Telefónica

REPORTE DE TENDENCIAS_

Informe global de aplicaciones bancarias

En colaboración de:

etisalat | SoftBank | Singtel

CYBER SECURED BY ElevenPaths

elevenpaths.com

Índice

1. Resumen ejecutivo.

A medida que el mundo se vuelve digital, surgen nuevas oportunidades y amenazas.

Este informe pretende ofrecer una visión general de algunas de las amenazas digitales para una de las industrias más importantes y de mayor confianza: el **sector bancario**.

A medida que seguimos creciendo digitalmente, tendemos a centrarnos más en los negocios. Esto significa que cuando estamos tratando de desarrollar un nuevo producto, sitio web o aplicación, entre otros, tendemos a priorizar la velocidad, conveniencia y facilidad de implementación **en lugar de la seguridad**.

Este informe aborda lo que consideramos tres aspectos clave, importantes y a menudo olvidados, de la seguridad:

- La **seguridad** integrada **en las aplicaciones móviles**
- Los **metadatos** disponibles **en los documentos públicos**
- La **información** que podemos obtener **sobre las comunicaciones de los servicios y su calidad** (es decir, los puertos abiertos en los servidores, sus vulnerabilidades, etc.).

Los resultados obtenidos pueden darnos información como el desarrollador de aplicaciones para móviles y averiguar si este desarrollador trabaja con otras empresas (y si puede estar reutilizando código no optimizado para la aplicación bancaria, o incluso descubrir servicios "ocultos" y normalmente más inseguros).

Estos tres aspectos de la seguridad se conocen como seguridad periférica en comparación con la seguridad más tradicional, como los controles de acceso, el endurecimiento de los servidores....

Intentaremos arrojar algo de luz sobre estas cuestiones.

2. Introducción

Hemos realizado un estudio global con el objetivo de determinar el nivel de madurez de los controles de seguridad en **las aplicaciones móviles de los bancos** y **los metadatos contenidos en los archivos públicos**. Este informe se ha realizado para evaluar cómo los bancos están protegiendo sus aplicaciones móviles, la prevención de fugas de información de metadatos y los dispositivos y hosts expuestos en Internet.

El análisis se basa en archivos públicos, aplicaciones web y móviles de **56 de los mayores bancos del mundo**. Además, hemos investigado los dos principales bancos de algunos de los países más importantes de todos los continentes/regiones. El objetivo es ofrecer una visión general de lo que los bancos están haciendo en cada región con respecto a sus servicios de atención al cliente en línea.

Hemos analizado la aplicación oficial del banco utilizando dos herramientas desarrolladas y propiedad de uno de los miembros de la Alianza, para evaluar qué vulnerabilidades tiene cada aplicación y proporcionar una puntuación de vulnerabilidad. Además, hemos investigado qué permisos pide cada aplicación y cuál es la relación entre ellos.

Para ver los metadatos en los archivos, hemos utilizado documentos públicos detectados en los dominios del banco, a los que puede acceder cualquier usuario de la red a través de los motores de búsqueda o directamente en los sitios web de los diferentes bancos.

El estudio se centró en la obtención de información de fuentes públicas. En ningún momento se intentó acceder a documentos privados o confidenciales. Sin embargo, toda la información que podría ayudar a identificar a un banco y sus vulnerabilidades ha sido borrada (o borrada) y filtrada para evitar que los posibles atacantes puedan utilizarla para llevar a cabo una acción maliciosa contra las compañías financieras.

En este informe, la información se recopila a partir de tres fuentes principales:

- **FOCA OpenSource**, una herramienta gratuita para encontrar documentos a través de los buscadores. Una vez descargados los documentos, la FOCA extrae los metadatos contenidos en los archivos y los analiza.

- **Tacyt** y **mASAPP**, dos herramientas de desarrollo propio que se centran en encontrar vulnerabilidades de aplicaciones móviles entre muchas otras funcionalidades.

- **Censys** (Se definen a sí mismos como "Security driven by data"), un buscador público de servidores y dispositivos expuestos a Internet. Censys también permite encontrar hosts y servicios específicos asociados a los dominios del banco que proporcionamos y ver cómo se configuran los sitios web y los certificados.

3. Metodología

La primera etapa consistió en determinar cuántos bancos analizar y desde qué países. Queríamos dar una visión de seguridad del sector bancario en todo el mundo. Por lo tanto, decidimos dividir el mundo en siete regiones (Asia, Oriente Medio, América del Norte, América del Sur, Europa, África y Oceanía).

A continuación, seleccionamos los mejores países para cada región - la cantidad de países seleccionados dependía de la región (2 para Oceanía y América del Norte; 5 para Europa, África, Asia y América del Sur; 4 para el Medio Oriente). **28 países** en total.

Elegimos dos bancos bien establecidos en cada país, un total de **56 bancos** en todo el mundo.

Utilizamos las herramientas de **Tacyt** y **mASAPP** para analizar la aplicación oficial más actualizada de cada banco. Sólo nos hemos ocupado de las aplicaciones móviles para Android.

Tacyt nos ayudó a:

- Hacer comparaciones entre las aplicaciones en términos de número de **permisos** requeridos y sus características específicas.
- Obtener las cantidades totales de las aplicaciones oficiales de cada banco actualmente disponibles en Google Play.
- Para obtener estos resultados, comprobamos la principal aplicación oficial del banco para obtener su nombre de desarrollador asociado y ejecutamos esta consulta (cambiando <DeveloperName> por el nombre real del desarrollador registrado):

developerName:" *<DeveloperName>*" -deadDate:* origin:GooglePlay categoryName:Finance

- Esta consulta sólo se refiere a las aplicaciones de un desarrollador (la que hizo la aplicación principal). El escenario más frecuente es tener sólo uno, pero un banco puede tener muchos desarrolladores diferentes para sus diferentes aplicaciones oficiales. Probamos diferentes consultas adicionales personalizadas y adaptadas a cada banco, para obtener resultados más precisos.
- Posteriormente utilizamos **mASAPP** para analizar cada aplicación móvil y obtener la puntuación general de seguridad, las vulnerabilidades y el comportamiento de riesgo.
- También se buscaron aplicaciones no oficiales relacionadas con cada banco. Esto era más difícil de hacer porque cada cargador puede cambiar cualquiera de los parámetros originales (título, nombre del desarrollador, categoría, etc.) y hacerlo más difícil de encontrar.
- Utilizamos muchas consultas diferentes para cada caso, pero siempre empezamos con este (cambiando <Palabras clave del nombre> por las palabras clave del nombre de cada banco):

(<Palabras clave del nombre>) AND (-deadDate:* AND -origin:GooglePlay -origin:AppleStore)

Tuvimos que eliminar algunas cláusulas como **categoryName:Finance** porque nos dimos cuenta de que muchas aplicaciones se volvieron a cargar en mercados no oficiales sin cierta información.

Para el análisis de metadatos, utilizamos **FOCA**. **FOCA** nos permite encontrar los documentos digitales expuestos públicamente por los dominios de los bancos. Una vez detectados todos ellos, **FOCA** descarga estos documentos y extrae sus metadatos.

Al extraer los metadatos, es posible obtener información como nombres de usuario, direcciones IP, direcciones de correo electrónico, nombres de red, directorios de almacenamiento y sistemas operativos. A partir de esta información, es posible inferir procesos inseguros o malas prácticas desde la perspectiva de la seguridad de la información (uso de

usuarios genéricos, sistemas operativos obsoletos, correos electrónicos expuestos a fugas de credenciales, correos electrónicos de dominios no oficiales en documentos oficiales, etc.).

Finalmente, utilizando **Censys**, encontramos cualquier host relacionado con el dominio oficial de cada banco. Censys dispone de un motor de búsqueda de dominios que muestra una enorme cantidad de información relacionada con cada resultado (información relacionada con cada puerto abierto, así como atributos adicionales como dirección IP, ubicación, etc.) en forma de "atributos de resultado".

Si insertamos un dominio de la empresa (domain.com) en la barra de búsqueda de Censys:

- Busca coincidencias **parciales** de esta entrada en todos los atributos del resultado y devuelve los hosts como resultado.
- **Excepto** en uno: Para el puerto 443: *443.https.tls.certificate.parsed.names*, sólo muestra los hosts como nuevo resultado si el valor buscado coincide exactamente con uno de los que contiene.
  Por ejemplo, si el atributo *443.https.tls.certificate.parsed.names* de un host tiene los valores "www.domain.com" o "mail.domain.com" y hemos insertado "domain.com" en la barra de búsqueda, **no** lo considerará una coincidencia exacta y no se tomará como un resultado válido. Como queremos obtener coincidencias parciales en cada atributo, añadimos *"443.https.tls.certificate.parsed.names:domain.com"* a la consulta y unimos las condiciones de búsqueda con OR.

Para eliminar esos resultados incluyendo el dominio, **pero no** relacionados con el banco, dejamos caer los que sólo tenían coincidencias en su cuerpo http. Estos resultados suelen ser sitios no relacionados que mencionan al banco o que **no tienen ninguna relación** con su sitio web oficial. Por lo tanto, añadimos *NOT 80.http.get.body: Dominio de la empresa>* a la consulta con *AND*.

La consulta final para obtener los resultados más cercanos a lo que queremos es:

(<Dominio de la empresa> OR 443.https.tls.certificate.parsed.names: <Dominio de la empresa>) AND (NOT 80.http.get.body: <Dominio de la empresa>)

Optamos por mostrar resultados incluyendo **Akamai**. En caso de que los resultados de Akamai no se consideraran relevantes, sólo tendríamos que añadir "*AND NOT Akamai*" al final de la consulta.

Esta consulta inicial nos sirvió para darnos una visión general y conseguir que estos primeros resultados estuvieran presentes en este informe, ya que, utilizando la misma consulta para todas las búsquedas, esperamos tener resultados más coherentes.

Una vez recopilada toda la información proporcionada por estas herramientas, realizamos un análisis y determinamos qué información era relevante. Decidimos anonimizar todas estas entidades y evitar cualquier daño potencial a su imagen.

Toda esta Metodología puede ayudar a las empresas a identificar los **activos de TI "ocultos"**.

4. Resultados

En esta sección, presentamos los resultados que consideramos relevantes para mostrar.

4.1. Análisis de aplicaciones móviles y resultados

4.1.1. Puntuación de riesgo global

Usando **mASAPP**, pudimos obtener una puntuación de riesgo para cada aplicación móvil oficial. **mASAPP** calcula esta puntuación analizando el tipo de vulnerabilidades presentes en la aplicación y el número de veces que éstas ocurren dentro de la aplicación.

Una puntuación de 0 significa que la aplicación no tiene vulnerabilidades detectables y una puntuación de 10 significa que es muy insegura. Se encontró que la puntuación media por región fue de **7,27** (considerada una puntuación alta para la aplicación). Esto significa que casi todas las aplicaciones bancarias tienen **al menos una vulnerabilidad grave**.

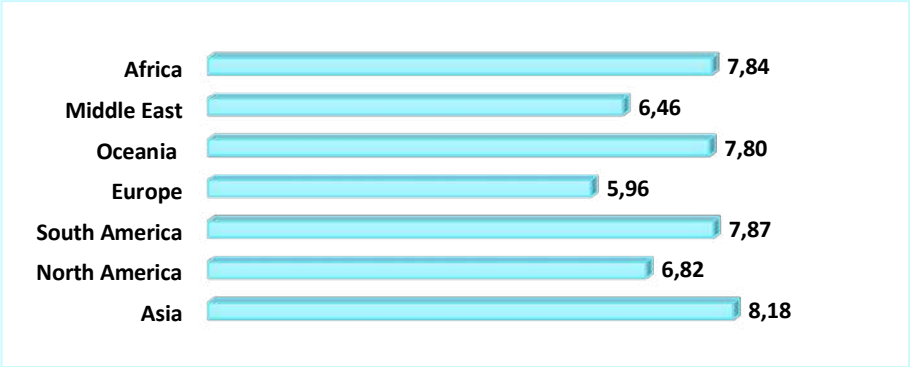

Figura 1. mASAPP – Puntuación de riesgo global

Como se observa en el gráfico anterior, Asia, África y América del Sur tienen los mayores riesgos - considerados como **HIGH (altos)**-, mientras que Europa, Oriente Medio y Norteamérica tienen una puntuación de riesgo **MEDIUM (media)**. No todos los bancos analizados en África disponían de una aplicación móvil.

A un nivel muy alto, esto significa que los bancos en las áreas donde el puntaje de riesgo es más alto tienen más vulnerabilidades en promedio.

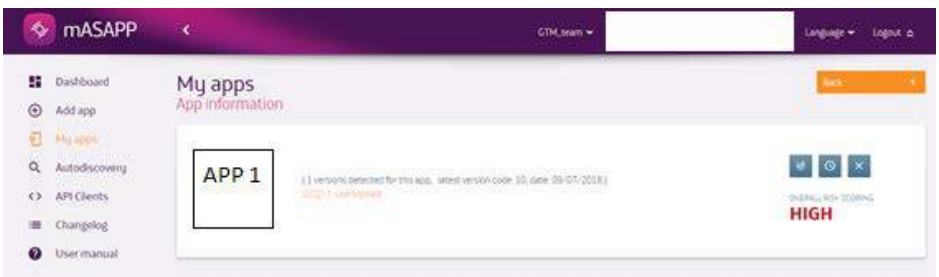

Imagen 1. mASAPP – Resumen de alto nivel

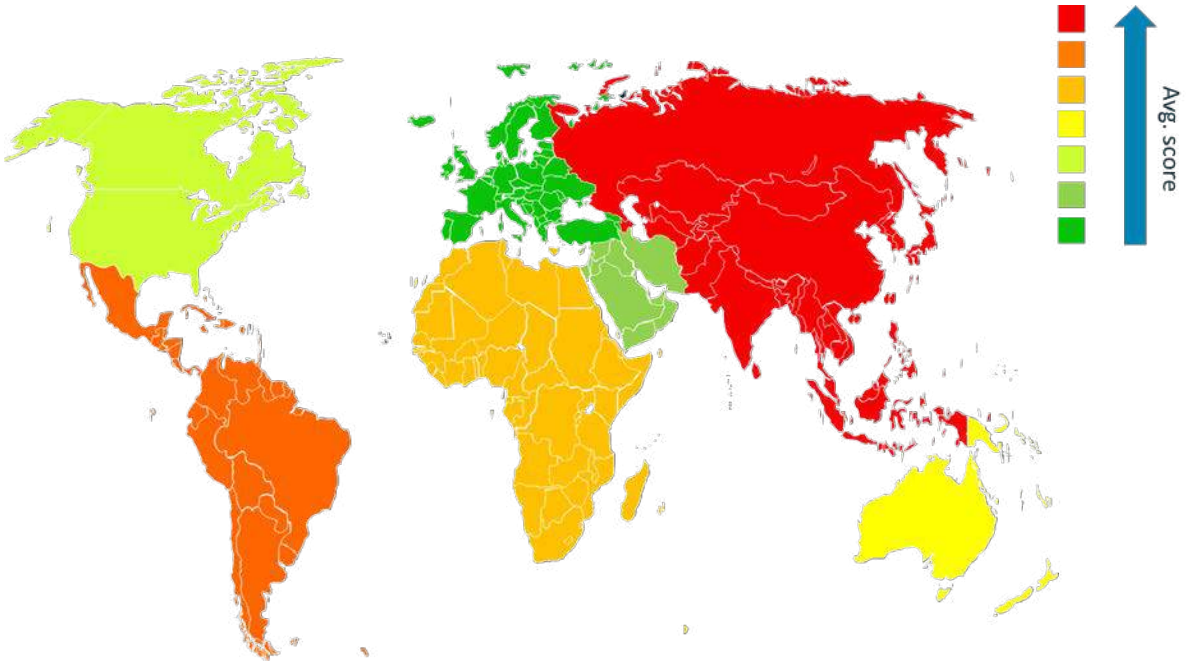

Imagen 2. mASAPP – Puntuación de riesgo global por región

4.1.2. Vulnerabilidades

Las clases de vulnerabilidades que **mASAPP** puede identificar incluyen **Calidad de Código, Uso Inapropiado de la Plataforma, Criptografía, Almacenamiento de Datos y Privacidad, Comunicación de Red y Reputación** entre otras.

La vulnerabilidad de alto riesgo más común fue la **"Potencial Inyección SQL"** que estaba presente en **34 de las 53** aplicaciones (56 bancos, 3 de los cuales no tenían una aplicación móvil).

La **inyección de SQL** (o *SQL injection*) es una técnica de inyección de código utilizada para atacar aplicaciones basadas en datos, en la que se insertan instrucciones SQL maliciosas en un campo de entrada para su ejecución. Un ataque exitoso de inyección SQL podría extraer datos de clientes (como números de tarjetas de crédito), lo que es extremadamente importante en el sector bancario, ya que las aplicaciones móviles pueden transportar datos muy sensibles.

La segunda vulnerabilidad más común encontrada afectó a **17 de las 53** solicitudes bancarias -aproximadamente un 32% de los bancos del estudio- y fue el "***Insecure Certificate Signature Algorithm***" **(Algoritmo de firma de certificados inseguros).**

En aplicaciones con esta vulnerabilidad, el certificado de la aplicación se firma con un **algoritmo hash inseguro** (como MD5 o SHA1). Esta vulnerabilidad podría permitir a los atacantes llevar a cabo ataques de suplantación de identidad.

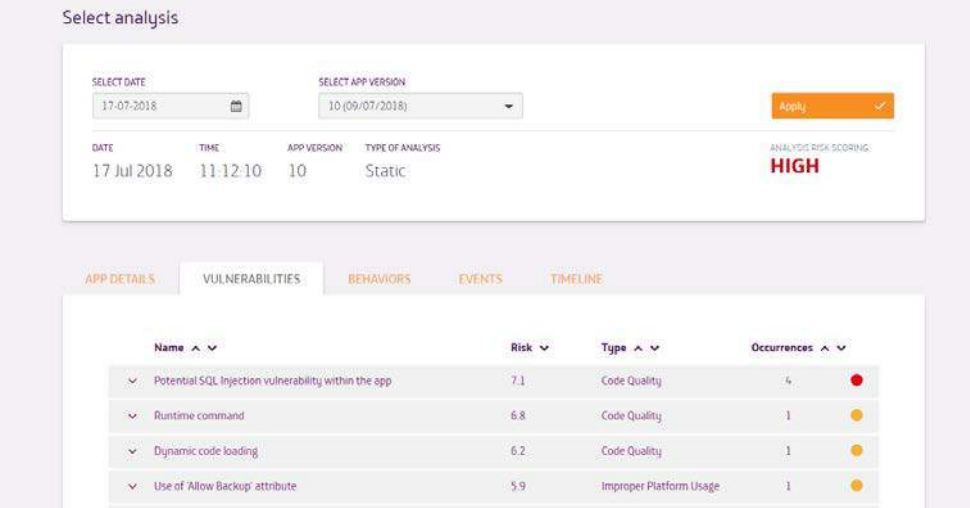

Imagen 3. mASAPP – Vulnerabilidades identificadas

Muchas de las vulnerabilidades más comunes tenían la causa principal en la calidad del código. Esto podría haber ocurrido porque los equipos que desarrollaron las aplicaciones móviles no siguieron las medidas de seguridad adecuadas para garantizar que el entorno fuera seguro, sino que se centraron más en la comodidad, la velocidad, la interfaz de usuario y/o la usabilidad del usuario.

4.1.3. Permisos

La siguiente figura muestra el número medio de permisos solicitados por cada región.

Los bancos de Oriente Medio son los que piden menos permisos, un promedio de 15, mientras que los bancos de Asia tienden a pedir más permisos, un promedio de 23. Una diferencia de 8 permisos en las solicitudes de los principales bancos que se supone que deben proporcionar en general el mismo tipo de servicios. Ignoramos si esto tiene algo que ver con las diferentes culturas o regulaciones en cada área.

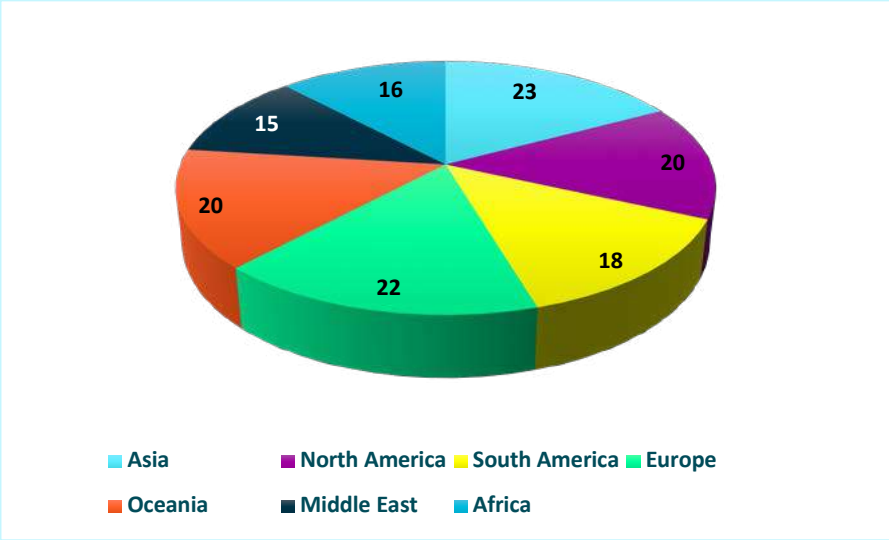

Figura 2. Medias de permisos solicitados por región.

Estos resultados llevan a la pregunta de cuántos permisos son **estrictamente necesarios**.

mASAPP destacó que muchos de los permisos solicitados se consideraban **intrusivos**. Los permisos intrusivos incluyen **permisos a nivel de sistema** (como *WRITE_SECURE_SETTINGS, INSTALL_PACKAGES, CALL_PRIVILEDGED*, etc.).

Además de esto, destacamos algunos permisos que categorizamos como **cuestionables**.

Los permisos cuestionables son aquellos que no podemos asegurar que sean intrusivos o innecesarios (ya que no conocemos exactamente todas las funcionalidades de cada aplicación bancaria), pero consideramos que podrían serlo. Algunos ejemplos de permisos que consideramos cuestionables son:

- **RECORD_AUDIO**: las aplicaciones bancarias no suelen tener ninguna funcionalidad de audio.
- **CALL_PHONE**: permite que una aplicación inicie una llamada telefónica sin pasar por la interfaz de usuario del marcador para que el usuario confirme la llamada. Esto significa que la aplicación puede hacer llamadas telefónicas sin que el usuario tenga que pulsar el botón de llamada. Las aplicaciones bancarias normalmente no necesitan hacer llamadas telefónicas, pero si tienen que hacerlo (por ejemplo, si la aplicación ofrece algún atajo para llamar al servicio de atención al cliente), deben permitir que el usuario confirme la llamada cada vez que lo haga.
- **READ_CALL_LOG** y **READ_CONTACTS**: el registro de llamadas del usuario debe ser irrelevante para el banco y sus aplicaciones. Lo mismo para los contactos de la agenda del usuario.
- **READ_SMS**: permitir que la aplicación lea los SMS le permite leer todos los mensajes, no sólo los enviados por el banco. La aplicación podría analizar los mensajes del banco para obtener información procesada para el usuario, pero lo más probable es que sea sólo un permiso intrusivo.

Otros permisos como *CAMERA* o *ACCESS_FINE_LOCATION* pueden parecer intrusivos, pero es importante entender los servicios proporcionados y cómo estos permisos pueden mejorar la experiencia del cliente.

- El permiso *CAMERA* puede ser solicitado debido a la característica de acceder a la cuenta bancaria por métodos biométricos.
- *ACCESS_FINE_LOCATION* puede ser preguntado porque el banco necesita saber en qué país se encuentra el usuario y entender el comportamiento del usuario por razones de seguridad (por ejemplo: alguien puede estar retirando dinero en Madrid cuando el usuario y su teléfono móvil están en Singapur, lo que podría significar que alguien está cometiendo un fraude).

mASAPP encontró muchos tipos diferentes de permisos intrusivos (*permisos a nivel de sistema, emisión a nivel de sistema identificada, permisos peligrosos de Google* y *acceso a almacenamiento externo*) y algunas características peligrosas (*comando en tiempo de ejecución* y *carga de código dinámico*).

La siguiente captura de pantalla muestra los comportamientos encontrados por **mASAPP** en una aplicación bancaria en particular.

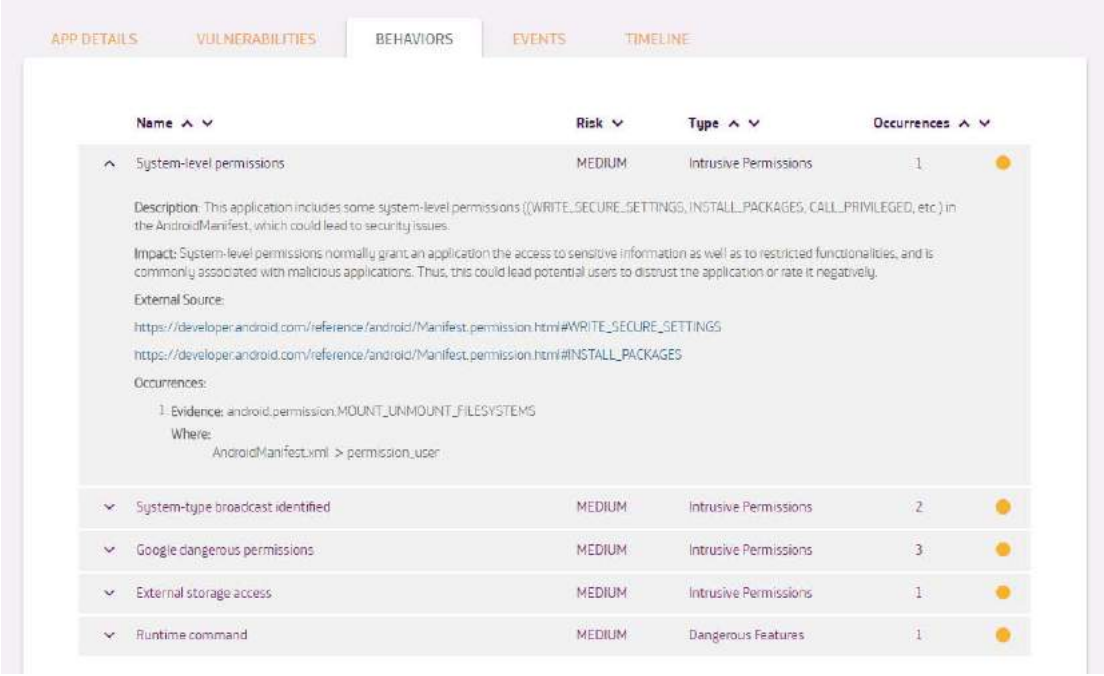

Imagen 4. mASAPP – Comportamientos identificados

Queríamos hacer una comparación de los permisos solicitados por las aplicaciones bancarias de todo el mundo para ver si eran consistentes. Lo que encontramos fue que aunque el promedio de permisos solicitados era de 19, **sólo había un permiso común a todas las aplicaciones bancarias - Permiso de acceso a Internet**.

Esto cambia cuando intentamos encontrar permisos comunes por región. En este escenario, encontramos más permisos que son comunes: de 1 en África (*INTERNET*) a 7 en Oceanía (*VIBRATE, INTERNET, com.google.android.c2dm.permission.RECEIVE, WAKE_LOCK, ACCESS_NETWORK_STATE, ACCESS_FINE_LOCATION* y *USE_FINGERPRINT*).

Usamos a **Tacyt** para estas comparaciones. Nos centramos en los permisos solicitados, pero **Tacyt** proporciona muchas otras comparaciones de datos, como se muestra en las siguientes capturas de pantalla.

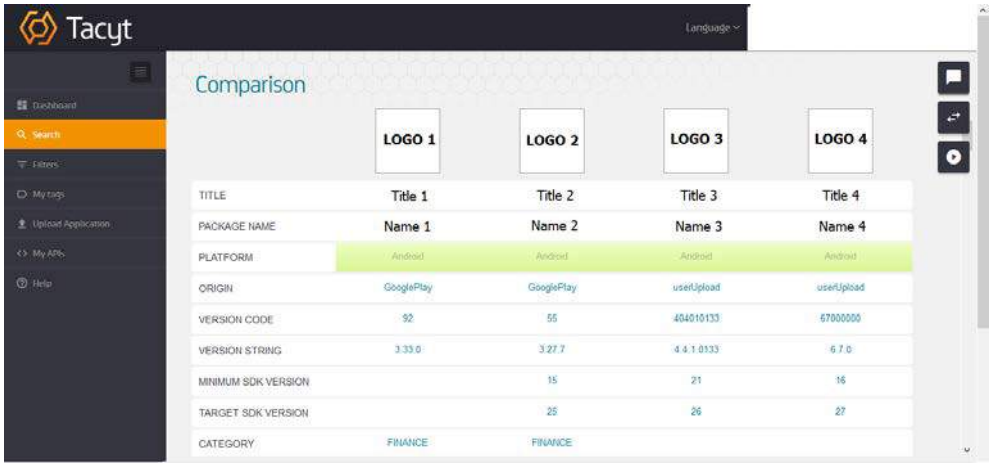

Imagen 5. Tacyt – Panel de comparaciones

Imagen 6. Tacyt – Categorías de comparaciones

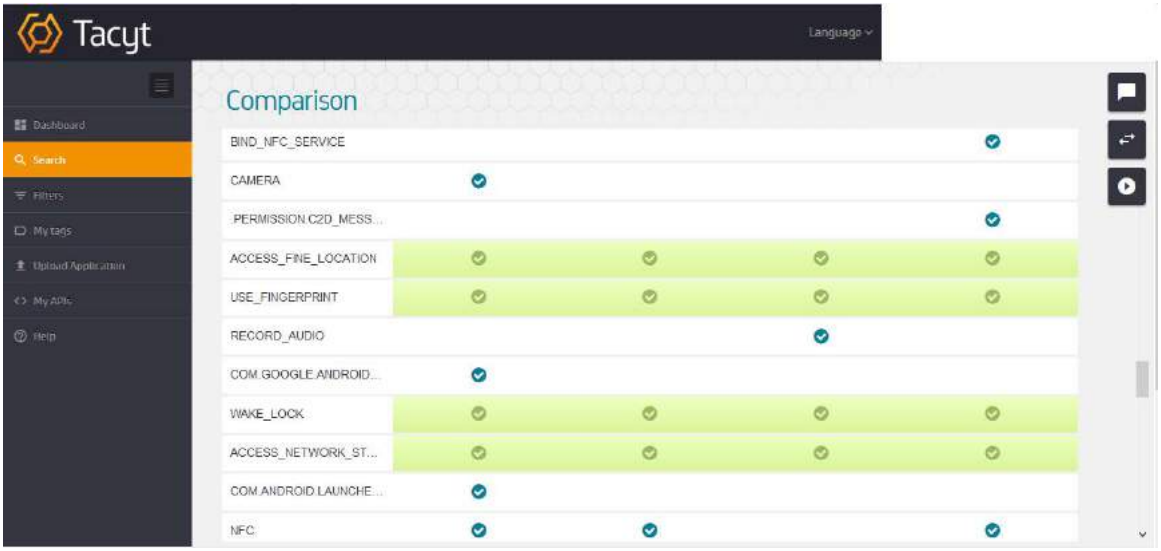

Imagen 7. Tacyt – Comparación de permisos

4.1.4. Promedio de aplicaciones en Google Play

Utilizando **Tacyt**, hemos identificado el número de aplicaciones bancarias oficiales subidas a Google Play. Cuantas más aplicaciones estén disponibles, mayores serán las oportunidades para que un potencial actor malicioso ataque al banco.

- El **promedio mundial** de solicitudes por banco es de **4**.
- **África** tiene el **promedio más bajo** por región: **2** aplicaciones.
- **Europa** tiene el **promedio más alto** por región: **11** aplicaciones oficiales.

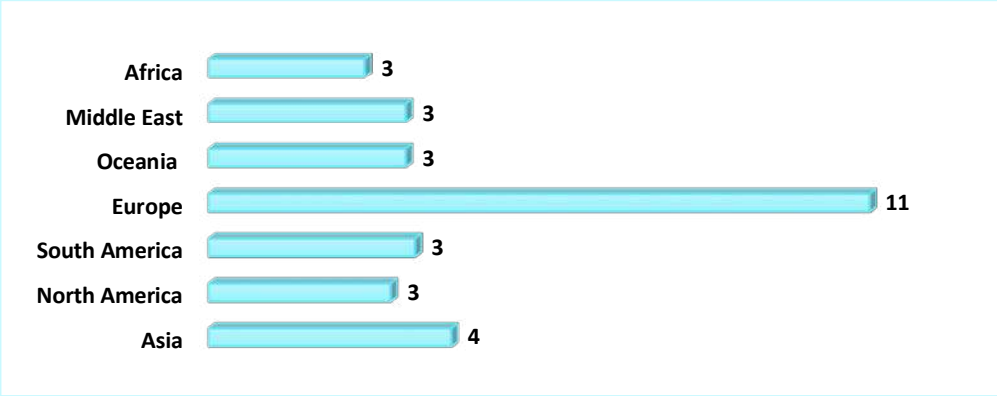

Figura 3. Tacyt - Cifras medias de aplicaciones oficiales por región en Google Play

4.1.5 Promedio de aplicaciones en mercados no oficiales.

Se realizaron búsquedas en ocho mercados no oficiales diferentes: **Aptoide, Mobogenie, NineApps, SlideMe, Mobile9, 1Mobile, Apkpure** y **A2zapk.**

La siguiente figura muestra el promedio de resultados por región:

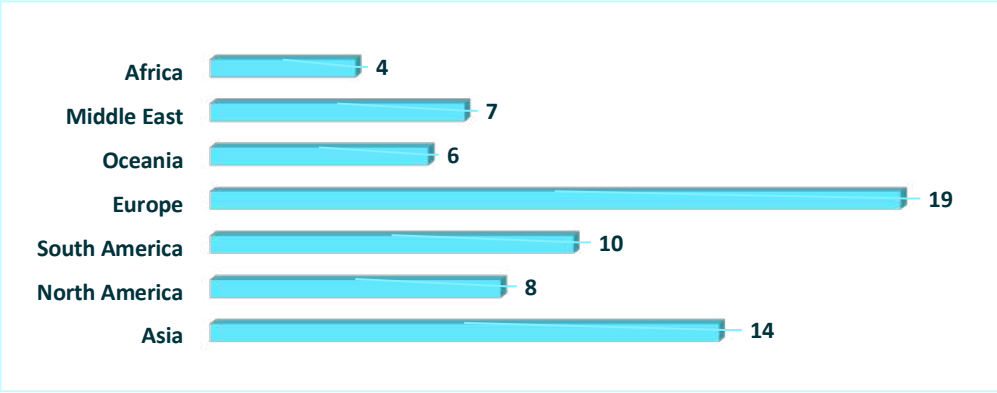

Figura 4. Tacyt – Promedio de aplicaciones por región en los principales mercados no oficiales

- El **promedio mundial** de solicitudes por banco es de **10**.
- **África** tiene el **promedio más bajo** por región: **4** aplicaciones.

- **Europa** tiene el **promedio más alto** por región: **19** aplicaciones no oficiales.
- **Asia** es la región con menos control de carga de aplicaciones. Su número de aplicaciones no oficiales es **3,5 veces** su número de aplicaciones oficiales.
- Individualmente, el banco con la mayoría de las aplicaciones no oficiales cargadas tenía **49**.
- Todos los bancos analizados tenían al menos una aplicación cargada en un mercado no oficial.

4.2. Análisis de metadatos - FOCA

Hemos realizado un análisis de los dominios de los bancos con **FOCA OpenSource** (https://www.elevenpaths.com/labstools/foca/index.html). Este análisis nos proporcionó información como cuántos documentos son públicos, qué tipo de documentos son, sistemas operativos, software utilizado, nombres y detalles de los usuarios, etc. En esta sección, señalaremos los hallazgos más relevantes.

4.2.1. Análisis inicial

Configuramos **FOCA** para que pudiera realizar una búsqueda automática de las 22 principales extensiones de archivos utilizando las claves de la API de Google, Bing y Exalead, permitiéndoles encontrar los enlaces a esos archivos y descargarlos.

En la Figura 6 se muestra la cantidad de documentos analizados por región (4 bancos en Oceanía y Norteamérica; 10 bancos en Europa, África y Asia, Sudamérica; y 8 bancos en el Medio Oriente).

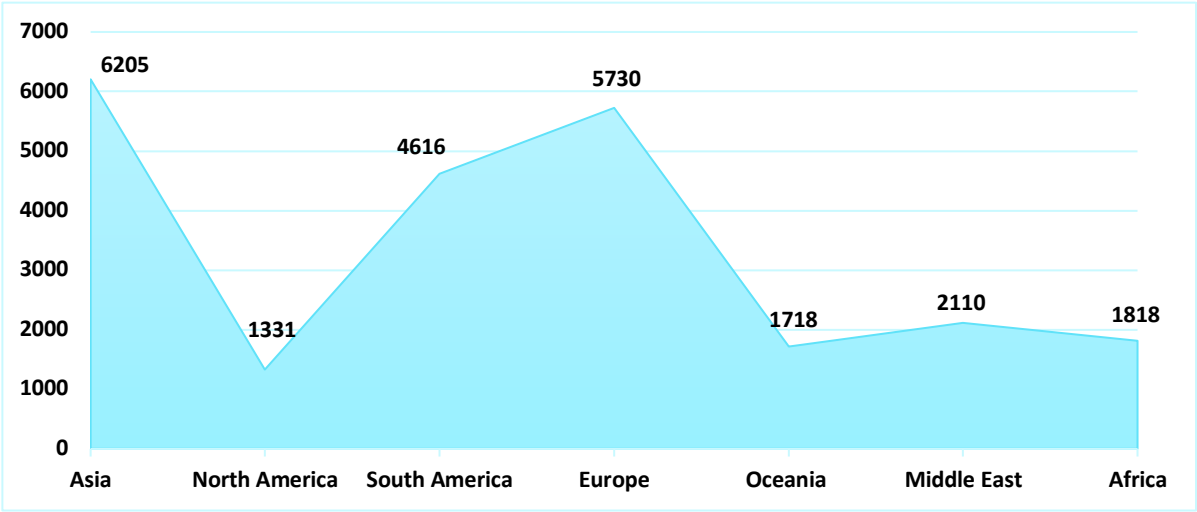

Figura 5. FOCA – Ficheros totales analizados por región

Identificamos que **la mayoría de los archivos** (75 % de ellos) **eran documentos PDF** seguidos de documentos de extensión no identificados (8 %), procesadores de texto (8 %), hojas de cálculo (7 %) y presentaciones (1 %) como se puede ver en la siguiente figura.

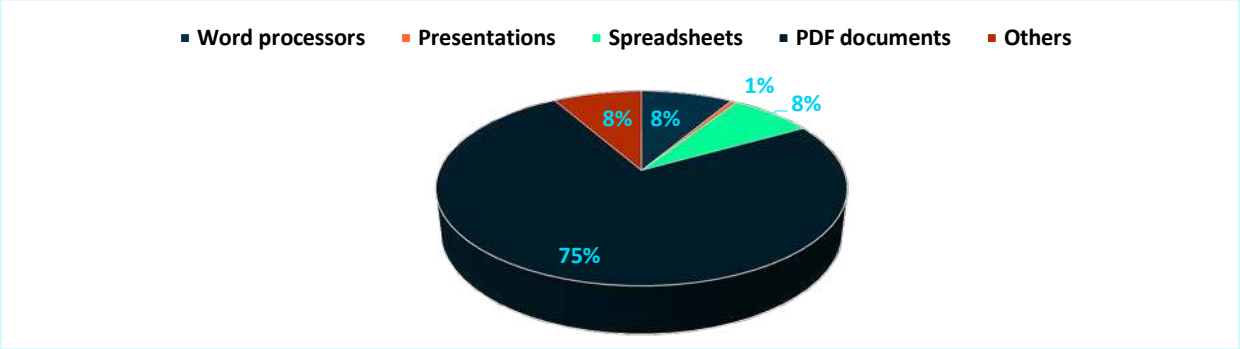

Figura 6. FOCA – Porcentajes de extensiones en los ficheros analizados

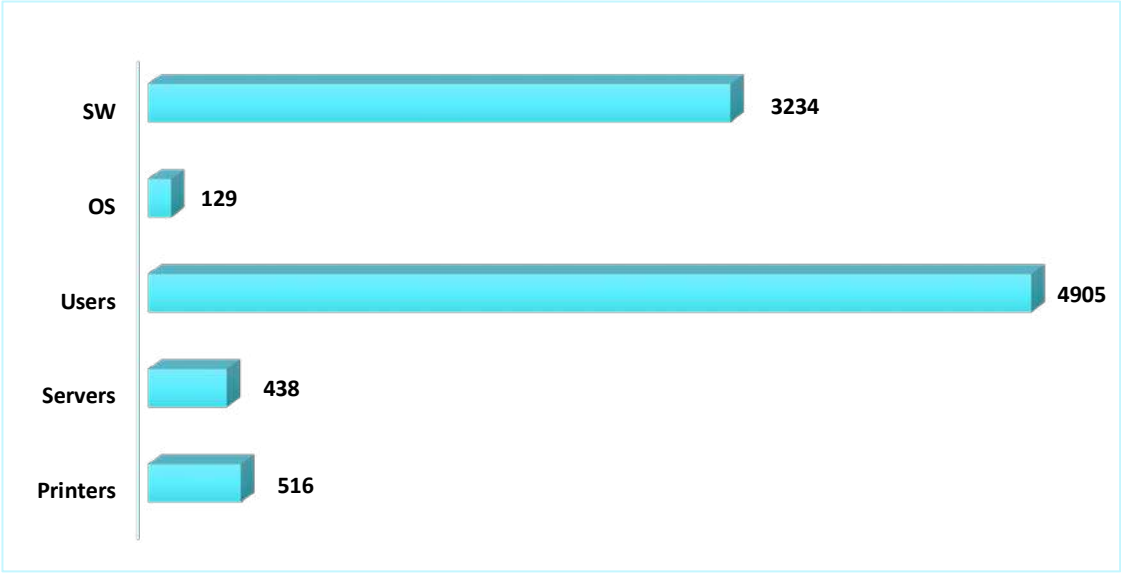

Figura 7. FOCA – Parámetros importantes extraídos y sus cantidades

Los programas más utilizados son los de **Adobe** (por ejemplo: Acrobat, Acrobat Distiller, InDesign o PDF Library) **y las diferentes versiones de Microsoft Office** (XP, 2000, 2007, etc.). Esto tiene sentido ya que los archivos que encontramos son principalmente PDFs (Adobe), documentos de procesamiento de texto (Word de Microsoft Office), archivos de hojas de cálculo (Excel de Microsoft Office) y archivos de presentación (PowerPoint de Microsoft Office).

4.2.2. Análisis del Sistema

Los metadatos ofrecen información muy valiosa que se utiliza en las investigaciones informáticas forenses para identificar el dispositivo en el que se elaboró el documento o para determinar un calendario.

Sin embargo, también permite al delincuente informático delinear las características del ordenador o empresa que desea atacar, reduciendo las opciones y mejorando la efectividad del ataque.

4.2.2.1. Sistemas Operativos

Se encontraron alrededor de **10 sistemas operativos diferentes** desplegados en **2759 ordenadores** - aproximadamente el 65% fueron identificados en Asia. La siguiente figura muestra el número de sistemas operativos detectados en cada uno de los dominios analizados por región.

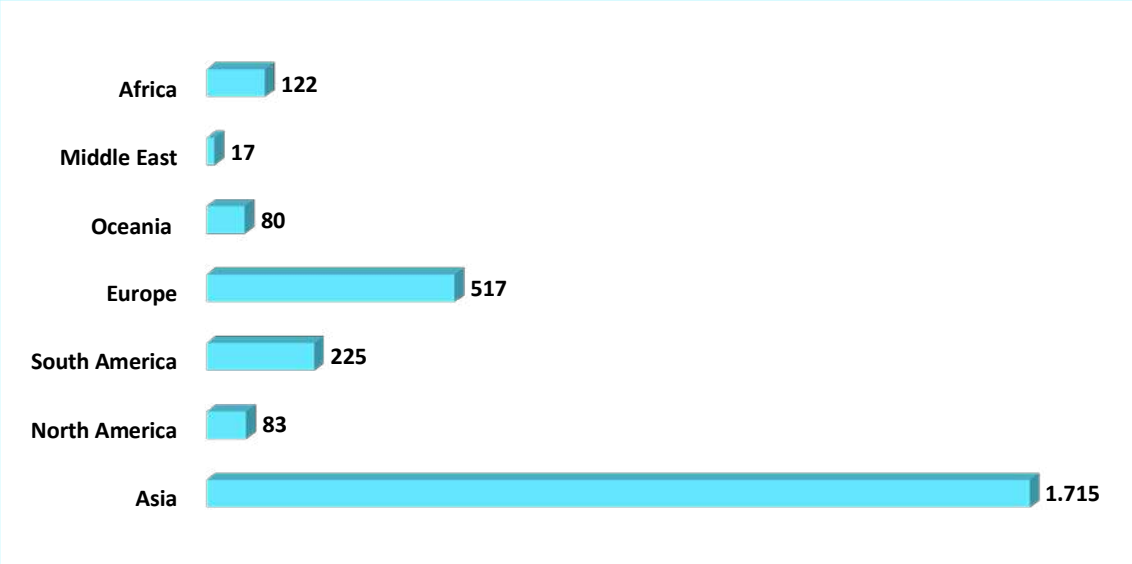

Figura 8. FOCA – Cifras de metadatos relacionados con Sistemas Operativos hallados por región

Desde hace algunos años, los sistemas operativos más utilizados ya no son soportados por sus fabricantes. Esto genera un riesgo crítico para la información que poseen, **suponiendo que el equipo con el que se hicieron esos documentos aún esté disponible**.

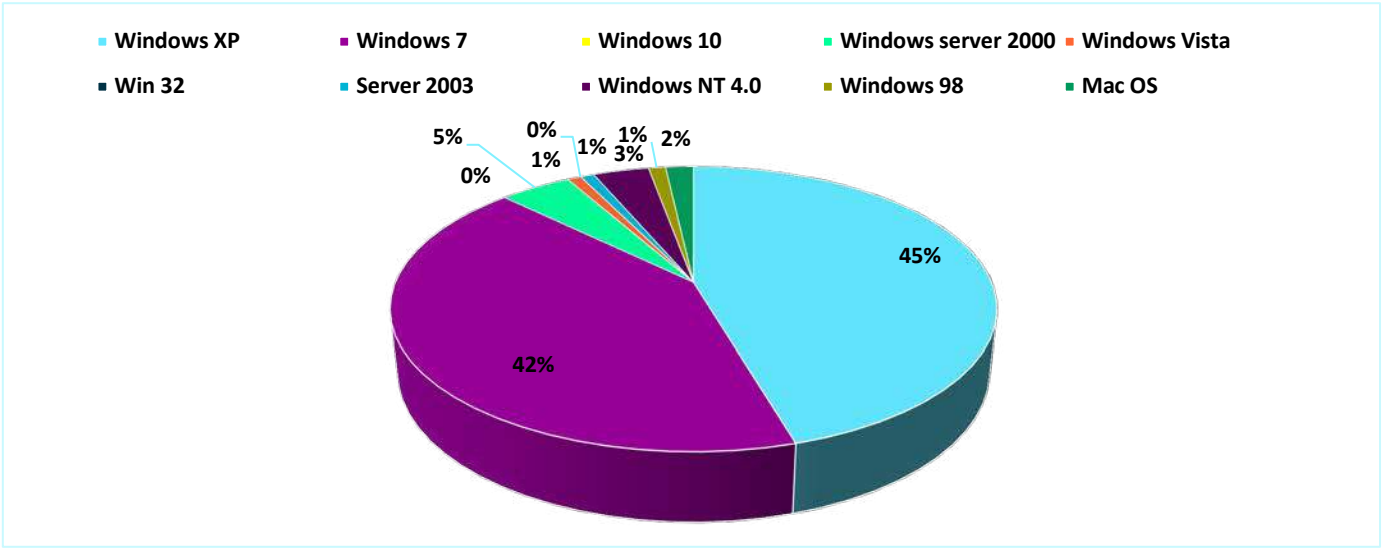

Figura 9. FOCA – Proporción global de sistemas operativos

El caso de Windows XP (que se encuentra en casi la mitad de todos los ordenadores) es especialmente relevante. No ha tenido ninguna actualización de seguridad ni soporte de Microsoft desde abril de 2014, por lo que un tercero malintencionado podría explotar esta información.

4.2.2.2 Usuarios

La identificación de usuarios a través de metadatos permite a un atacante obtener una lista de **usuarios válidos dentro de la infraestructura de la organización**. En el proceso de análisis se encontró un promedio de 700 usuarios por región con **4905 usuarios identificados** en los metadatos de los documentos analizados, los cuales fueron distribuidos por región como se muestra en la siguiente figura.

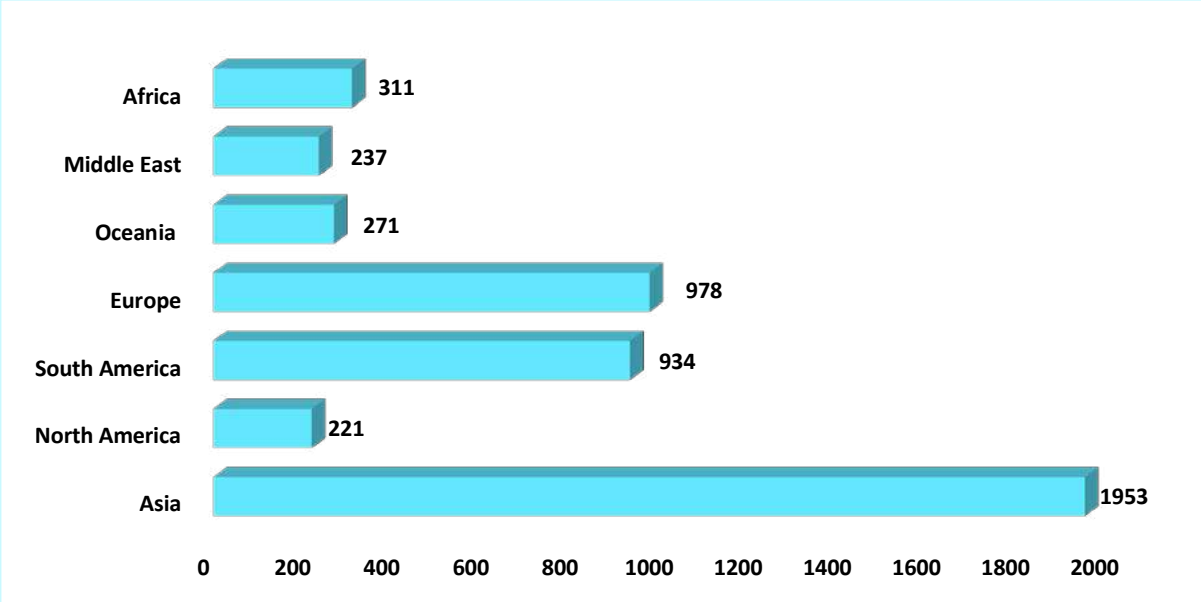

Figura 10. FOCA – Usuarios identificados por región

La región que nos proporcionó la mayor parte de la información de sus metadatos es Asia. En el extremo inferior, tenemos a Oriente Medio, Oceanía y Norteamérica.

El uso de cuentas de usuario genéricas es una mala práctica. Esto hace imposible rastrear los eventos dentro de los diferentes sistemas hasta un usuario específico, lo que aumenta el riesgo de pérdida de información confidencial por parte de un empleado desleal. Encontramos que **la mayoría de los bancos tenían al menos una cuenta genérica**.

También encontramos **289 cuentas de administrador**, que se supone que tienen privilegios más altos, lo que las convierte en un objetivo muy atractivo para los atacantes potenciales.

4.2.3 Información adicional interesante obtenida

- Encontramos una cuenta de usuario en Asia llamada "Any Authorized User" ("Cualquier usuario autorizado"). El uso de cuentas de usuario genéricas es una mala práctica como se explicó anteriormente.
- Dos bancos del mismo grupo comparten aplicaciones oficiales y redes internas - esta es una práctica peligrosa porque las vulnerabilidades encontradas en una de las aplicaciones también se aplican a la otra.

- Un banco en Asia utiliza el software Open Office - el software Open Office no es una buena idea, ya que no garantiza el soporte ni la seguridad.
- Las impresoras de algunos bancos proporcionan demasiada información (edificio, piso y dirección interna) - esta información puede ser útil para los atacantes potenciales cuando hacen ingeniería social, por ejemplo.
- Pudimos encontrar información relacionada con el departamento de Recursos Humanos de algunos bancos. Dicha información debería ser interna.
- Tener servidores asignados en muchos países diferentes (debido a servicios como Akamai) es una práctica frecuente, pero algunos países conocidos por sus medidas restrictivas tienen el 100% de sus servidores en el mismo país en el que se encuentra el banco.
- Fuimos capaces de identificar dónde estaban ubicados físicamente algunos servidores. Esta información no debe ser pública, ya que los actores maliciosos pueden utilizarla de muchas maneras diferentes.
- Un apunte "gracioso" es que un banco en África nombra a sus servidores en base a diferentes especies de animales (*Wale, Rhyno*, etc.). Este mismo banco identifica el PC utilizado por el Administrador como "PC_Administrator". Esta es una práctica muy insegura (a menos que se haya hecho a propósito como parte de un Honeypot).

4.2.4 Puntuaciones globales de FOCA

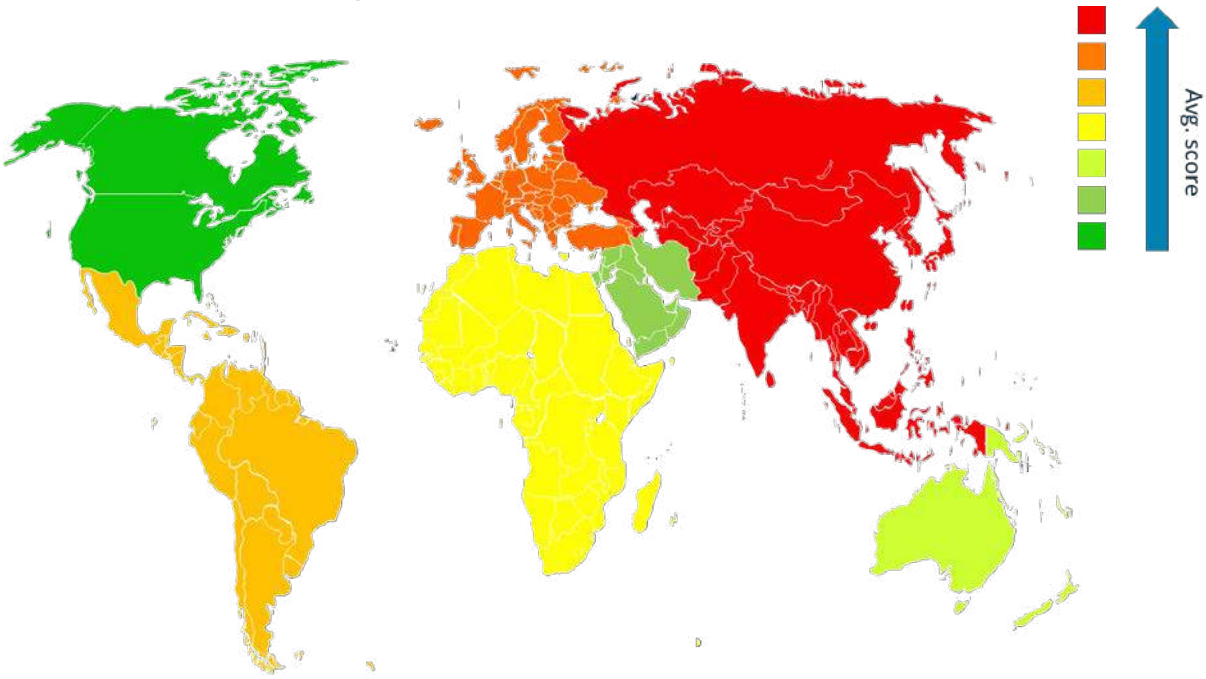

Imagen 8. FOCA – Puntuación global de riesgo por región basada en la información disponible.

Desarrollamos un nuevo sistema de puntuación basado en diferentes parámetros obtenidos a partir de los resultados de FOCA (donde una puntuación más alta significa que FOCA puede extraer menos información).

El gráfico anterior muestra que no existe una relación directa entre el puntaje FOCA y el puntaje del mASAPP. Por ejemplo, Europa es la región con la puntuación más baja del mASAPP, pero tiene la segunda puntuación más alta de FOCA.

4.3. Análisis de Hosts – Censys

A través de Censys.io[1] pudimos ver qué tipo de servicios y protocolos estaban vinculados a los hosts asociados a los dominios oficiales del banco.

Se llevó a cabo un proceso de análisis de los servicios detectados para determinar cuántos servicios realizan un aseguramiento del tráfico de información utilizando encriptación en la conexión. También se analizó la ubicación física del servidor basada en la dirección IP.

4.3.1 Servicios detectados

Como se puede ver en el gráfico siguiente, **todas las regiones tienen más del 94 % de sus dominios con una conexión HTTPS disponible**. Por otro lado, el promedio total de dominios **con conexión HTTP disponible es del 67 %**, lo que es relativamente importante ya que se trata de un protocolo inseguro.

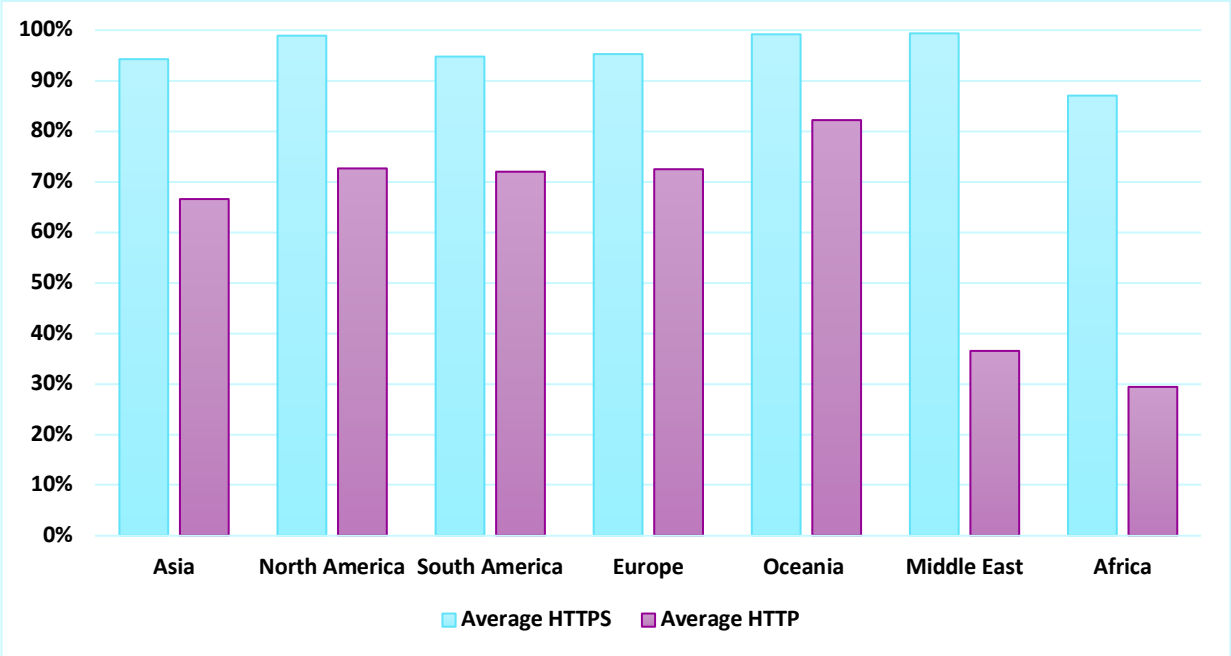

Figure 12. Censys – Promedios de conexiones HTTP y HTTPS por región

Censys detectó un pequeño porcentaje de conexiones **Telnet**. Telnet es un antiguo protocolo desarrollado en 1969 y fue sustituido por SSH (actualmente Telnet se considera inseguro). Sugerimos a todos los bancos con Telnet que hagan

[1] Es necesario mencionar que puede ejecutar la consulta en dos días diferentes y los resultados variarán un poco. Una persona malintencionada puede ejecutar Censys.io para averiguar qué nuevos servicios, como los FTP, están disponibles y comenzar a lanzar nuevos ataques sobre estos nuevos servicios detectados.

un examen exhaustivo de los protocolos en vigor, ya que esto podría ser una forma de que un atacante dañe la seguridad del banco.

4.3.2 Ubicación de los servicios

Para los bancos, es vital tener control sobre sus políticas de información. Por lo tanto, la ubicación de los servidores es de suma importancia, ya que es donde se localizan físicamente los datos. Es por ello que el análisis de la ubicación de los diferentes servidores detectados se incluyó en nuestro informe.

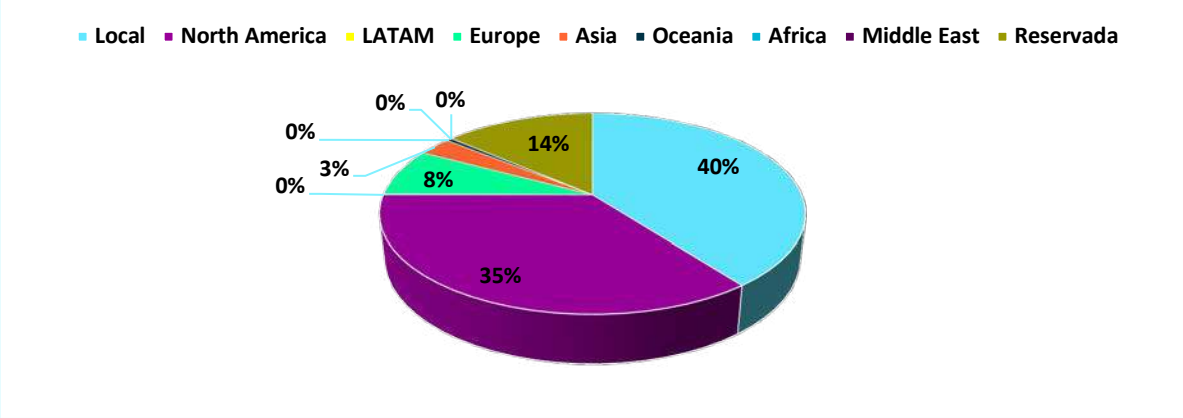

Figura 13. Censys – Ubicación de los servicios

Como se puede ver más arriba, la mayor parte del servicio prestado está alojado localmente (40%) o en América del Norte (35%).

Tener los servicios ubicados en el país de origen del banco es una buena práctica, ya que suele ser más fácil proteger y asegurar que el banco cumpla con las regulaciones del país en materia de protección de datos. África y Oriente Medio son las regiones donde la mayoría de los países mantienen sus servicios a nivel local.

También es importante destacar que la mayoría de los bancos utilizan **Akamai**[2], que se incluyó en nuestra búsqueda de Censys. La mayoría de los servicios de Akamai se ofrecen desde los Estados Unidos y es por eso que estamos viendo el mayor porcentaje en ese país, seguido por los Países Bajos en Europa. **Utilizar un servicio como Akamai es también una buena práctica de seguridad.**

[2] Akamai es una red de entrega de contenido (CDN) y proveedor de servicios en la nube. Otras empresas utilizan sus servicios para distribuir contenidos en servidores ubicados en todo el mundo. Esto significa que cuando usted descarga algo de una de esas compañías, el archivo será accedido desde un servidor físicamente cercano a usted, resultando en una velocidad de descarga más rápida.

5. Conclusiones

5.1. Aplicaciones Móviles

- Encontramos que todos los bancos, independientemente de su ubicación e ingresos, tenían vulnerabilidades en sus aplicaciones oficiales. Teniendo en cuenta la cantidad de datos confidenciales de los clientes con los que tratan, se trata de un problema grave.

- El análisis mostró que la puntuación global de riesgo era de **7,27 (alta),** siendo los bancos de Asia, África y América del Sur los que obtuvieron la puntuación más alta.
- Encontramos varias vulnerabilidades en las aplicaciones móviles analizadas, causadas principalmente por fallas en la calidad del código. La vulnerabilidad más común era la **Potencial Inyección SQL**.

- Comparamos qué permisos pedía cada aplicación bancaria. A pesar de estar en la misma industria y proporcionar el mismo servicio, sólo había un permiso común para todas las aplicaciones: **acceso a Internet**.

- Algunos bancos africanos nunca han tenido ninguna aplicación móvil (al menos no pudimos encontrarlos), hecho que se alinea con las noticias de Internet sobre cómo algunos países no han desarrollado su mercado de aplicaciones móviles.

- El número medio de permisos solicitados por una aplicación bancaria fue de **19**. Oriente Medio fue la región con el menor promedio de permisos solicitados, mientras que Asia fue la región con el mayor número de permisos solicitados.

- Permisos intrusivos como *CALL_PHONE*, *READ_CONTACTS*, *READ_SMS*, *WRITE_SMS*, *READ_CALENDAR* y *WRITE_SETTINGS* estaban presentes en varias aplicaciones.

5.2. Metadatos en ficheros públicos

- Se detectaron **289 cuentas de administrador** y varias cuentas genéricas con características de administradores.

- La infraestructura tecnológica de la mayoría de los bancos puede seguir utilizando sistemas operativos que actualmente no son soportados por sus fabricantes. No podemos confirmarlo porque los archivos pueden haber sido publicados hace muchos años**, mientras que la tecnología podría haber sido actualizada**.

- Se encontraron **más de 3.000 metadatos relacionados con el software**, la mayoría de ellos versiones antiguas que ya no son compatibles con sus desarrolladores. Un atacante podría intentar utilizar exploits para que este software acceda a la red de la organización.

- El análisis de los archivos públicos también nos ha dado información relacionada con **ubicaciones físicas y los nombres de varios servidores e impresoras**. Esta información no debe ser pública debido a las posibles implicaciones que puede causar si un actor malicioso quiere causar daño.

- Para la elaboración de este informe se analizaron otros aspectos además de los mencionados en la introducción:

    - Sistemas operativos y sus usuarios.
    - Ubicación de direcciones IP.
    - Cuentas de correo electrónico asociadas a los metadatos de los documentos públicos descargados.

Es posible mejorar la seguridad de estos bancos evitando la exposición de datos mediante la implementación de procedimientos y controles manuales o automatizados, sobre la infraestructura tecnológica y sobre sus usuarios.

5.3. Hosts

- **Más del 96 %** de los hosts identificados utilizaron **HTTPS**.

- Todavía hay una gran cantidad de servicios **HTTP**, que **se considera un protocolo no seguro**.

- Alrededor del **50 %** de los bancos consideraron que **utilizan Akamai**. Esto implica que el tráfico pasa principalmente por servidores norteamericanos.

- **Los bancos que no utilizan Akamai tienden a alojar sus servicios localmente**. La única excepción es Asia, donde los bancos que no trabajan con Akamai también tienen sus servidores en EE.UU.

- **Ninguno de los bancos analizados de África utiliza Akamai**. Esta es una de las regiones con más anfitriones locales.

- Uno de los hosts relacionados con un banco de África tiene la vulnerabilidad **Heartbleed**. Heartbleed es un error de seguridad en la biblioteca de criptografía OpenSSL, una implementación del protocolo TLS (*Transport Layer Security*).

- El servicio más popular cuando no hay ningún Akamai involucrado es **FTP**, seguido por **SMTP** y diferentes tipos de bases de datos.

- La mayoría de los servicios están alojados en **Norteamérica**. **Europa** parece ser la segunda mejor opción, pero con una gran diferencia con respecto a NA.

- **África** es la región en la que la mayoría de sus servicios están alojados localmente **(92%)**, seguida por **Oriente Medio (70 %).**

Acerca de la Telco Security Alliance

La alianza, compuesta por Telefónica, Etisalat, Softbank y Singtel, es uno de los mayores proveedores de seguridad cibernética del mundo, con más de 1.200 millones de clientes en más de 60 países de Asia Pacífico, Europa, Oriente Medio y América. A través de sus recursos y capacidades combinadas, el grupo puede proteger a las empresas contra los crecientes riesgos de ciberseguridad a medida que el entorno de seguridad de la información se vuelve cada vez más complejo.

A través de la alianza, los miembros pueden lograr sinergias operativas y economías de escala que, con el tiempo, ayudarán a reducir los costos para sus clientes. Los miembros del grupo operan 22 Centros de Operaciones de Seguridad (SOCs) de clase mundial y emplean a más de 6.000 expertos en seguridad cibernética. Para ampliar su presencia global, la alianza está abierta a la incorporación de nuevos miembros con el tiempo.

Bajo el acuerdo, el grupo compartirá la inteligencia de la red sobre las amenazas cibernéticas y aprovechará su alcance global conjunto, sus activos y sus capacidades de seguridad cibernética para servir a los clientes de todo el mundo. Aprovechando la huella geográfica y la experiencia de cada miembro, la alianza es capaz de apoyar a los clientes de los demás en cualquier lugar y en cualquier momento, permitiéndoles responder rápidamente a cualquier amenaza de seguridad cibernética.

Para mejorar su cartera de seguridad cibernética, los miembros también estudiarán la posibilidad de desarrollar nuevas tecnologías, como el análisis predictivo mediante el aprendizaje automático y la seguridad cibernética avanzada para la Internet de los objetos. La alianza también considerará el desarrollo de una hoja de ruta conjunta para la evolución de sus carteras de seguridad y explorará inversiones conjuntas en productos y servicios de seguridad, SOCs, plataformas, start-ups e I+D.