

CIBERSEGURIDAD EN ENTORNOS DE DESARROLLO MOBILE



SEGURIDAD DE LA INFORMACIÓN

INTEGRIDAD

CONFIDENCIALIDAD

DISPONIBILIDAD

NO REPUDIO



CIBERSERGURIDAD

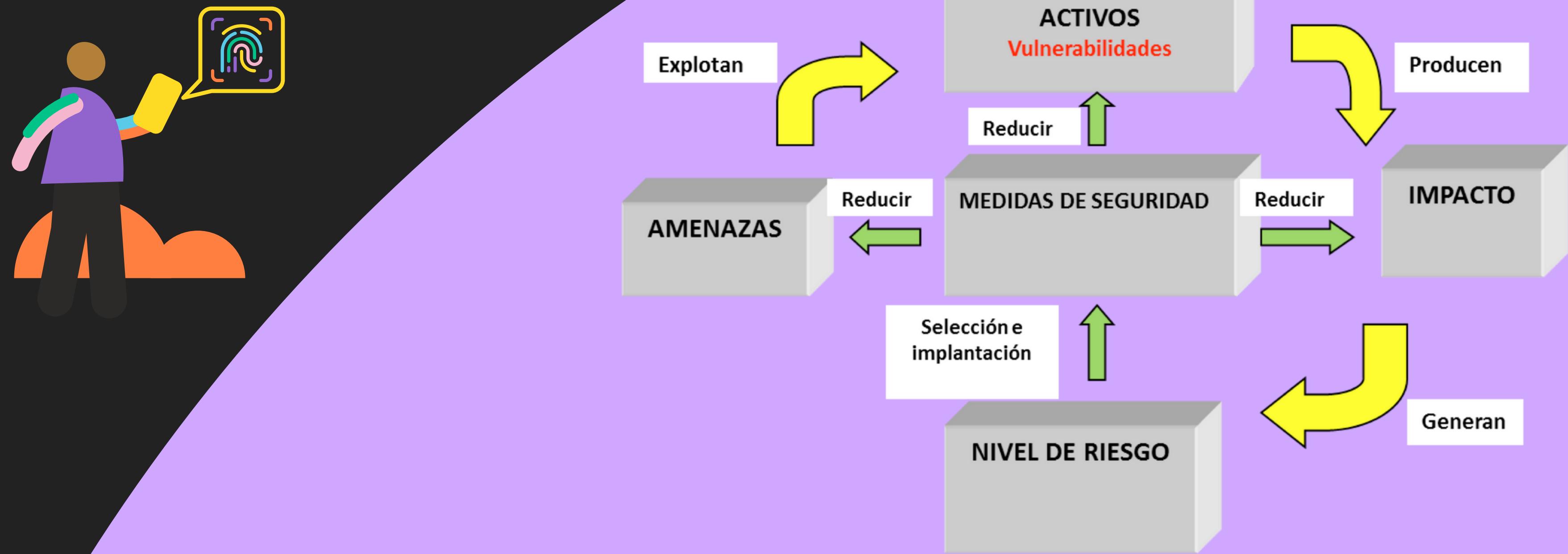


Fig 1: Riesgos, Amenazas y Vulnerabilidades, Alexander Suma

OWASP - MASVS



Fig 2: OWASP MASVS, Owasp Foundation

OWASP TOP 10 MOBILE VULNERABILIDADES

1

USO INCORRECTO DE
LA PLATAFORMA

2

ALMACENAMIENTO
DE DATOS INSEGURO

3

COMUNICACIÓN
INSEGURA

4

AUTENTICACIÓN
INSEGURA

5

CRPTOGRAFÍA
INSUFICIENTE



OWASP TOP 10 MOBILE VULNERABILIDADES

6

AUTORIZACIÓN
INSEGURA

8

MANIPULACIÓN
DEL CÓDIGO

7

MALA CALIDAD DEL
CÓDIGO

9

INGENIERÍA
INVERSA

10

FUNCIONALIDADES EXTRAÑAS

OTRAS AMENAZAS COMUNES EN AMBIENTES DE DESARROLLO



REPOSITORIOS



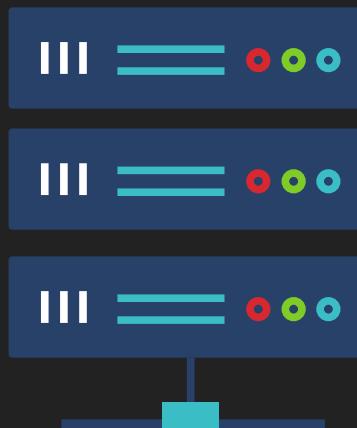
VULNERABILIDADES
DE FRAMEWORKS



VULNERABILIDADES
DE CÓDIGO



AUSENCIA DE
PRUEBAS



SERVIDORES



HERRAMIENTAS

FLUTTER Y EL RETO DE LA SEGURIDAD

ARQUITECTURA BASADA EN WIDGETS

DART

SEGURIDAD INTRÍNSECA DEL FRAMEWORK

ALMACENAMIENTO SEGURO DE DATOS

AUTENTICACIÓN Y AUTORIZACIÓN

PRUEBAS DE SEGURIDAD



BUENAS PRACTICAS DE SEGURIDAD AL DESARROLLAR CON FLUTTER

USO DE HERRAMIENTAS DE SEGURIDAD QUE IMPIDAN MODIFICACIONES NO AUTORIZADAS

GARANTIZAR EL USO DE VERSIONES ACTUALIZADAS DEL FRAMEWORK.

USO DE HERRAMIENTAS DE MONITOREO.

REALIZAR ANÁLISIS ESTÁTICO DEL CÓDIGO

USAR HERRAMIENTAS DE AUTOMATIZACIÓN CI/CD

GARANTIZAR EL USO DE ARQUITECTURAS LIMPIAS

MANTENER DOCUMENTACIONES ACTUALIZADAS

CAPACITACIÓN CONSTANTE AL EQUIPO DE DESAROLLADORES

NEGOCIO



BUENAS PRACTICAS DE SEGURIDAD AL DESARROLLAR CON FLUTTER

USO DE LINTERS PARA VERIFICACIÓN DE CÓDIGO

USO DE VARIABLES DE ENTORNO (USANDO HERRAMIENTAS SEGURAS)

CREAR PRUEBAS UNITARIAS Y DE INTEGRACIÓN

REVISIÓN ESTRICTA DE PERMISOS

HACER PRUEBAS DE SEGURIDAD MIENTRAS SE EJECUTAN HERRAMIENTAS DE ACCESIBILIDAD.

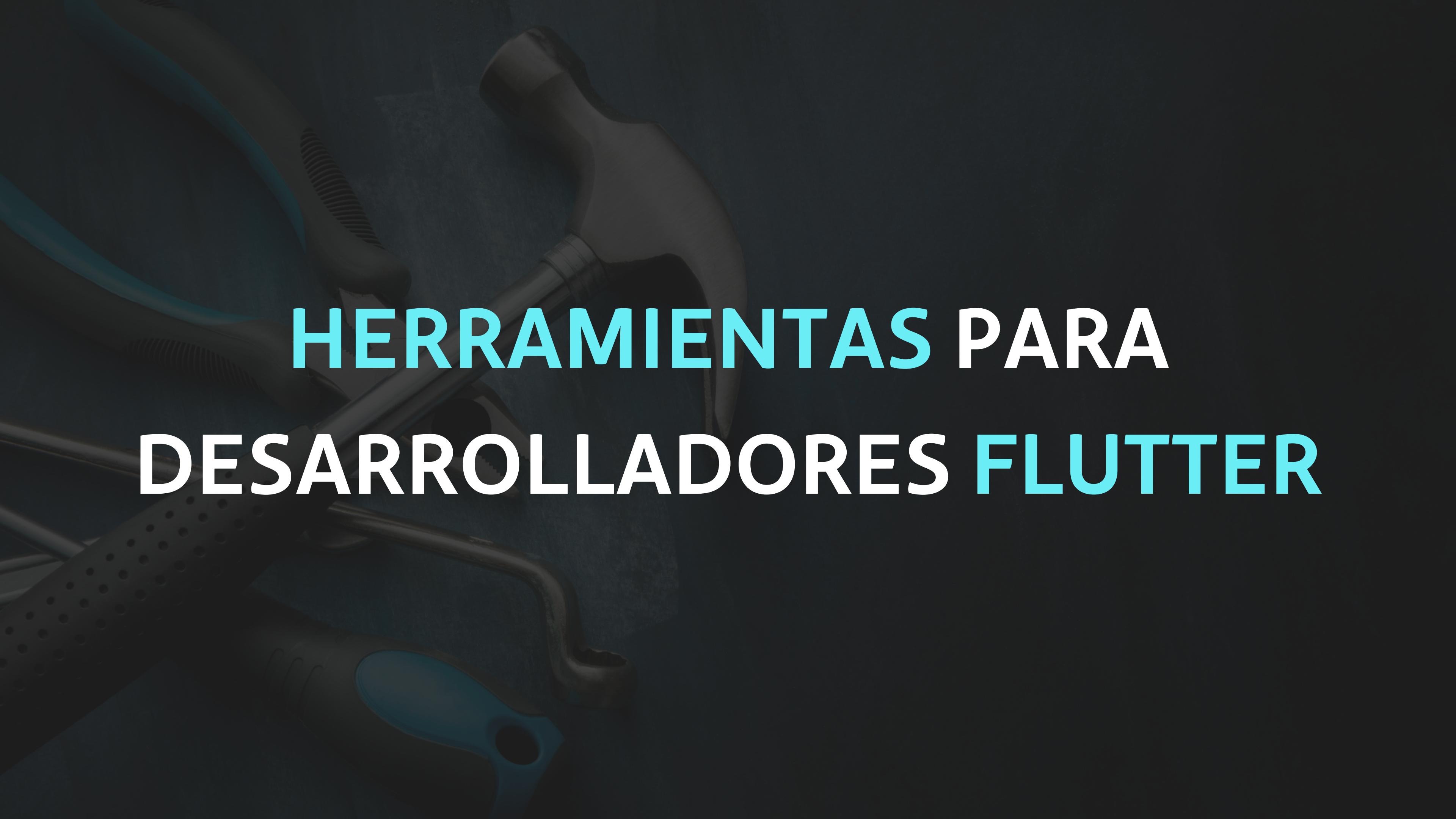
DESARROLLAR USANDO CRITERIOS DE CÓDIGO LIMPIO.

USAR VERSIONES ESPECÍFICAS DE LAS DEPENDENCIAS Y ACTUALIZAR EL README.

SEGUIR ESTRICTAMENTE LOS LINEAMIENTOS DEL NEGOCIO.

DESARROLLADOR





HERRAMIENTAS PARA DESARROLLADORES FLUTTER



Dart Code Metrics

Analyse and improve your code quality.

[Get Started](#)

Star 785



Improve your code quality



Additional rules



Use as Analyzer plugin

HCL APPSCAN CODESWEEP

Wow!

File Edit Selection View Go Run Terminal Help translate.js - Sample-File - Visual Studio Code

APPSCAN

translate.js X

SECURITY ISSUES

/*when using angular-translate and variable content, the re

Currently there is an issue with the sanitize mode, it will

Additionally, there are this defaults only valid for versio

null: nothing, unsecure default (will be removed in 3.0)

escaped: alias for 'escapeParameters' for backwards compati

PROBLEMS 3 OUTPUT ... Filter: E.g.: text, **/*.ts, !**/node_modules/**

JS translate.js 3

- Expression expected. ts(1109) [25, 1]
- ';' expected. ts(1005) [25, 11]
- ';' expected. ts(1005) [45, 18]

AppScan marker On Ln 5, Col 31 Spaces: 4 UTF-8 LF JavaScript R Q

MOBSF

The image shows the MOBSF (Mobile Security Framework) web application interface. The background features a vibrant, abstract graphic with horizontal bands of orange, yellow, blue, and green against a black backdrop. The main content area has a blue-to-green gradient background.

Top Navigation Bar:

- RECENT SCANS
- DYNAMIC ANALYZER
- MOBSF** (Logo)
- API DOCS
- ABOUT

Middle Section:

- Upload & Analyze** button with a cloud icon.
- A placeholder text "Drop & Drag your APK here!" below the upload button.

Search Bar:

Search MDS

Footer:

- RECENT SCANS | DYNAMIC ANALYZER | API DOCS | ABOUT
- © 2020 Mobile Security Framework - MobSF v3.1.7 Beta

CONCLUSIONES

LECTURAS RECOMENDADAS

OWASP MASVS: [HTTPS://MAS.OWASP.ORG/MASVS/](https://mas.owasp.org/MASVS/)

OWASP MASTG: [HTTPS://MAS.OWASP.ORG/MASTG/](https://mas.owasp.org/MASTG/)

OWASP MAS CHECKLIST:

[HTTPS://MAS.OWASP.ORG/MAS_CHECKLIST/](https://mas.owasp.org/MAS_CHECKLIST/)

NORMA ISO 27001: [HTTPS://WWW.ISO.ORG/ISOIEC-27001-INFORMATION-SECURITY.HTML](https://www.iso.org/ISOIEC-27001-INFORMATION-SECURITY.HTML)

SECURING FLUTTER APPS:

[HTTPS://MEDIUM.COM/@MEHMETF_71205/SECURING-FLUTTER-APPS-ADA13E806A69](https://medium.com/@MEHMETF_71205/SECURING-FLUTTER-APPS-ADA13E806A69)



¿Preguntas?



AGRADECIMIENTOS

DIEGO ADEMIR DUARTE, SECURITY AND COMPLIANCE OFFICER, PLATZI

DANIEL HERRERA SANCHEZ, SR. FRONT-END ENGINEER, BANCOLOMBIA

OWASP COMMUNITY

¡Muchas Gracias!



SCAN ME

