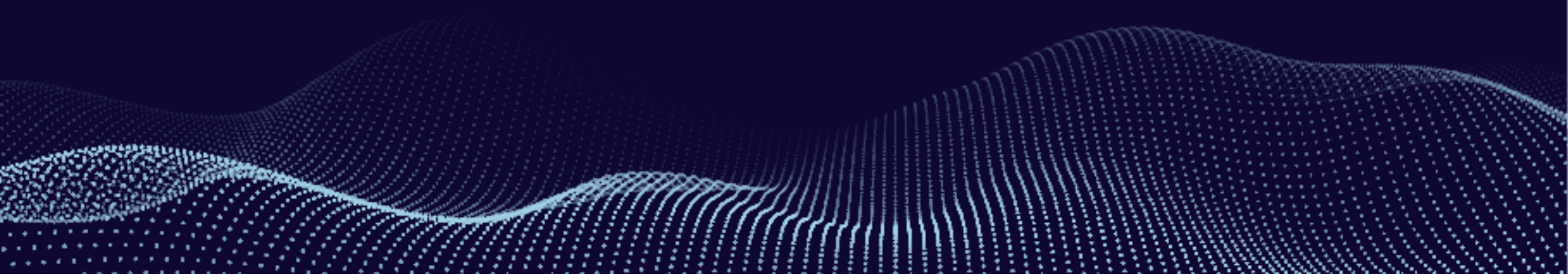


# Seguridad en plataformas móviles



# ¿Quién Soy?

## Mauricio Trujillo Londoño

Cybersecurity Consultant @ Tarlogic Security

Coorganizador @ Bitup Alicante 

Máster Oficial Ciberseguridad por la OUC

Grado Ingeniería Informática por la UA

Certificaciones/Certificados:

WAPT-X, CEH, CSX, CCNA R&S, CCNA Security,  
CPHE...



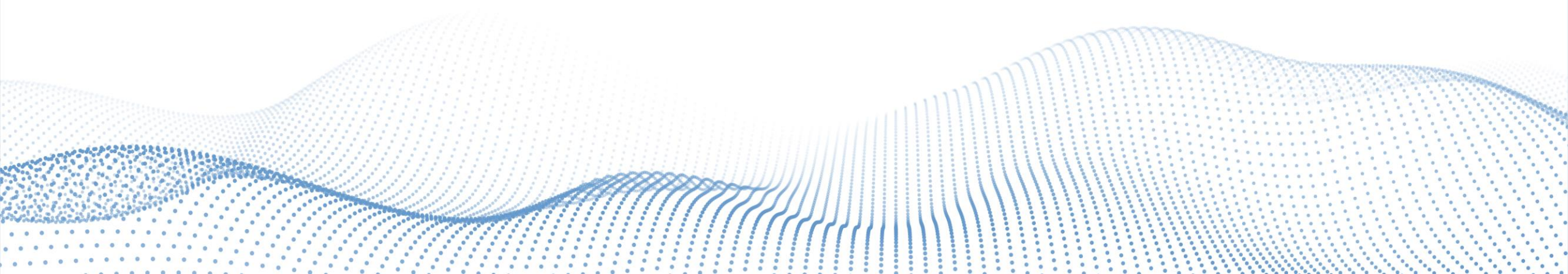
<https://es.linkedin.com/in/mauricio-trujillo-londono>



fm\_trujillo

# Motivación

- ❖ Devolver a la comunidad lo aprendido
- ❖ Muy pocas charlas/talleres enfocadas a auditorias
- ❖ #SharingIsCaring





# Consejos

- ❖ Tener actualizado el sistema operativo
- ❖ Tener actualizadas las apps a la última versión
- ❖ Tener un antivirus ¿de pago?
- ❖ Instalar alguna app de seguridad (Conan mobile)
  - ❖ <https://www.osi.es/es/conan-mobile>
  - ❖ <https://www.osi.es/sites/default/files/docs/manual-usuario-conan-mobile.pdf>
  - ❖ <https://www.osi.es/sites/default/files/docs/guia-seguridad-ios.pdf>
  - ❖ <https://www.osi.es/sites/default/files/docs/guia-seguridad-android.pdf>
- ❖ Descargar las apps de sitios confiables
- ❖ Usar/activar MFA/2FA siempre que lo admita
- ❖ Desinstalar apps sin uso
- ❖ Uso de MDM en entornos corporativos

# Otros Riesgos

## ❖ Smishing



<https://www.osi.es/es/campanas/ingenieria-social/prueba-deteccion-ingenieria-social>

## Verificar URLs:

- <https://urlscan.io/>
- <https://www.virustotal.com/gui/home/url>
- Aplicaciones Android/iOS

## ❖ QRishing



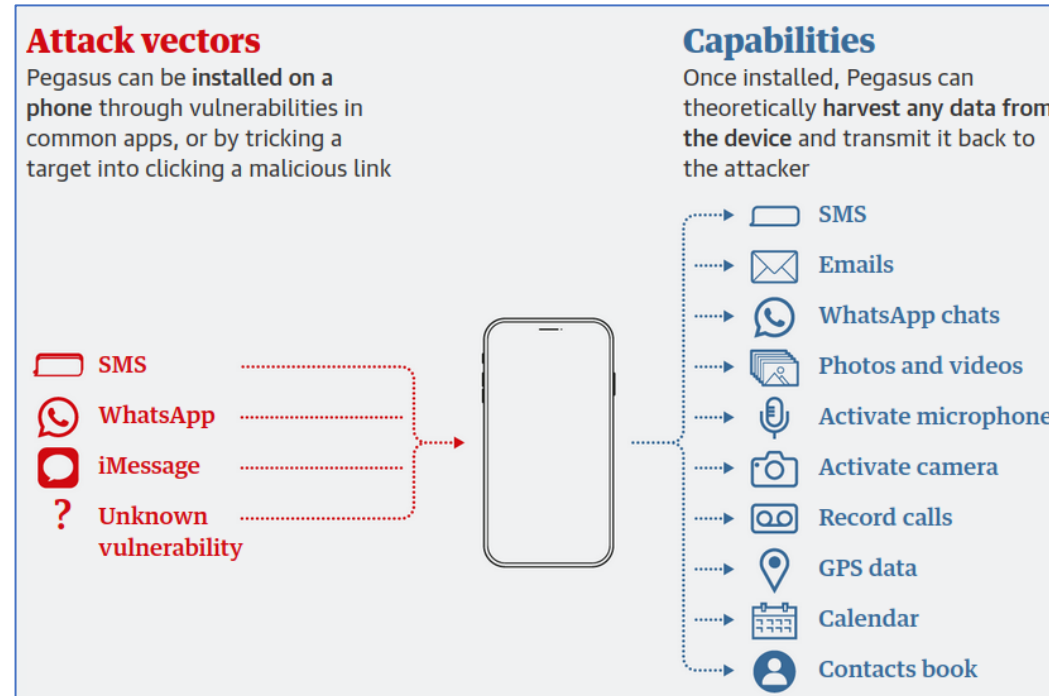
<https://www.tekcrispy.com/2021/09/19/qrishing-estafa-codigos-qr/>



# Intentaremos evitar malware



<https://www.kaspersky.es/blog/pegasus-spyware/10374/>



<https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware>

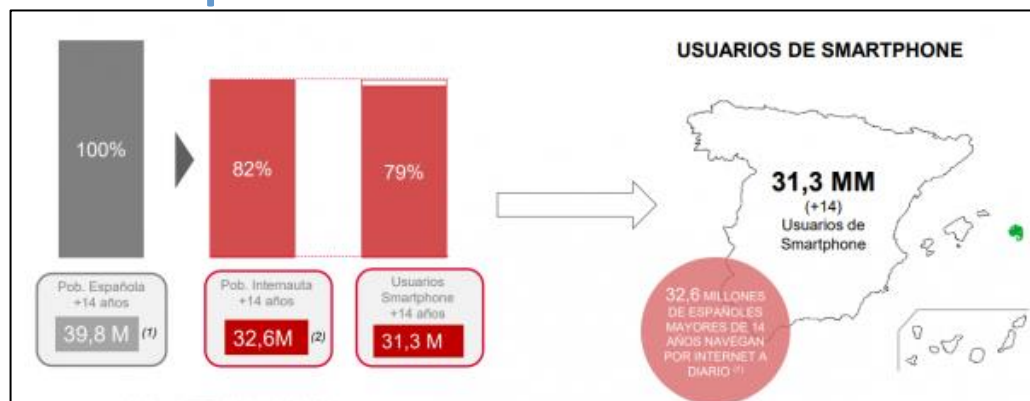
# ¿Qué no veremos?

- ❖ Pentesting desde Android
- ❖ Hackear un dispositivo Android
- ❖ Vulnerabilidades en el sistema operativo Android



# Estado del arte

## ❖ España 2019



							
1	 Comunicación	100,0%	100,0%	10	 Búsqueda Web	98,9%	99,3%
2	 Compras / Subastas / Alquiler	100,0%	100,0%	11	 Gaming	97,7%	99,0%
3	 Video Online	100%	100%	12	 Administración del dinero	94,3%	95,0%
4	 On-Site Search	99,8%	99,9%	13	 Personalización	85,7%	86,3%
5	 Productividad	99,6%	99,9%	14	 Comparador de precio / producto	83,6%	85,0%
6	 Noticias / Información	99,5%	99,8%	15	 Gambling	17,9%	19,0%
7	 Redes sociales	99,4%	99,8%	16	 Otra actividad	99,4%	99,7%
8	 Descargas	99,2%	99,7%				
9	 Utilidades	99,2%	99,6%				

**Evolución de las descargas de aplicaciones a nivel mundial**  
Descargas anuales en miles de millones

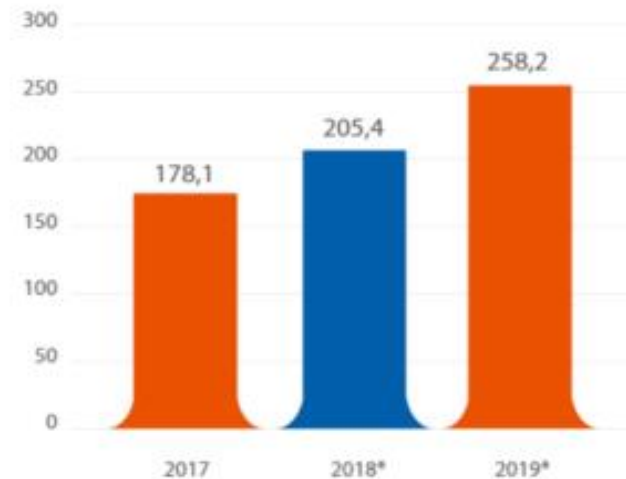


Gráfico elaborado por Ditrendia a partir de datos de Statista

**ditrendia**  
digital marketing trends



# ¿Qué es Android?

- ❖ Sistema operativo
- ❖ Plataforma abierta
- ❖ Adaptable a diversos tipos de hardware
- ❖ Portabilidad asegurada
- ❖ Filosofía de dispositivo siempre conectado a Internet
- ❖ Arquitectura basada en componentes inspirados en Internet
- ❖ Gran cantidad de servicios incorporados
- ❖ Aceptable nivel de seguridad
- ❖ Optimizado para baja potencia y poca memoria
- ❖ Alta calidad de gráficos y sonido

# ¿Qué es Android?

- ❖ Google adquiere Android Inc. en 2005
- ❖ Se crea en 2007 el consorcio Open Handset Alliance con el objetivo de desarrollar estándares abiertos para móviles. Está formado por Google, Intel, Texas Instruments, Motorola, T-Mobile, Samsung, Ericsson, Toshiba, Vodafone, NTT DoCoMo, Sprint Nextel y otros.
- ❖ El objetivo fundamental de la alianza es promover el diseño y la difusión de la plataforma Android.
- ❖ Código abierto bajo licencia Apache v2.0

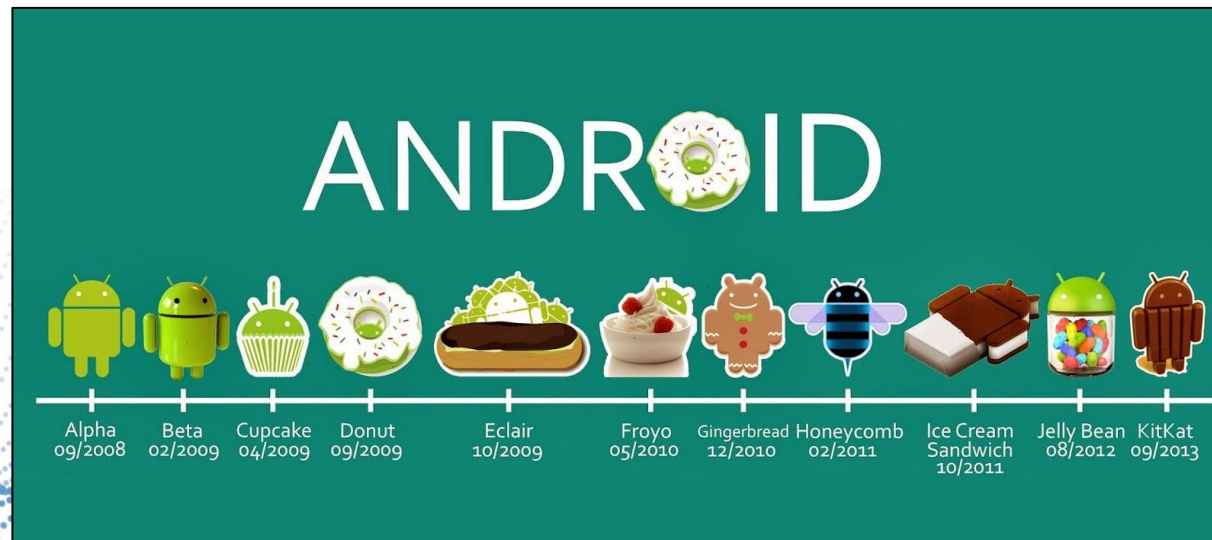
# Versiones de Android

- ❖ Android 1.0 (API 1) Sept 2008
- ❖ Android 1.1 (API 2) Feb 2009
- ❖ Cupcake: Android 1.5 (API 3) Abril 2009
- ❖ Donut: Android 1.6 (API 4) Sept 2009
- ❖ Éclair: Android 2.0 (API 5) Oct 2009 y 2.1 (API 7) Enero 2010
- ❖ Froyo: Android 2.2 (API 8) Mayo 2010
- ❖ Gingerbread: Android 2.3 (API 9) Dic 2010
- ❖ Honeycomb: Android 3.0 (API 11) Feb 2011, 3.1 (API 12) Mayo 2011 y 3.2 (API 13) Julio 2011
- ❖ Ice Cream Sandwich: Android 4.0 (API 14) Sept 2011 y 4.0.3 (API 15) Dic 2011
- ❖ Jelly Bean: Android 4.1 (API 16) Julio 2012, 4.2 (API 17) Nov 2012 y 4.3 (API 18) Julio 2013
- ❖ KitKat: Android 4.4 (API 19) Oct 2013
- ❖ Lollipop: Android 5.0 (API 21) Nov 2014 y 5.1 (API 22) Marzo 2015

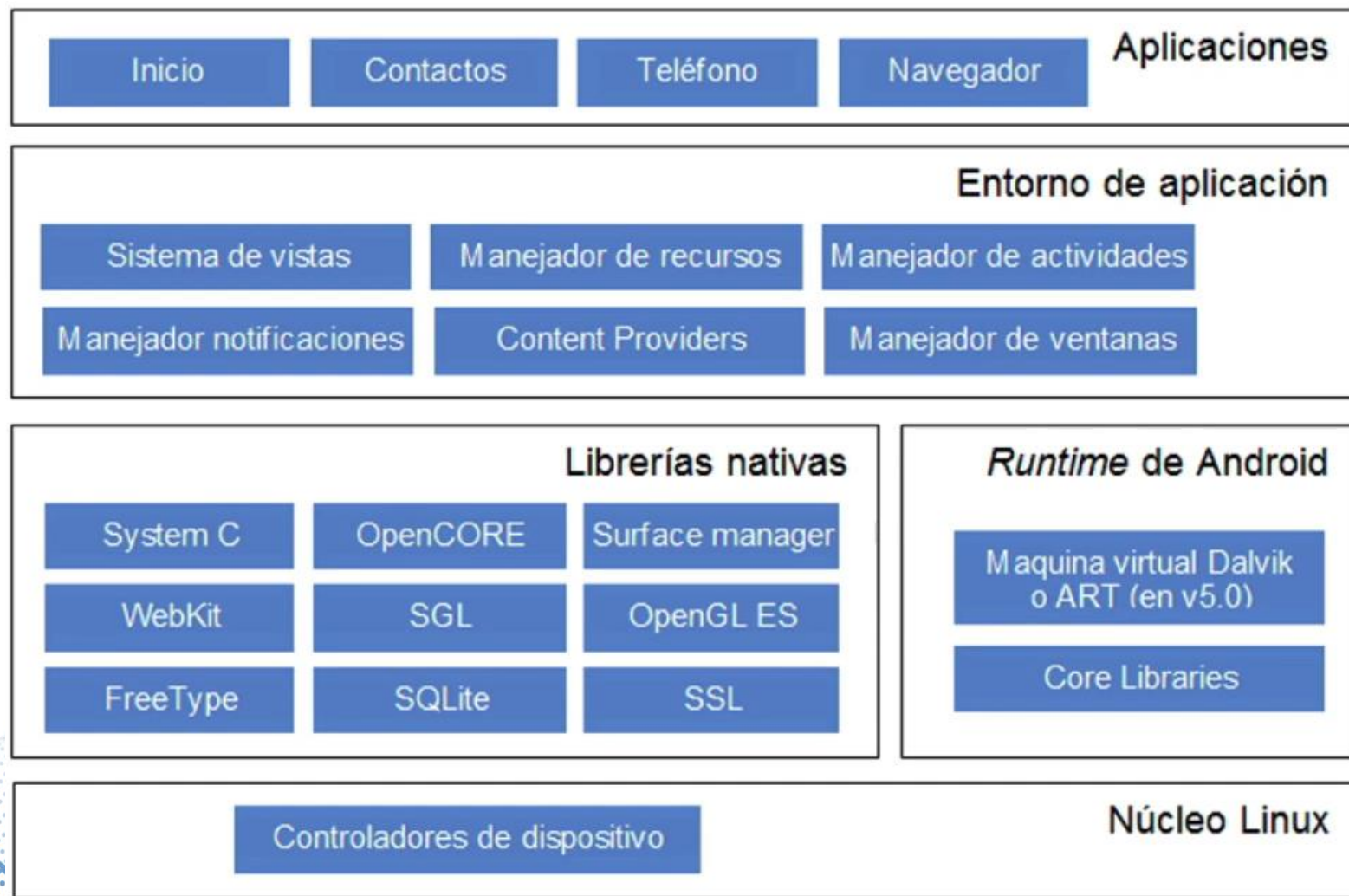


# Versiones de Android

- ❖ Marshmallow: Android 6.0 (API 23) Oct 2015
- ❖ Nougat: Android 7.0 (API 24) Julio 2016 y 7.1 (API 25) Dic 2016
- ❖ Oreo: Android 8.0 (API 26) Agosto 2017 y 8.1 (API 27)
- ❖ Pie: Android 9.0 (API 28) Agosto 2018
- ❖ Android 10.0 (API 29) Sept 2019
- ❖ Android 11.0 (API 30) Sept 2020
- ❖ Android 12.0 (API 31) Sept 2021
- ❖ Android 13.0 (en desarrollo)



# Arquitectura de Android



El gran libro de Android

# Tipos de apps Android

- ❖ Nativas

  - ❖ Java

  - ❖ Kotlin

- ❖ Híbridas

  - ❖ Xamarin (C# / .Net)

  - ❖ Flutter (Dart compilado)

  - ❖ React Native (JS / React)

  - ❖ NativeScript (JS / Angular)

  - ❖ Apache Cordova, PhoneGap, Ionic (HTML, CSS, JS)

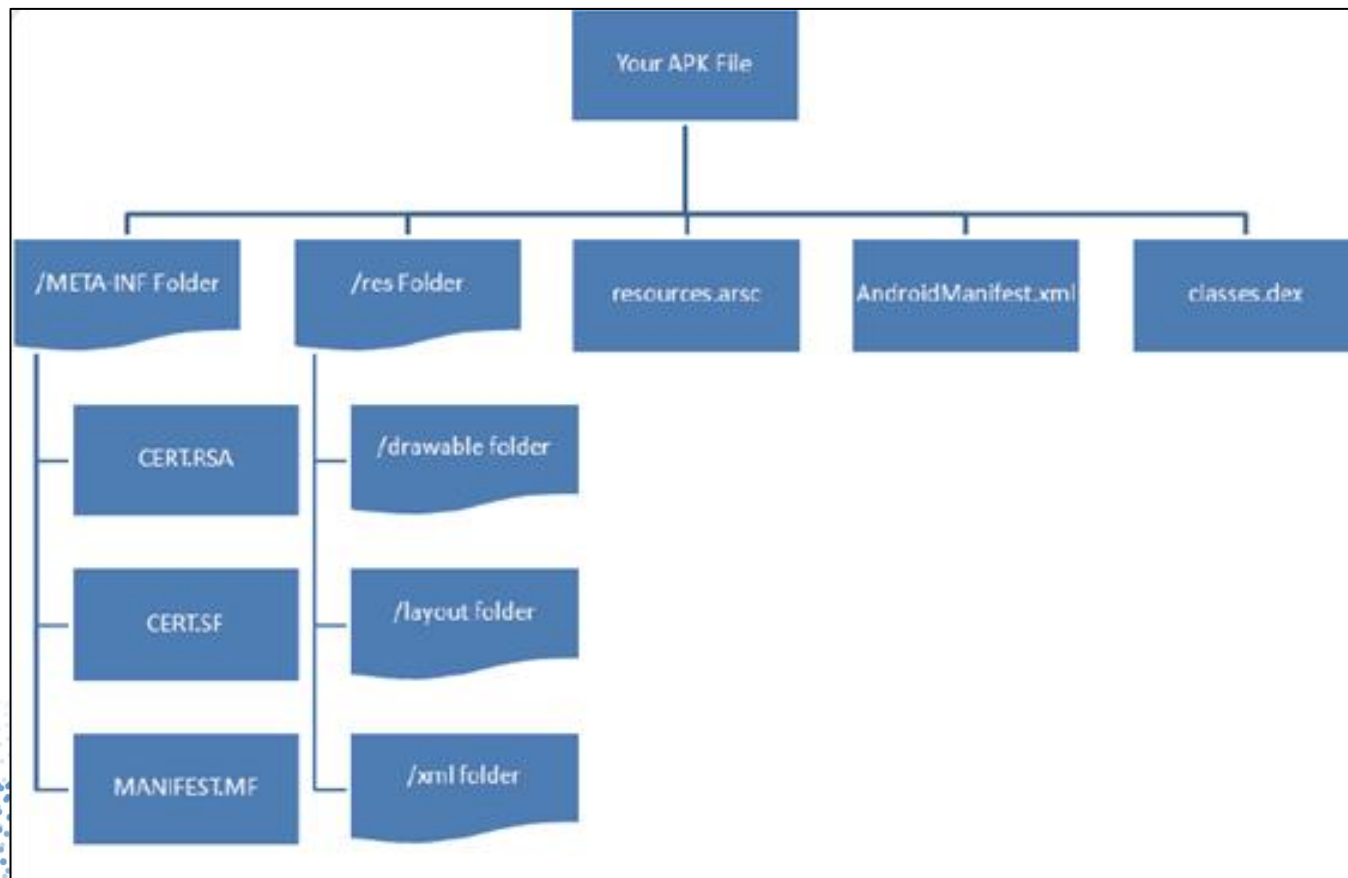
- ❖ Web

  - ❖ Navegador embebido



# Estructura de una app Android

## ❖ Fichero APK



## ❖ Una vez instalada:


databases/: base de datos de la aplicación  
lib/: librerías nativas de la app  
files/: otros ficheros  
shared\_prefs/: ficheros de preferencias  
cache/: ficheros caché

# Seguridad en Android

## ❖ Objetivo

- ❖ Protegernos de aplicaciones mal intencionadas que intenten violar la privacidad del usuario y evitar que realicen acciones no deseadas.

## ❖ Fundamentos:

- ❖ Ejecución en procesos independientes de Linux
  - ❖ Firma digital de los APKs
  - ❖ Esquema de permisos en Android
  - ❖ Cambios en la privacidad (Android 9 y 10)
- 

# Seguridad en Android

- ❖ Ejecución en procesos independientes de Linux
  - ❖ Concepto de sandbox
  - ❖ Android crea una cuenta de usuario Linux (user ID) nueva por cada paquete (APK) instalado en el sistema. Se elimina al desinstalar la app.
  - ❖ Cualquier dato almacenado por la app será asignado a su usuario Linux, por lo que normalmente no tendrán acceso a otras aplicaciones.



# Seguridad en Android

## ❖ Firma digital

- ❖ Cuando publicamos una aplicación, esta ha de ser firmada digitalmente. Sistema criptográfico que garantiza la autenticación, integridad y no-repudio.
- ❖ Verificar que el certificado es el original y el APK no ha sido modificado.
- ❖ En Google Play solo se pueden subir actualizaciones de la app con el mismo certificado.

# Seguridad en Android

## ❖ Esquema de permisos

- ❖ Proteger algunos recursos y características especiales.
- ❖ Para usar estos permisos cada aplicación debe declarar su intención de usarlo.
- ❖ Un usuario puede revisar los permisos cuando instala la aplicación.
- ❖ A partir de Android 6 se clasifican como Peligrosos y Normales, los cuales podrá conceder o retirar.

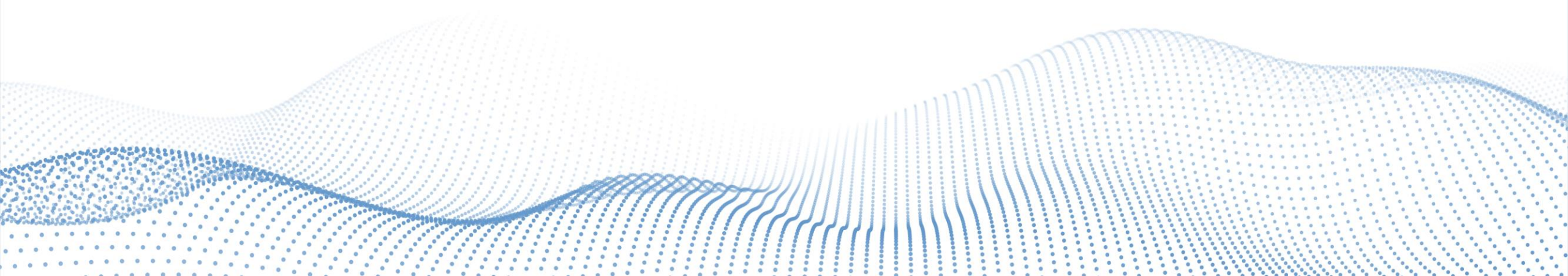
# Seguridad en Android

- ❖ Cambios en la privacidad (Android 9)
  - ❖ Nuevo grupo de permisos: CALL\_LOG (Antes en grupo Teléfono)
  - ❖ READ\_CALL\_LOG, WRITE\_CALL\_LOG y PROCESS\_OUTGOING\_CALLS
  - ❖ Solo las apps por defecto tendrán acceso a SMS y llamadas. Se eliminan los permisos de las apps de Google Play que no los usan como base para su funcionamiento.



# Seguridad en Android

- ❖ Cambios en la privacidad (Android 10)
  - ❖ Scoped Storage: Solo pueden ver el contenido de las carpetas creadas por ellas. Ya no será necesario solicitar permisos para acceder a almacenamiento externo para acceder a ficheros creados por la app.
  - ❖ Solicitud de permisos de acceso unitario y si lleva mucho tiempo sin usarlo, se vuelve a solicitar.



# Mecanismos de comunicación

## ❖ Activities

- ❖ Pantallas de la aplicación
- ❖ Creación de interfaz del usuario
- ❖ Desciende de Activity

## ❖ Broadcast Receivers

- ❖ Recibe anuncios broadcast y reacciona ante ellos
- ❖ Originados por el sistema o por las aplicaciones
- ❖ Pueden iniciar una actividad

## ❖ Services

- ❖ Se ejecuta en background sin interacción del usuario
- ❖ Dos tipos: locales y remotos

## ❖ Content Provider

- ❖ Compartir información entre varias aplicaciones

# ¿Son inseguros los mecanismos de comunicación?

```
android:exported=["true" | "false"]
```

```
<!-- This activity also handles "SEND" and "SEND_MULTIPLE" with media data -->
<intent-filter>
  <action android:name="android.intent.action.SEND"/>
  <action android:name="android.intent.action.SEND_MULTIPLE"/>
  <category android:name="android.intent.category.DEFAULT"/>
  <data android:mimeType="application/vnd.google.panorama360+jpg"/>
  <data android:mimeType="image/*"/>
  <data android:mimeType="video/*"/>
</intent-filter>
```



# Tipos de auditorias

- ❖ Caja blanca
  - ❖ Nos facilitan toda la información necesaria para la realización de las pruebas
- ❖ Caja gris
  - ❖ Nos facilitan parcialmente la información necesaria para la realización de las pruebas
- ❖ Caja negra
  - ❖ No nos facilitan ningún tipo de información para la realización de las pruebas

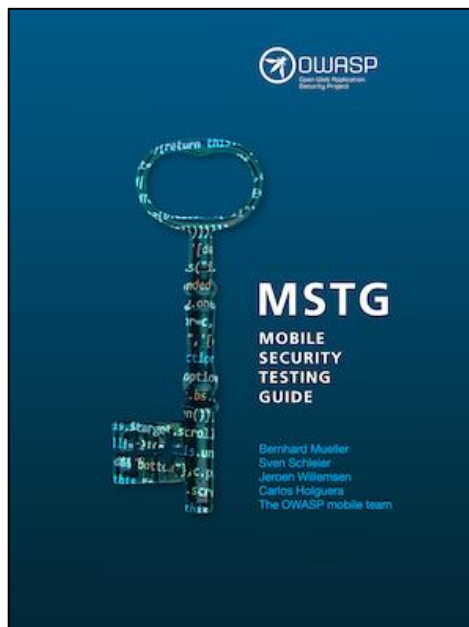
# OWASP MASVS & MSTG

Mobile Application Security  
Verification Standard (MASVS)



<https://github.com/OWASP/owasp-masvs>

Mobile Security  
Testing Guide (MSTG)



<https://github.com/OWASP/owasp-mstg>

Checklist

Nivel 1	Nivel 2
✓	✓
✓	✓
✓	✓
✓	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓

<https://github.com/OWASP/owasp-mstg/tree/master/Checklists>



# Developers



<https://twitter.com/SecuRingPL/status/1196729960444170240/photo/1>



# Almacenamiento Inseguro de Información

- ❖ Almacenamiento Inseguro de Información

- ❖ MSTG: MSTG-STORAGE-13/14/15
- ❖ MASV: Level 2 - Defense in Depth

- ❖ Abrir aplicación y usarla.

- ❖ Buscar información sensible:

- |                      |                  |
|----------------------|------------------|
| ❖ Shared Preferences | ❖ SQLite         |
| ❖ Internal storage   | ❖ SQLite cifrada |
| ❖ External storage   | ❖ Memoria RAM    |

## Mitigación:

# Almacenamiento Inseguro de Información

- ❖ Cifrar los datos en el dispositivo
- ❖ Usar Keystore
- ❖ Eliminar el contenido una vez usado
- ❖ Si es una contraseña usar la clase StringBuilder/Arrays
- ❖ Cifrar las bases de datos con información sensible
  - ❖ Librería SQLCipher
- ❖ Eliminar datos sensibles de las bases de datos
- ❖ Vacuum de la base de datos para eliminar tuplas huérfanas

# Información sensible en el Log

- ❖ Información sensible en el Log
  - ❖ MSTG: MSTG-STORAGE-3
  - ❖ MASV: Level 1 – Standard Security
- ❖ Abrir aplicación y usarla
- ❖ Obtener el PID del proceso
- ❖ Ejecutar logcat
- ❖ Buscar información sensible

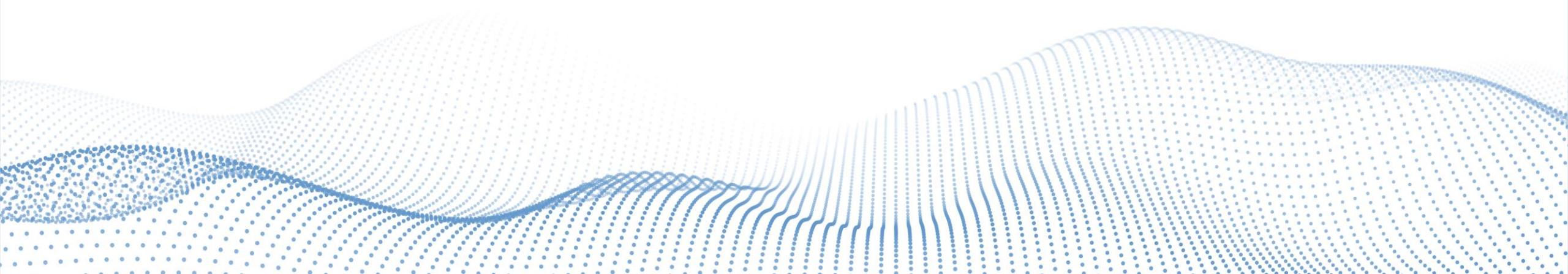


# Mitigación info sensible en el Log

- ❖ Eliminar el uso de la clase Log.\* del código
- ❖ Revisar permiso READ\_LOG en el Manifest para versiones antiguas de Android.

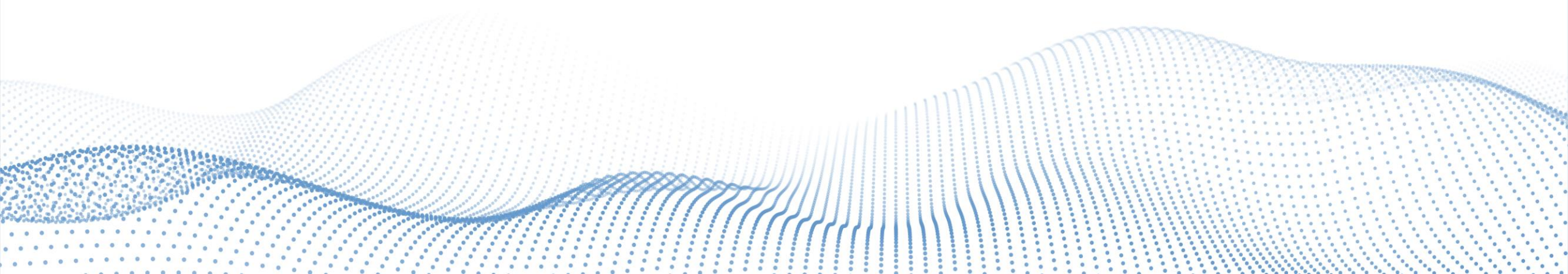
# Info sensible en caché del teclado

- ❖ Info sensible en caché del teclado
- ❖ Abrir aplicación y usarla
- ❖ Verificar si guarda info sensible en la caché del teclado



# Mitigar Info sensible en caché del teclado

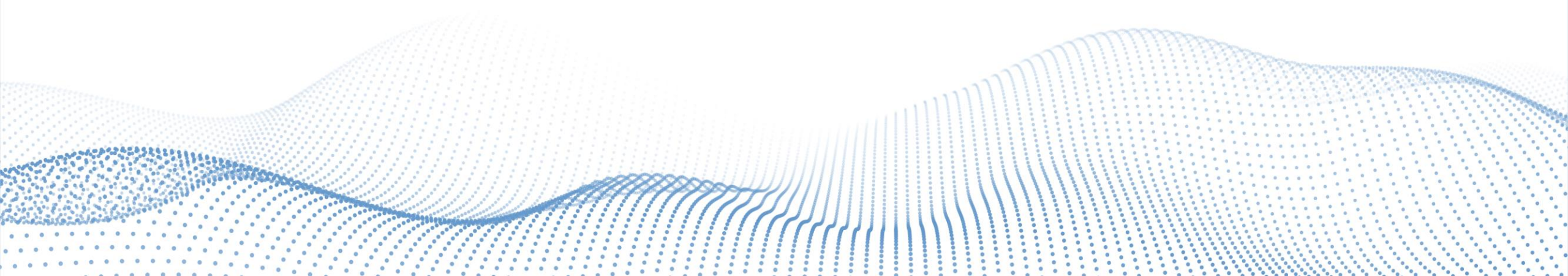
- ❖ Deshabilitar la caché del teclado en las partes más sensibles de la aplicación:
  - ❖ `android:inputType="textNoSuggestions"`





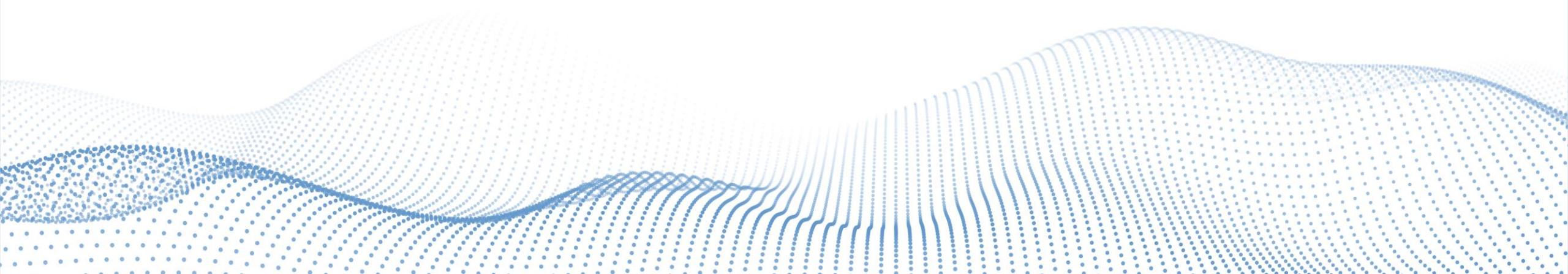
# Info sensible en portapapeles

- ❖ Info sensible en portapapeles
  - ❖ Abrir aplicación y usarla
  - ❖ Escribir en un formulario sensible
  - ❖ Intentar seleccionar y copiar/pegar los datos



# Mitigar Info sensible en portapapeles

- ❖ Deshabilitar el portapeles en las partes más sensibles de la aplicación



# Caso Real

- ❖ Aplicación: Adobe Reader
- ❖ Versión: 10.3.1 (10 Sept 2012)
- ❖ Vulnerabilidad: Path traversal en content provider
- ❖ Fuente: <https://web.archive.org/web/20151222213312/http://blog.seguese.com/2012/09/path-traversal-vulnerability-on-adobe-reader-android-application/>
- ❖ PoC:
  - ❖ `run app.package.attacksurface com.adobe.reader`
  - ❖ `run scanner.provider.traversal -a com.adobe.reader`
  - ❖ `run app.provider.read content://com.adobe.reader.fileprovider/../../../../proc/cpuinfo`
  - ❖ `run app.provider.read content://com.adobe.reader.fileprovider/../../../../etc/hosts`



# Recursos

- ❖ Leer, entender, practicar
  - ❖ <https://developer.android.com/?hl=es>
  - ❖ <https://github.com/B3nac/MobileApp-Pentest-Cheatsheet>
  - ❖ <https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/mobile.md>
  - ❖ <https://github.com/B3nac/Android-Reports-and-Resources>

# Q&A

## Contacto

---

**Mauricio Trujillo Londoño**

Consultor de Ciberseguridad

[mauricio.trujillo@tarlogic.com](mailto:mauricio.trujillo@tarlogic.com)

