



TAREA 04


**DETECCIÓN DE
PROBLEMAS DE
SEGURIDAD EN
APLICACIONES PARA
DISPOSITIVOS MÓVILES**

PUESTA EN PRODUCCIÓN SEGURA

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información



Caso práctico

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.

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 valorarán.

Apartado 1: [MASTG](#)

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, centrándose 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?	Son dispositivos a los que se les han eliminado las restricciones del fabricante. Esto permite al usuario tener un control total sobre el sistema operativo, pudiendo instalar aplicaciones no oficiales, personalizar el dispositivo y acceder a funciones avanzadas. Sin embargo, aumenta los riesgos de seguridad.
Indica 1 medida para comprobar el rooteado	Para comprobar que un dispositivo Android está rooteado se puede utilizar la aplicación Root Checker. Verifica si el dispositivo tiene acceso al superusuario (root) y proporciona un informe sobre su estado.
Indica 1 medida para comprobar el Jailbreak	Para comprobar que un dispositivo iOS tiene jailbreak, se puede buscar la aplicación Cydia en el dispositivo. Es una tienda de aplicaciones alternativas que solo estarán disponibles para ese tipo de dispositivos.

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

¿ En qué consiste la ofuscación?	Técnica de seguridad que transforma el código legible, en algo difícil de leer (formato ininteligible) y entender para los humanos, pero que sigue funcionando igual. Se hace para proteger el código de los atacantes que intentan analizarlo o modificarlo. (ejemplo: cambiar nombres de funciones)
Indica para qué se utiliza la herramienta ProGuard y cómo se utiliza	Herramienta de línea de comandos que se usa en aplicaciones Android para reducir, optimizar y ofuscar el código (Java). Ayuda a hacer el archivo APK más pequeño y seguro. Para utilizarlo se añade una configuración en el archivo build.gradle, activando la opción minifyEnabled y especificando las reglas de la herramienta.
Indica para qué se utiliza la herramienta SwiftShield y cómo se utiliza	Es una herramienta para aplicaciones iOS que ofusca el código escrito en Swift. Protege la lógica y la propiedad intelectual de la aplicación contra la ingeniería inversa. Para usarlo, se integra en el proceso de compilación del proyecto, configurando las opciones de ofuscación en el archivo de configuración del proyecto.

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 JDWP en Android	(Java Debug Wire Protocol) Se utiliza para evitar que los atacantes depuren la aplicación. Es un protocolo que permite la depuración de aplicaciones Java y en Android se usa para depurar aplicaciones en ejecución. Para proteger la aplicación, se puede implementar medidas que detecten si un depurador está conectado y si es así, cerrar la aplicación o cambiar su comportamiento para dificultar la depuración.
Explica qué es ptrace y cómo se puede utilizar para evitar la depuración en IOS	Es una función en sistemas Unix que permite controlar un proceso a través de otro (proceso padre), lo que es útil para la depuración. En iOS, se puede usar esta herramienta con la opción PT_DENY_ATTACH para evitar que otros depuradores se adjunten a la aplicación. Si un depurador intenta adjuntarse, el proceso se termina automáticamente (porque el proceso padre observa, examina y controla el resto de procesos), lo que dificulta la depuración por parte de los atacantes.

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 Frida	Es una herramienta de instrumentación dinámica que permite a los desarrolladores y analistas de seguridad inyectar código en aplicaciones móviles a tiempo real. Esto significa que pueden observar y modificar el comportamiento de una aplicación mientras se ejecuta. Se utiliza para el análisis de seguridad, la depuración y la ingeniería inversa de aplicaciones en múltiples plataformas (incluyendo Android e iOS)
Explica cómo se puede detectar en IOS (Frida Detection)	Para detectar si una aplicación está siendo manipulada con Frida en iOS, se pueden implementar diferentes técnicas. Una de ellas es buscar la presencia de procesos o librerías asociadas con Frida (frida-server o FridGadget.dylib). Otra técnica, es monitorear las conexiones de red inusuales que podrían indicar que Frida está interactuando con la aplicación.

Apartado 2: MDM y CASB

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- Rellena la siguiente tabla comparativa CASB vs MDM

	CASB	MDM
Objetivo principal	(Cloud Access Security Broker) Proteger y controlar el acceso a los datos y aplicaciones en la nube. Actúa como un intermediario entre los usuarios y los servicios en la nube para asegurar el cumplimiento de las políticas de seguridad.	(Mobile Device Management) Gestionar y asegurar los dispositivos móviles utilizados en una organización (smartphones, tablets y otros dispositivos). Garantizando que cumplan con las políticas de seguridad de la empresa.
Alcance y enfoque	Seguridad de aplicaciones y datos en la nube, proporcionando visibilidad, control y protección contra amenazas para todas las aplicaciones (autorizadas como no autorizadas).	Gestión y seguridad de dispositivos móviles, controlando el acceso a recursos, administrando aplicaciones y configuraciones y protegiendo los datos almacenados en el dispositivo.
Gestión (¿qué elementos se gestionan?)	Acceso a aplicaciones y datos en la nube, monitoreo del uso de las aplicaciones, prevención de pérdida de datos y detección de amenazas.	Dispositivos móviles, incluyendo instalación de aplicaciones, configuración de políticas de seguridad, monitoreo de dispositivos, protección de datos (mediante cifrado) y eliminación remota, por pérdida o robo.
Arquitectura (¿cómo se implementa?)	Generalmente se implementa como un servicio en la nube, que actúa como intermediario entre los usuarios y las aplicaciones en la nube. Pueden funcionar como un proxy directo o inverso.	Se implementa a través de un servidor central que gestiona los dispositivos móviles conectados. Puede ser una solución basada en la nube o en las instalaciones de la empresa.
¿Qué problemas o limitaciones tiene cada una (por ejemplo, con la protección de datos)?	Pueden ser complejos de configurar y gestionar, y pueden no cubrir todas las aplicaciones SaaS utilizadas por la empresa. También pueden tener limitaciones en la integración con soluciones de identidad y acceso.	Pueden ser difíciles de implementar y gestionar debido a la diversidad de dispositivos y sistemas operativos. Además, pueden enfrentar problemas de compatibilidad y fragmentación (especialmente en dispositivos Android)
Da 3 ejemplos de soluciones MDM y 3 CASB	Netskope Microsoft Cloud App Security. McAfee Mvision Cloud	AirDroid Business Scalefusion Hexnode

A la hora de escoger una solución CASB es importante conocer cuales son las características más importantes de las mismas.

2- Rellena la siguiente tabla, identificando y describiendo detalladamente y con un ejemplo al menos cinco características clave que suelen ofrecer las soluciones CASB (ejemplo: control de acceso, prevención de fuga de datos, etc.). Como ejemplo de lo que se pide se rellena una característica típica como el control de acceso.

Característica	Descripción detallada	Ejemplo
Control de acceso y autenticación	Implementa políticas de acceso basadas en el contexto, como ubicación, tipo de dispositivo, nivel de riesgo o autenticación multifactor (MFA). Se puede restringir el acceso en función del usuario o del rol dentro de la empresa.	Un usuario intenta acceder a la aplicación de contabilidad desde un dispositivo no administrado. El CASB impide el acceso o solicita autenticación adicional.
Prevención de pérdida de datos (DLP)	Protege la información confidencial evitando que se compartan o se transmitan de manera no autorizada. Utiliza políticas para identificar y bloquear la transmisión de datos sensibles, como números de tarjetas de crédito o información personal	Un empleado intenta enviar un correo electrónico con un archivo que contiene datos de clientes. El CASB detecta la información sensible y bloquea el envío del correo.
Visibilidad y monitoreo	Proporciona una visión completa del uso de aplicaciones en la nube, incluyendo quién accede, qué datos se comparten y cómo se utilizan las aplicaciones. Esto ayuda a identificar comportamientos sospechosos y a tomar medidas preventivas.	El equipo de seguridad puede ver que un usuario está descargando grandes cantidades de datos desde una aplicación en la nube fuera de horario laboral, podría indicar una actividad no autorizada.
Protección contra amenazas	Detecta y responde a comportamientos anómalos y amenazas en la nube, como malware, ransomware o accesos no autorizados. Utiliza un análisis avanzado para identificar y mitigar riesgos en tiempo real.	El CASB detecta el intento de acceso desde una ubicación geográfica inusual y bloquea el acceso para evitar una posible brecha de seguridad.
Cumplimiento normativo	Ayuda a la empresa a cumplir con las regulaciones y normativas de seguridad, como GDPR, HIPAA o PCI- DSS. Proporciona herramientas para auditar y reportar el cumplimiento de políticas de seguridad en la nube.	Una empresa necesita demostrar que cumple con las regulaciones de protección de datos. El CASB genera informes detallados sobre el uso de datos y las medidas de seguridad implementadas.
Evaluación y administrador	Identifica y gestiona el uso de aplicaciones en la nube no autorizadas por la empresa, conocidas como Shadow IT. Esto ayuda a controlar los riesgos asociados con el uso de aplicaciones no aprobadas.	El CASB detecta que varios empleados están utilizando una aplicación de almacenamiento en la nube no autorizada y bloquea su uso para proteger los datos corporativos.

Apartado 3: Diseño y capacidades de CASB

Elige una solución CASB disponible en el mercado (ejemplo: Microsoft Defender for Cloud Apps, Netskope, McAfee MVISION Cloud, Palo Alto Prisma Access, etc.).

1- Rellena la siguiente tabla describiendo cinco características de dicha solución que te han parecido las más importantes (deben ser distintas a las que has puesto en el apartado 2.2). Justifica por qué te parecen importantes.

Característica	Justificación
Análisis de comportamiento de usuarios y entidades (UEBA)	Esta característica utiliza inteligencia artificial para analizar el comportamiento de los usuarios y detectar actividades inusuales que podrían indicar una amenaza. Es importante porque ayuda a identificar y mitigar riesgos antes de que se conviertan en problemas graves.
Control de aplicaciones no autorizadas (Shadow IT)	Permite a las empresas identificar y gestionar el uso de aplicaciones en la nube que no han sido aprobadas oficialmente. Esto es crucial para evitar riesgos de seguridad asociados con el uso de aplicaciones no controladas.
Protección de datos a tiempo real	Y monitorea y protege los datos en tiempo real mientras se mueven entre dispositivos y aplicaciones en la nube. Esto es esencial para prevenir la pérdida de datos y garantizar que la información sensible esté siempre segura.
Integración con otras soluciones de seguridad	Se integra fácilmente con otras herramientas de seguridad, como soluciones de gestión de identidades y accesos y sistemas de información y gestión de eventos de seguridad. Esta integración mejora la capacidad de respuesta ante incidentes y proporciona una visión más completa de la seguridad.
Cumplimiento normativo automatizado	Ayuda a las empresas a cumplir con regulaciones normativas de seguridad mediante la ayuda automatización de políticas y generación de informes de cumplimiento. Esto es importante para reducir el riesgo de sanciones y mantener la confianza en los clientes.
Cifrado de datos	Esta característica asegura que los datos sensibles estén cifrados tanto en tránsito como en reposo. El cifrado protege la información contra accesos no autorizados, incluso si los datos son interceptados o robados. Es crucial mantener la confidencialidad y la integridad de los datos empresariales.
Gestión de entidades y accesos (IAM)	Integra capacidades avanzadas de gestión de identidades y accesos, permitiendo una administración centralizada de las identidades de los usuarios y sus permisos. Esto es importante para garantizar que solo las personas autorizadas puedan acceder a los datos y aplicaciones sensibles, reduciendo el riesgo de accesos no autorizados.

2- Responde a las siguientes cuestiones:

¿Qué problema supone cuando un usuario se va de la empresa en un entorno de BYOD (Bring Your Own Device)?

Cuando un usuario abandona la empresa en un entorno BYOD surgen diferentes problemas de seguridad y gestión:

- Un antiguo trabajador puede seguir teniendo acceso a datos y aplicaciones corporativas desde su dispositivo personal, lo que representa un riesgo significativo de fuga de información confidencial.
- La empresa pierde la capacidad de gestionar y controlar el dispositivo, lo que dificulta la implementación de políticas de seguridad y la protección de datos sensibles de la organización.
- Existe el riesgo de que el usuario utilice el dispositivo con un fin malintencionado, existe la posibilidad de que el antiguo trabajador utilice la información y los accesos para fines maliciosos, como compartir datos con personas externas (competencia) o realizar actividades fraudulentas.
- Quitar los accesos a aplicaciones y datos corporativos en dispositivos personales puede ser complicado y no siempre puede resultar efectivo, especialmente si el dispositivo no está bajo la gestión de la empresa.

¿Qué mecanismos deberías tener en la solución CASB que has planteando en el apartado 3.1 para cuando un usuario abandone la compañía y siga siendo compatible con BYOD?

Para abordar dichos problemas, la solución CASB (Microsoft Defender for Cloud Apps) debe incluir los siguientes mecanismos:

- El CASB debe permitir la revocación inmediata de accesos a aplicaciones y datos corporativos en cuanto se detecte que un usuario ha dejado la empresa. Se podría realizar mediante la integración con sistemas de gestión de identidades y accesos (IAM) para desactivar cuentas y permisos de forma centralizada.
- Implementar alguna política que restrinja el acceso a datos sensibles desde dispositivos no administradores o no autorizados. Esto asegura que, una vez que el usuario deja la empresa, su dispositivos personal no pueda acceder a los datos, no podrá leerlos sin las claves de acceso adecuadas.
- Mantener un monitoreo o auditoría constante de las actividades de los usuarios y generar alertas en caso de comportamientos sospechosos. Esta ayuda a detectar y responder rápidamente a cualquier intento de acceso no autorizado después de que un usuario se haya ido de la empresa.
- Implementar políticas de DLP (Prevención de Pérdida de datos) que bloqueen la transferencia de datos sensibles a dispositivos no autorizados o a ubicaciones no seguras. Esto previene que los ex-empleados puedan copiar o transferir información crítica fuera de la red corporativa.
- Integrar la solución CASB con sistemas de gestión de dispositivos móviles (MDM) para asegurar la eliminación remota de datos corporativos en caso de necesidad.

Cuando un empleado deja la empresa en un entorno BYOD, puede seguir teniendo acceso a datos sensibles, lo que representa un riesgo de seguridad. Para mitigar estos riesgos, es esencial usar una solución CASB como Microsoft Defender Cloud Apps, que permite revocar accesos en tiempo real, controlar dispositivos no autorizados, cifrar datos, monitorear actividades y cumplir con normativas de seguridad. Estos mecanismos aseguran que la información corporativa permanezca protegida bajo control, incluso cuando se utilizan dispositivos personales.