos indios o 2 programas gubernamentales.

3

La falsa actualización

Una pantalla de «actualización» al estilo de Google Play consigue que se instale la app y se concedan sus permisos.

4

La superposición

Una copia de las pantallas del banco pide los datos de la tarjeta, las credenciales de acceso y el PIN.

5

Los SMS

El troyano lee los SMS entrantes y reenvía los códigos de un solo uso a los operadores.

Vincule los códigos al dispositivo y a la transacción, no a un simple SMS

6

El robo

Con las credenciales y los códigos, los operadores vacían las cuentas. Las pérdidas comunicadas superan los 30 500 $.

LO QUE ENCONTRÓ NUESTRO ANÁLISIS

Protección contra superposiciones en la app **75,6 %**

Admiten códigos de un solo uso por SMS **33,7 %**

Porcentaje de apps Android. La protección contra superposiciones solo protege la app auténtica: una app falsa enviada durante una llamada nunca la ejecuta. El ataque triunfa cuando el banco acepta un código SMS como prueba de identidad.

QUÉ LO HABRÍA EVITADO

- Avise a los clientes, en la app y en todos los canales, de que el banco nunca envía una app ni pide instalarla durante una llamada.
- Sustituya los códigos SMS por aprobaciones vinculadas al dispositivo y a la transacción.
- Retenga para revisión los nuevos dispositivos y beneficiarios que aparezcan durante una llamada.

Group-IB, *False Protection, Emptied Accounts: The Seven Android Trojan Families Targeting Indian Banking Apps*, 28 de octubre de 2026.
No se nombra a ningún banco: Group-IB no identifica a los bancos suplantados.

CASO DE ESTUDIO 2 DE 4 · LA APP SECUESTRADA

WindRelay: un préstamo pedido desde la propia app bancaria de la víctima.

Dos herramientas usadas conjuntamente en Europa Central: SpyNote, un troyano de acceso remoto que entrega al operador el teléfono de la víctima, y WindRelay, que retransmite por NFC la tarjeta de pago de la víctima a un teléfono en manos de una mula.

2
herramientas combinadas: un troyano de acceso remoto y un relé NFC

3
países objetivo: Chequia, Eslovaquia y Eslovenia

23
muestras recogidas de noviembre de 2025 a julio de 2026

Publicado por Group-IB, 12 de agosto de 2026

Cómo funciona el ataque

1

La llamada

Un operador de vishing contacta con la víctima haciéndose pasar por el banco u otra parte de confianza.

2

La instalación

La víctima instala una app; cada compilación de SpyNote lleva el nombre de la víctima.

3

La tarjeta acercada

La app de retransmisión hace que la víctima acerque su tarjeta al teléfono y teclee el PIN, y lo reenvía a una mula.

4

El efectivo

La mula paga o retira efectivo con la tarjeta retransmitida.

5

La toma de control

A través de SpyNote, el operador maneja el teléfono y abre la app bancaria auténtica.

Detecte si la pantalla se comparte o se controla en remoto

6

El préstamo

En al menos un caso, los operadores pidieron un préstamo a nombre de la víctima desde esa app.

Controles reforzados en el servidor para préstamos, beneficiarios y límites

LO QUE ENCONTRÓ NUESTRO ANÁLISIS

Detección de control remoto en la app **33,0 %**

Atestación en el servidor (Play Integrity) **16,0 %**

Porcentaje de apps Android. La toma de control se produce dentro de la app real en el dispositivo real de la víctima, así que la vinculación al dispositivo y las comprobaciones de la SIM se superan. Solo la app puede ver que su pantalla se está manejando desde otro lugar.

QUÉ LO HABRÍA EVITADO

- Detecte la pantalla compartida y el control remoto, y envíe la señal al motor de riesgo del banco.
- Exija una aprobación nueva y vinculada a una clave para préstamos, nuevos beneficiarios y aumentos de límite.
- Trate como patrón de fraude que una app pida el PIN después de acercar una tarjeta.

Group-IB, *WindRelay and SpyNote: an NFC and RAT combination in fraud*, 12 de agosto de 2026.
No se nombra a ningún banco: Group-IB no identifica a los bancos afectados.

CASO DE ESTUDIO 3 DE 4 · LA APP SUSTITUIDA

Hirudo: el troyano que sustituye su app bancaria.

Un troyano bancario para Android que no se limita a dibujar pantallas falsas. Desinstala la app real e instala una copia parcheada cuyos hooks ocultos dan respuestas falsificadas a los propios controles de seguridad de la app.

42
apps financieras en la lista de objetivos de Hirudo

8
apps bancarias de 7 bancos indonesios con una copia parcheada ya preparada

1
línea de código añadida a cada copia para cargar el motor de hooking

Publicado por ThreatFabric, 14 de octubre de 2026

Cómo funciona el ataque

1

El señuelo

Una app funcional de compras, microdramas, fútbol o vídeos para adultos.

2

La falsa actualización

El señuelo instala el troyano, que pide acceso a Accesibilidad y a las notificaciones.

3

Los secretos

Falsas pantallas de pago, del banco y de billeteras recogen PIN y contraseñas; una falsa pantalla de patrón obtiene el código de desbloqueo.

4

El objetivo

El troyano localiza una de las ocho apps bancarias objetivo y comprueba su certificado de firma.

5

El cambio

Un falso aviso de actualización abre el desinstalador y luego el troyano instala él mismo la copia parcheada.

6

La toma de control

La copia se ejecuta con señales de seguridad falsificadas mientras el operador observa la pantalla en directo.

Compruebe en el servidor el veredicto de Play Integrity para cada acción protegida

Dentro de la app parcheada

La copia conserva el nombre y el número de versión originales, pero está firmada con una clave de prueba pública de Android; por eso hay que eliminar antes la app auténtica. Una línea añadida carga un motor de hooking que solo se activa si existe un archivo escrito por el troyano.

Acceso remoto y recopilación

Visualización de la pantalla y sesiones de cámara en directo, un rastreo de los SMS de 90 días y objetivos de credenciales en China, la India, México, Marruecos y Tailandia. Un servidor del operador sin proteger contenía miles de credenciales robadas y perfiles financieros.

ThreatFabric, *Hirudo: from fake updates to patched banking apps*, 14 de octubre de 2026.

BleepingComputer, *Hirudo Android malware replaces banking apps to evade security checks*, 14 de octubre de 2026.

No se nombra a ningún banco: ThreatFabric no identifica a los bancos indonesios. Lo que encontró nuestro análisis: en la página siguiente.

Dentro de la copia, cualquier control puede falsearse.

Hirudo ejecuta los propios controles del banco dentro de un proceso que controla el atacante, y los responde él mismo. Entre el 61 % y el 85,4 % de las apps bancarias Android incorporan los controles en la app que falsifica.

LA PREGUNTA QUE HACE LA APP	LO QUE RESPONDE HIRUDO	APPS ANDROID QUE LA HACEN
Certificado de firma «¿Es esta la clave de firma del banco?» →	RESPUESTA FALSIFICADA DE HIRUDO Devuelve el certificado auténtico y oculta la firma con la clave de prueba.	Control de firma o de reempaquetado **85,4 %**
Servicios de accesibilidad «¿Hay otra app controlando la pantalla?» →	RESPUESTA FALSIFICADA DE HIRUDO Devuelve una lista vacía y oculta el servicio de control del troyano.	Protección contra superposiciones o abuso de accesibilidad **75,6 %**
Bloqueo de capturas «¿Se puede grabar esta pantalla?» →	RESPUESTA FALSIFICADA DE HIRUDO Elimina el indicador, de modo que las pantallas bancarias pueden verse y grabarse en remoto.	Protección contra capturas **61,0 %**
Atestación de claves por hardware «¿Está la clave en hardware seguro?» →	RESPUESTA FALSIFICADA DE HIRUDO Responde con un keybox de hardware filtrado cuyos certificados Google ha revocado.	No contabilizado: no puede distinguirse de otras llamadas de atestación
Play Integrity «¿Es la app auténtica en un teléfono auténtico?» →	RESPUESTA FALSIFICADA DE HIRUDO Envía la solicitud al servidor del atacante, que devuelve un veredicto favorable que la app acepta.	Llamada a Play Integrity **16,0 %**

Hooks: ThreatFabric. Porcentajes: apps Android con el control en el código propio del banco o dentro de un SDK integrado; Play Integrity: apps con código legible. Que un control exista no significa que resista un hook.

Lo que sigue funcionando: respuestas que el servidor del banco comprueba por su cuenta

- Verifique Play Integrity en el servidor, vinculado a la sesión y a la acción protegida.
- Compruebe los certificados de atestación de claves con la lista de revocación de Google.
- Mantenga en el servidor los controles de riesgo de las transacciones en el acceso, la recuperación de credenciales, los nuevos beneficiarios y la aprobación de pagos.
- Incorpore las señales de accesibilidad y de captura de pantalla a la puntuación de riesgo en lugar de usarlas como bloqueos aislados.

Fuentes: ThreatFabric (hooks); análisis de Ostorlab (apps).

CASO DE ESTUDIO 4 DE 4 · LA CLAVE FILTRADA

La clave de API de Google que se convirtió en una credencial de IA.

Google llevaba mucho tiempo diciendo a los desarrolladores que sus claves de API, las cadenas que empiezan por `AIza`, no son secretos: identifican un proyecto para Maps o Firebase y están pensadas para ir en las apps. Pero lo que una clave puede alcanzar se define en el proyecto en la nube, a menudo por otro equipo, mucho después de publicada la app.

2863
claves de API de Google activas con acceso a Gemini halladas en datos web públicos

32
claves activas con acceso a Gemini en 22 apps Android populares

82 314 $
de factura de Gemini declarada por una víctima de una clave abusada

Publicado por Truffle Security, febrero de 2026, y CloudSEK, abril de 2026

Cómo una clave inofensiva se convierte en una credencial de IA

1 → 2 → 3 → 4

La clave va en la app

La app lleva una clave de API de Google para Maps o Firebase, tal como permite la documentación de Google.

Restrinja cada clave publicada a las API y a la firma de app que la necesitan

Se activa Gemini

Otro equipo activa la Generative Language API en el mismo proyecto en la nube.

Mantenga las API de IA en un proyecto cuyas claves nunca lleguen a un dispositivo

La clave obtiene acceso a la IA

Todas las claves existentes del proyecto pueden ahora llamar a Gemini. En la app no cambia nada.

El abuso

Un atacante extrae la clave de la app, lee los archivos subidos a Gemini y dispara la factura: a una víctima se le cobraron 82 314 $.

LO QUE ENCONTRÓ NUESTRO ANÁLISIS

Apps Android	80,3 %
Apps iOS	30,6 %
Apps HarmonyOS	71,4 %

Porcentaje de apps con al menos una clave de API de Google en cualquier parte del paquete; el 72,5 % del total de apps. Las claves no se probaron: la mayoría probablemente esté limitada a Maps o Firebase, y el equipo de la app no puede saberlo a partir de la clave.

QUÉ LO HABRÍA EVITADO

- Restrinja cada clave a las API que necesita y al certificado de firma de la app.
- Mantenga Gemini y las demás API de IA en un proyecto en la nube independiente.
- Rote cualquier clave que se haya publicado en una app antes de activar una API nueva.

Truffle Security, *Google API keys weren't secrets, but then Gemini changed the rules*, 25 de febrero de 2026.
CloudSEK, *Hardcoded Google API keys in top Android apps now expose Gemini AI*, 7 de abril de 2026.
No se nombra a ningún banco: ninguna de las dos fuentes identifica a las entidades financieras cuyas claves quedaron expuestas.

Qué deben hacer los bancos en 2026: las 10 prioridades.

Diez acciones, cada una vinculada a un hallazgo de este informe y a un grupo de controles de OWASP MASVS, ordenadas según lo directamente que reducen el fraude.

01 Verifique la app en el servidor

Use Play Integrity y App Attest, compruebe el veredicto en el servidor y rechace las solicitudes que no lo superen. Es la única defensa que una app parcheada o sustituida no puede desactivar.

79,8 % de las apps no usan atestación

MASVS-RESILIENCE

02 Vincule cada acción sensible a una clave

Haga pasar los accesos y las aprobaciones de pago por biometría vinculada a una clave respaldada por hardware, nunca por una comprobación de sí o no.

35,1 % de las apps Android tienen una biometría eludible

MASVS-AUTH MASVS-CRYPTO

03 Ofrezca llaves de acceso

Añada el acceso con llaves de acceso y publique los asset links y dominios asociados correspondientes, para que una contraseña robada por phishing deje de bastar.

4,9 % integran una API de llaves de acceso

MASVS-AUTH

04 Saque los secretos de la app

Traslade al servidor las claves privadas, las claves de la nube y los tokens de servicio, y emita tokens de corta duración. Restrinja las claves que deban ir en la app a la firma de su app y a las API que necesita.

20,3 % embeben credenciales aparte de las claves de API de Google

MASVS-STORAGE MASVS-CRYPTO

05 Cierre la redirección del inicio de sesión

Devuelva los inicios de sesión mediante enlaces universales y app links que solo su app pueda reclamar, nunca mediante esquemas de URL personalizados que otra app pueda registrar.

21,1 % de las apps iOS permiten un robo de cuenta OAuth

MASVS-PLATFORM MASVS-AUTH

06 Detecte el control remoto y las superposiciones

Combine la detección de root, hooking, manipulación, superposiciones y pantalla compartida, active los controles que ya incluyen sus SDK y pruébelos en dispositivos reales.

33 % de las apps Android incorporan detección de control remoto

MASVS-RESILIENCE

07 Sepa qué publica

Mantenga una lista de materiales de software para cada versión, incluidos los SDK y las plataformas de proveedores, y corrija los componentes críticos en un plazo fijado.

41,1 % incluyen un componente vulnerable

MASVS-CODE

08 Cifre todas las conexiones

Desactive el tráfico en texto claro, ancle los certificados de sus propias API y limite los WebView a sus propias páginas.

29,4 % de las apps Android permiten tráfico sin cifrar

MASVS-NETWORK MASVS-PLATFORM

09 Vigile los dispositivos antiguos

Compruebe el nivel de parches del sistema operativo al iniciar sesión y limite las acciones de alto riesgo en los dispositivos que ya no reciben actualizaciones.

99,5 % de las apps Android funcionan en Android sin parches

MASVS-CODE

10 Publique etiquetas veraces y un contacto visible

Alinee las etiquetas de privacidad de las tiendas con lo que hace la app y publique un security.txt para que los investigadores puedan contactar con usted.

7,1 % de los dominios bancarios publican security.txt

MASVS-PRIVACY

Definiciones y notas sobre los datos.

Muestra

El estudio abarca las apps móviles de los 500 principales bancos. Se recopilaron 2841 fichas de apps y se descargaron y analizaron 2686, en Android, iOS y HarmonyOS. Los países y regiones siguen el mercado de origen del banco.

Severidad

La severidad de una app es su hallazgo crítico, alto, medio o bajo más grave. «Potencial» (un patrón que debe confirmar una persona) y «refuerzo» (una salvaguarda ausente) no cambian esa calificación; un gráfico que los cuenta lo indica. «Alto o crítico» significa al menos un hallazgo de cualquiera de esos niveles; «bajo o inferior» significa ningún hallazgo crítico, alto ni medio.

Reglas específicas de plataforma

Las reglas de elusión biométrica, redirección de intents, serialización, criptografía, tráfico sin cifrar y almacenamiento solo se ejecutan en Android; las de App Transport Security y manifiesto de privacidad, solo en iOS. Sus porcentajes usan como denominador las apps de esa plataforma.

Valores desconocidos

Cuando el código de una app está empaquetado o es ilegible, los controles devuelven «desconocido». Esas apps se excluyen del denominador de ese control y su número se indica junto a la cifra. Los gráficos de blindaje muestran lo desconocido como un segmento propio.

Credenciales embebidas

Secretos con un formato reconocido, como claves de API, tokens de acceso o claves privadas. Las claves de API de Google Cloud se indican por separado. No se comprobó la validez de las claves.

Llaves de acceso y atestación

API de llaves de acceso integrada significa que la app llama a Android Credential Manager, a la API FIDO2 de Google o a las API de llaves de acceso de AuthenticationServices de Apple. Las clases FIDO2 incluidas por otras bibliotecas no cuentan. Atestación significa Play Integrity, SafetyNet, HMS Safety Detect, App Attest o DeviceCheck.

Blindaje

Protecciones halladas en el código o en productos integrados, en las tres plataformas. En iOS, la detección de jailbreak sustituye a la de root y la protección contra superposiciones no se aplica. La presencia no se probó en dispositivos.

Versiones de SO sin parches

Android y HarmonyOS: por debajo del nivel de API 34 (Android 14), sin parches del boletín de seguridad de Android desde marzo de 2026. iOS: por debajo de iOS 18, la versión principal más antigua a la que Apple sigue aplicando todos los parches.

Datos del lado del banco

La exposición de backends y las CVE proceden del índice pasivo InternetDB de Shodan y se deducen de las versiones, sin probarse. Los registros de brechas proceden de VCDB, Have I Been Pwned, ransomware.live, informes 8-K de la SEC y, para los G-SIB, de noticias y reguladores; cada coincidencia se revisó a mano. Las certificaciones son declaraciones de las webs.

Datos externos

Las comprobaciones web y de correo cubren 1252 dominios bancarios. La compatibilidad poscuántica se leyó de negociaciones TLS registradas. Las listas de objetivos de troyanos proceden de 47 listas publicadas. Los hosts de phishing proceden de una única instantánea de cuatro fuentes públicas. Las etiquetas de privacidad proceden de Google Play y App Store. Para las 142 webs bancarias que no pudimos abrir, leímos la copia de archivo pública más reciente (Internet Archive) de 2025 o posterior; las copias archivadas pueden ser más antiguas que el sitio activo.

Estadísticas de fraude

536 cifras publicadas por reguladores, bancos centrales y organismos del sector, cada una con su periodo y su población. Describen el fraude en cada mercado, no pérdidas causadas por las debilidades de este informe.

Casos de estudio

Resúmenes de investigaciones públicas, citadas en cada página. Las cifras de análisis que las acompañan son nuestras.

Ostorlab

Informe **2026** de seguridad de aplicaciones de banca móvil

Versión 3 · 12 de noviembre de 2026