

# Tarea online PPS04.

---

Título de la tarea: Defensas anti-ingeniería inversa y soluciones CASB.

Unidad: 4

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Puesta en Producción Segura.

## ¿Qué contenidos o resultados de aprendizaje trabajaremos?

### Resultados de aprendizaje

- ✓ **RA4.** Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

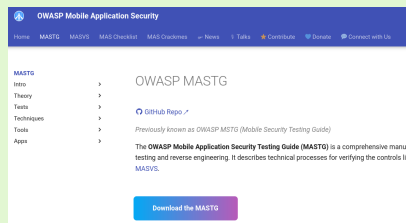
### Contenidos

- 1.- Detección de problemas de seguridad en aplicaciones para dispositivos móviles.
  - 1.1.- Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.
  - 1.2.- Firma y verificación de aplicaciones.
  - 1.3.- Almacenamiento seguro de datos.
  - 1.4.- Validación de compras integradas en la aplicación.
  - 1.5.- Fuga en los ejecutables
  - 1.6.- Soluciones CASB.

# 1.- Descripción de la tarea.



## Caso práctico



[MASTG](#) (Captura de pantalla)

**Julián** ha estado trabajando en un proyecto de una aplicación móvil junto con una solución CASB que quiere salir al mercado y ser revolucionaria.

Para comprobar que la aplicación es segura se ha seguido la última versión de la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) desarrollada por OWASP. **Julián** entiende que el Estándar de Verificación de

Seguridad de Aplicaciones Móviles (MASVS) proporciona un marco claro y detallado que aborda los requisitos de seguridad esenciales para el desarrollo y la evaluación de aplicaciones móviles. Por otro lado, la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) se alinea estrechamente con los requisitos establecidos por la MASVS, ofreciendo un conjunto adicional de directrices específicas para realizar pruebas de seguridad efectivas en aplicaciones móviles. La combinación de ambas herramientas, MASVS y MASTG, proporciona un enfoque integral para evaluar y mejorar la seguridad en aplicaciones móviles, permitiendo a los profesionales adaptar sus estrategias según el contexto específico.

Uno de los puntos que más se han trabajado durante el proyecto de la solución CASB es ser diferenciadores y poder corregir los problemas de adopción que han tenido las soluciones de MDM (Mobile Device Management). Saben que las soluciones para móviles tienen que ser capaces de lidiar con varios problemas como la privacidad, 🇺🇸 BYOD (*Bring Your Own Device*), etc.

## ¿Qué te pedimos que hagas?

Esta tarea es eminentemente teórica donde el alumno deberá responder y desarrollar una serie de preguntas. El alumno debe saber manejar guías para comprobar si una aplicación móvil es segura o no, entender distintos conceptos como CASB, MDM, BYOD, etc y ser capaz de entender que capacidades aportan las soluciones tecnológicas, con qué problemas se encuentran en el mercado y qué capacidades adicionales podrían tener y qué las empresas valorarían.

✔ **Apartado 1: MASTG** (ver [enlace](#) 📄 )

En la unidad 2 ya vimos que OWASP ha desarrollado el proyecto Mobile Application

Security (MAS) que proporciona un estándar de seguridad para aplicaciones móviles (OWASP MASVS) y una guía de pruebas exhaustiva (OWASP MASTG) que cubre los procesos, técnicas y herramientas utilizados durante una prueba de seguridad de aplicaciones móviles, así como un conjunto exhaustivo de casos de prueba que permite a los probadores ofrecer resultados coherentes y completos.

En este apartado se pide **revisar la guía MASTG**, centrándote en las **diferentes defensas contra la Ingeniería Inversa en Android** (Android Anti-Reversing Defenses) y **en IOS** (IOS Anti-Reversing Defenses)

1.- Una medida defensiva es **comprobar el "Rooteado" en Android y el "Jailbreak" en IOS**. Rellena la siguiente tabla utilizando la guía MASTG

¿Qué son los dispositivos rooteados o con jailbreak?	
Indica 1 medida para comprobar el rooteado	
Indica 1 medida para comprobar el Jailbreak	

2.- Otra medida defensiva es la **ofuscación**. Rellena la siguiente tabla utilizando la guía MASTG

¿ En qué consiste la ofuscación?	
Indica para que se utiliza la herramienta <b>ProGuard</b> y cómo se utiliza	
Indica para que se utiliza la herramienta <b>SwiftShield</b> y cómo se utiliza	

3.- Explorar aplicaciones utilizando un depurador es una técnica muy poderosa. No solo se puede rastrear variables que contienen datos confidenciales y modificar el flujo de control de la aplicación, sino también leer y modificar la memoria y los registros. Rellena la siguiente tabla utilizando la guía MASTG

Explica qué consiste la técnica antidepuración <b>JDWP en Android</b>	
Explica qué es <b>ptrace</b> y cómo se puede utilizar para evitar la depuración en <b>IOS</b>	

4.- La presencia de herramientas, frameworks y aplicaciones comúnmente utilizadas por la ingeniería inversa puede indicar un intento de realizar ingeniería inversa en la aplicación. Algunas de estas herramientas sólo pueden ejecutarse en un dispositivo con jailbreak o rooteado, mientras que otras obligan a la aplicación a entrar en modo de depuración o dependen del inicio de un servicio en segundo plano en el teléfono móvil. Por lo tanto, **existen diferentes formas que una aplicación puede implementar para detectar un ataque de ingeniería**

**inversa y reaccionar ante él**, por ejemplo, finalizándose ella misma. Utilizando la guía MASTG

Explica qué es y para que se utiliza la herramienta <b>Frida</b>	
Explica cómo se puede detectar en IOS (Frida Detection)	

## ✓ Apartado 2: CASB y MDM

Los servicios **CASB (Cloud Access Security Broker)** y las plataformas **MDM (Mobile Device Management)** desempeñan roles esenciales en la seguridad de la información en entornos empresariales modernos. La combinación de CASB y MDM proporciona un enfoque integral para abordar las amenazas modernas, asegurando tanto los datos en la nube como los dispositivos móviles, lo que es crucial para salvaguardar la integridad y confidencialidad de la información empresarial.

- 1.- ¿Qué diferencias hay entre CASB y MDM (Mobile Device Management)?
- 2.- ¿Con qué problemas se han encontrado las soluciones de MDM?

## ✓ Apartado 3: Diseño y capacidades de CASB

- 1.- ¿Qué ventajas y desventajas en un entorno de CASB aporta tener un agente instalado en los terminales?
- 2.- ¿Qué problema supone cuando un usuario se va de la empresa en un entorno de BYOD (Bring Your Own Device)? ¿Qué mecanismos podríamos tener en nuestro entorno de CASB ideal para cuando un usuario abandone la compañía y siga siendo compatible con BYOD?
- 3.- ¿Qué capacidades adicionales podríamos añadir a nuestra solución de CASB?

### NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

## 2.- Información de interés.


---

### Recursos necesarios y recomendaciones

#### Recursos necesarios

- ✓ Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- ✓ Conexión a Internet.
- ✓ Navegador web.

#### Recomendaciones

- ✓ Antes de abordar la tarea:
  - ➔ Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el docente y aclara las dudas que te surjan con él.
  - ➔ Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- ✓ Familiarízate con:
  - ➔ Guía OWASP MASTG: <https://mas.owasp.org/MASTG/> 
  - ➔ Concepto "dispositivo roteado o con jailbreak"
  - ➔ Concepto ofuscación de código
  - ➔ Concepto depuración de código.
  - ➔ Herramientas de ingeniería inversa: Frida
  - ➔ Concepto CASB
  - ➔ Concepto BYOD (Bring Your Own Device)
  - ➔ Concepto MDM (Mobile Device Management)
- ✓ Para responder a las preguntas es recomendable ponerse tanto del lado de la empresa que adopta una serie de medidas o soluciones tecnológicas como del lado de los usuarios de dispositivos móviles.



### Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

**Apellido1\_Apellido2\_Nombre\_PPS\_Tarea04**

### 3.- Evaluación de la tarea.

#### Criterios de evaluación implicados

##### Criterios de evaluación RA4

- ✓ a. Se han comparado los diferentes modelos de permisos de las plataformas móviles.
- ✓ b. Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.
- ✓ c. Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.
- ✓ d. Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.
- ✓ e. Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.

#### ¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
<b>Apartado 1.1:</b> Rellena la tabla	1,5 punto
<b>Apartado 1.2:</b> Rellena la tabla	1 punto
<b>Apartado 1.3:</b> Rellena la tabla	1,5 puntos
<b>Apartado 1.4:</b> Rellena la tabla	1 punto
<b>Apartado 2.1:</b> ¿Qué diferencias hay entre CASB y MDM (Mobile Device Management)?	1 puntos
<b>Apartado 2.2:</b> ¿Con qué problemas se han encontrado las soluciones de MDM?	1 punto

<b>Apartado 3.1:</b> ¿Qué ventajas y desventajas en un entorno de CASB aporta tener un agente instalado en los terminales?	1 punto
<b>Apartado 3.2:</b> ¿Qué problema supone cuando un usuario se va de la empresa en un entorno de BYOD (Bring Your Own Device)? ¿Qué mecanismos podríamos tener en nuestro entorno de CASB ideal para cuando un usuario abandone la compañía y siga siendo compatible con BYOD?	1 punto
<b>Apartado 3.3:</b> ¿Qué capacidades adicionales podríamos añadir a nuestra solución de CASB?	1 punto

### NOTA IMPORTANTE

**Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.**