

**UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS**



Guía Práctica de Laboratorio

Laboratorio 02 “Auditoría Móvil”

Que se presenta para el curso:
“Auditoría de sistemas”

Integrante(s):

- Escobar Rejas, Carlos Andrés

Docente:

- Dr. Oscar Juan Jimenez Flores

**TACNA – PERÚ
2025**

Índice General

Introducción.....	3
1. Información sobre el evento práctico	4
1.1. Título del evento práctico	4
Laboratorio 02. Auditoria Móvil	4
1.2. Objetivos	4
1.3. Tiempo de duración (horas)	4
1.4. Resultados de Aprendizaje (RA)	4
1.5. Recursos (Equipos, materiales, programas y otros)	4
2. Procedimiento o Metodología	5
3. Conclusiones	89
4. Referencias Bibliográficas	99
5. Actividad	9

Introducción

La auditoría de seguridad en Tecnologías de la Información y Comunicación (TIC) es un proceso sistemático y estructurado que evalúa la eficacia y la integridad de los controles de seguridad implementados en una organización. Su objetivo principal es identificar vulnerabilidades, asegurar el cumplimiento de políticas y normas, y verificar que los sistemas de TIC protejan adecuadamente la confidencialidad, integridad y disponibilidad de la información.

Durante una auditoría de seguridad en TIC, se examinan diversos aspectos, como la configuración de hardware y software, los controles de acceso, las políticas de seguridad, los procedimientos de respaldo y recuperación, y la gestión de incidentes. Además, se evalúan las prácticas de gestión de riesgos y el cumplimiento de normativas y estándares relevantes.

El objetivo de este laboratorio es realizar una auditoría de seguridad, analizar los posibles riesgos asociados y proponer controles.

Guía de Laboratorio N° 02 “Auditoría de seguridad y hallazgos”

1. Información sobre el evento práctico

1.1. Título del evento práctico

Laboratorio 02. Auditoría Móvil

1.2. Objetivos

- Identificar los elementos que participan en la Auditoría de seguridad.
- Analizar los posibles riesgos asociados.
- Proponer controles efectivos para minimizar el riesgo asociado.

1.3. Tiempo de duración (horas)

06 horas académicas

1.4. Resultados de Aprendizaje (RA)

[AG-I02] Ética
[AG-I04] Comunicación
[AG-I07] Conocimientos de Ingeniería
[AG-I08] Análisis de Problemas
[AG-I09] Diseño y Desarrollo de Soluciones
[AG-I11] Uso de Herramientas

1.5. Recursos (Equipos, materiales, programas y otros)

- Computador con S.O.
- Descargar e instalar repositorio GIT

<https://github.com/OscarJimenezFlores/CursoAuditoria/tree/main/AuditoriaMovil>

2. Procedimiento o Metodología

Paso 1 – Preparación del Entorno

Descripción:

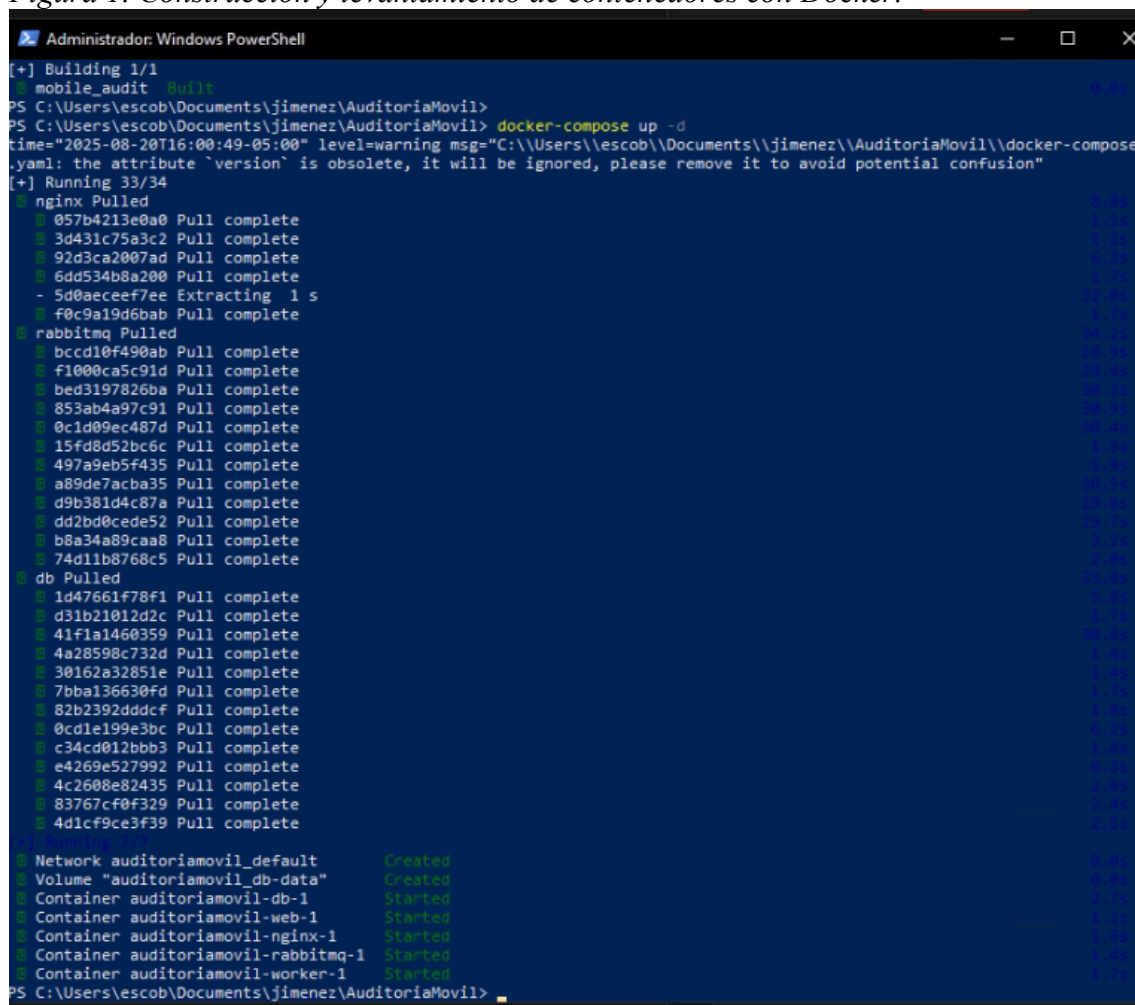
Clonar el repositorio oficial y preparar el entorno para levantar los servicios con Docker Compose.

Comando (PowerShell):

```
git clone https://github.com/OscarJimenezFlores/CursoAuditoria.git
cd CursoAuditoria/AuditoriaMovil
docker-compose build
docker-compose up -d
```

Imagen:

Figura 1. Construcción y levantamiento de contenedores con Docker.



```
Administrador: Windows PowerShell
[+] Building 1/1
  mobile_audit Built
PS C:\Users\escob\Documents\jimenez\AuditoriaMovil>
PS C:\Users\escob\Documents\jimenez\AuditoriaMovil> docker-compose up -d
time="2025-08-20T16:00:49-05:00" level=warning msg="C:\\Users\\escob\\Documents\\jimenez\\AuditoriaMovil\\docker-compose
.yaml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 33/34
  nginx Pulled
    057b4213e0a0 Pull complete
    3d431c75a3c2 Pull complete
    92d3ca2007ad Pull complete
    6dd534b8a200 Pull complete
    - 5d0aeecef7ee Extracting 1 s
    f0c9a19d6bab Pull complete
  rabbitmq Pulled
    bccd10f490ab Pull complete
    f1000ca5c91d Pull complete
    bed3197826ba Pull complete
    853ab4a97c91 Pull complete
    0c1d09ec487d Pull complete
    15fd8d52bc6c Pull complete
    497a9eb5f435 Pull complete
    a89de7acba35 Pull complete
    d9b381d4c87a Pull complete
    dd2bd0cede52 Pull complete
    b8a34a89caa8 Pull complete
    74d11b8768c5 Pull complete
  db Pulled
    1d47661f78f1 Pull complete
    d31b21012d2c Pull complete
    41f1a1460359 Pull complete
    4a28598c732d Pull complete
    30162a32851e Pull complete
    7bba136630fd Pull complete
    82b2392dddcf Pull complete
    0cd1e199e3bc Pull complete
    c34cd012bbb3 Pull complete
    e4269e527992 Pull complete
    4c2608e82435 Pull complete
    83767cf0f329 Pull complete
    4d1cf9ce3f39 Pull complete
  Network auditoriamovil_default Created
  Volume "auditoriamovil_db-data" Created
  Container auditoriamovil-db-1 Started
  Container auditoriamovil-web-1 Started
  Container auditoriamovil-nginx-1 Started
  Container auditoriamovil-rabbitmq-1 Started
  Container auditoriamovil-worker-1 Started
PS C:\Users\escob\Documents\jimenez\AuditoriaMovil>
```

Observación:

Si ocurre un error con puertos ocupados o fallos de PostgreSQL, ejecutar `docker-compose down` y reconstruir (`docker-compose build`).

Paso 2 – Acceso a la Aplicación Web**Descripción:**

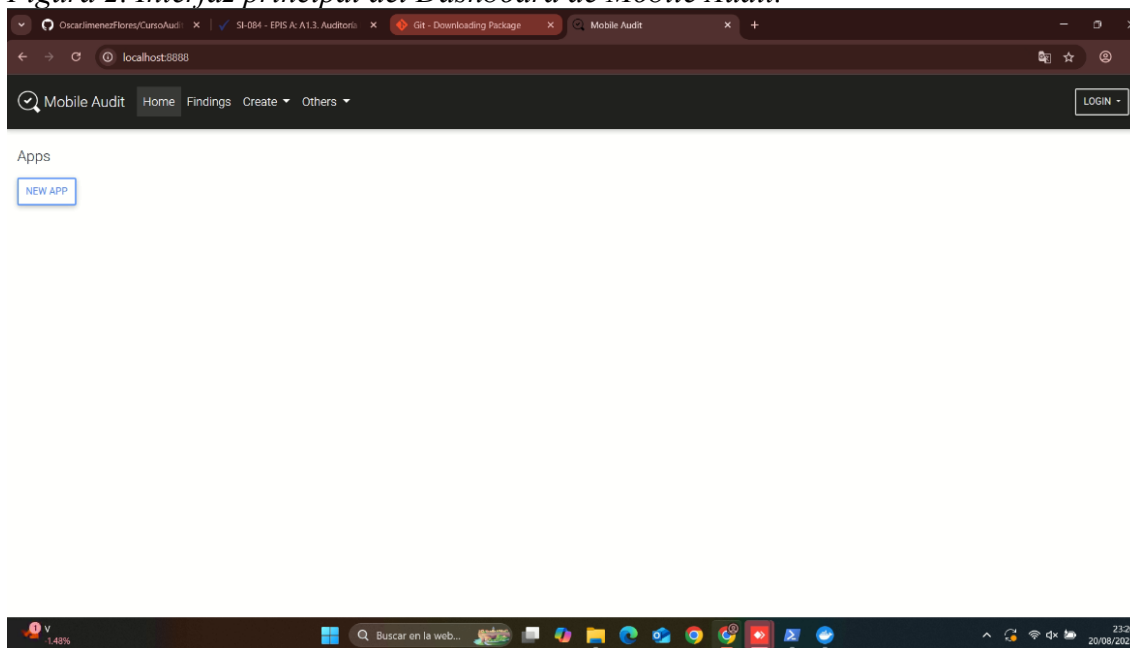
La aplicación Mobile Audit queda disponible en el navegador local.

Acceso:

- `http://localhost:8888`
- Con TLS: `docker-compose -f docker-compose.prod.yaml up` → `https://localhost`

Imagen:

Figura 2. Interfaz principal del Dashboard de Mobile Audit.

**Observación:**

El panel lateral muestra accesos a módulos de análisis, patrones, certificados y exportación de reportes.

Paso 3 – Análisis de APK 1 (Malicioso)**Descripción:**

Se carga el primer archivo APK malicioso en el sistema para ejecutar el análisis estático (SAST).

Acciones:

1. Seleccionar “Subir archivo”.
2. Cargar androRAT.apk (ejemplo).
3. Ejecutar análisis y revisar resultados.

Imagen:

Figura 3. Resultados del análisis del APK 1.

Mobile Audit

Home

Findings

Create

Others

Apps

NEW APP

ID	Name	Created by	Description	Scans																									
1	PZ Fusion v2.8.2	mpolar	plantas vs zombies	<table><thead><tr><th>ID</th><th>Description</th><th>Version</th><th>Created On</th><th>Status</th><th>Progress</th><th>Findings</th><th>By Severity</th><th>Delete</th></tr></thead><tbody><tr><td>1</td><td>plantas vs zombies</td><td>1</td><td>Aug. 21, 2025, 6:27 a.m.</td><td>Finished</td><td>100 %</td><td>50</td><td><div>Critical0</div><div>High9</div><div>Medium15</div><div>Low11</div><div>None15</div></td><td><div>NEW SCAN</div></td></tr></tbody></table>							ID	Description	Version	Created On	Status	Progress	Findings	By Severity	Delete	1	plantas vs zombies	1	Aug. 21, 2025, 6:27 a.m.	Finished	100 %	50	<div>Critical0</div> <div>High9</div> <div>Medium15</div> <div>Low11</div> <div>None15</div>	<div>NEW SCAN</div>	
ID	Description	Version	Created On	Status	Progress	Findings	By Severity	Delete																					
1	plantas vs zombies	1	Aug. 21, 2025, 6:27 a.m.	Finished	100 %	50	<div>Critical0</div> <div>High9</div> <div>Medium15</div> <div>Low11</div> <div>None15</div>	<div>NEW SCAN</div>																					

Observación:

El sistema muestra permisos abusivos (ej. acceso a SMS, cámara, contactos) y conexiones con dominios sospechosos.

Paso 4 – Análisis de APK 2 (Malicioso)

Descripción:

Se repite el proceso con un segundo APK malicioso.

Acciones:

1. Subir BankBot.apk (ejemplo).
2. Ejecutar análisis.
3. Guardar reporte.

Imagen:

Figura 4. Resultados del análisis del APK 2.

2

Spotify X v9.0.64.106

mpolar

spotify crack

ID	Description	Version	Created On	Status	Progress	Findings	By Severity	Delete
2	spotify crack	2147483647	Aug. 21, 2025, 6:38 a.m.	Finished	100 %	3689	<div>Critical64</div> <div>High817</div> <div>Medium2437</div> <div>Low74</div> <div>None297</div>	

Paso 5 – Exportación de Resultados

Descripción:

Los hallazgos pueden exportarse a PDF, CSV o Markdown para anexar al informe.

Acciones:

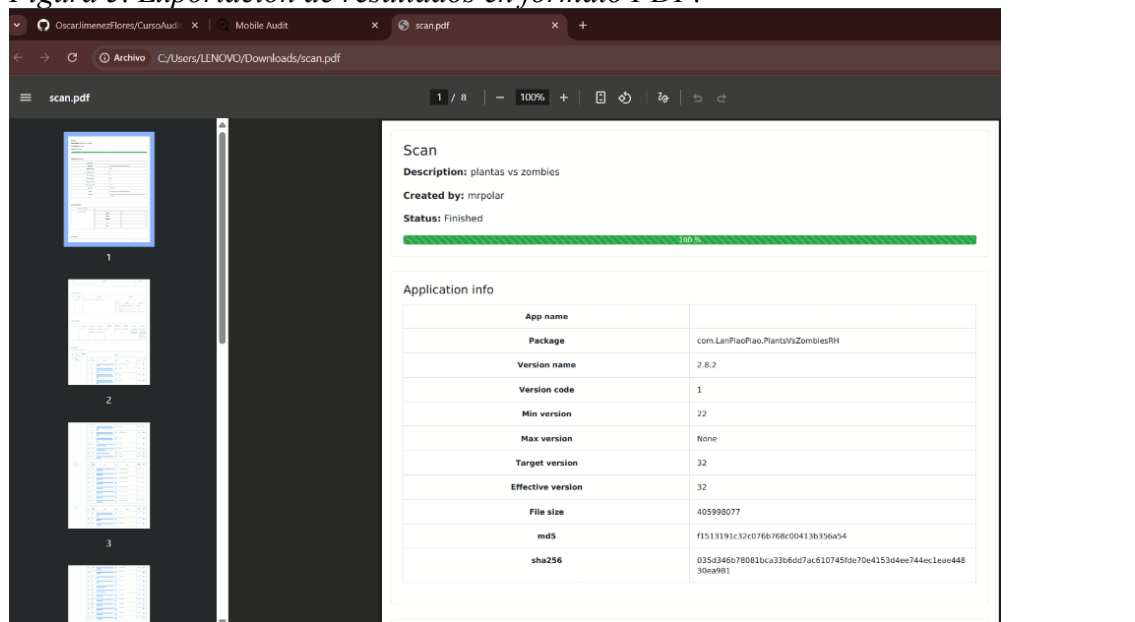
Para detener los servicios al terminar
docker-compose down

URL Github:

<https://github.com/MrPol4r/Lab02-Auditoria.git>

Imagen:

Figura 5. Exportación de resultados en formato PDF.



3. Conclusiones

En base al laboratorio desarrollado, sobre auditoría de seguridad, y particularmente en la extracción de evidencias u obtención de hallazgos, es importante reconocer los riesgos asociados en torno al caso y determinar los controles necesarios para minimizar el riesgo de exfiltrado de documentos privados de la organización.

4. Referencias Bibliográficas

- Calder, A., & Watkins, S. (2015). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page.
- Orebaugh, A., Ramirez, D., Beale, J., & Wright, J. (2006). Wireshark & Ethernet Network Protocol Analyzer Toolkit. Syngress.
- Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.
- Weaver, A. C. (2013). Computer Security: A Hands-on Approach. CRC Press.

AlphaCloud

- Del Peso, E., Del Peso, M., & Piattini, M. (2008). Auditoría de tecnologías y sistemas de información. Rama. ISBN 9788499646039.

5. Actividad

Desarrolla el laboratorio, recaba las evidencias del caso y presenta los resultados en un **informe PDF** con las siguientes características.

- Portada
- Resumen (descripción general de la actividad realizada con su resultado más importante)
- Materiales y métodos (recursos tecnológicos a utilizar y enlaces de descarga si corresponde)
- Resultados (incluye captura de imágenes)
- Conclusiones
- Anexos (opcional)

Rúbrica de evaluación

ESCALA	DESCRIPCIÓN				
[E] Excelente	El criterio evaluado cumple a cabalidad lo esperado				
[A] Aceptable	El criterio evaluado cumple parcialmente lo esperado				
[D] Deficiente	El criterio evaluado no cumple lo esperado				
[N] No desarrollado	El criterio no fue presentado				
CRITERIOS		E	A	D	N
1. Presenta portada y resumen		3	2	1	0
2. Identifica los materiales y métodos a emplear		5	4	2	0
3. Explica los resultados con sus evidencias (anexo)		7	6	3	0
4. Desarrolla coherentemente sus conclusiones		5	3	2	0
Puntajes		20	15	8	0