FUNDAMENTOS DE AUDITORIA INFORMATICA

Información general

- **Materia:** FUNDAMENTOS DE AUDITORIA INFORMATICA
- **Duración del curso:** Inicio 16-01-2025 Fin 01-06-2025
- **Docente:** José Guadalupe Alvarado Ornelas
- **Número de prácticas:** 5 + Proyecto Final

Objetivo general: Comprender las fases de una auditoría informática, identificar los riesgos y controles asociados a los sistemas de información, aplicar metodologías y herramientas de auditoría en escenarios simulados, desarrollar habilidades de análisis crítico y resolución de problemas y elaborar informes de auditoría claros y efectivos.

Introducción al Manual

Este recurso ha sido diseñado para complementar tu aprendizaje teórico, ofreciéndote una guía práctica paso a paso sobre cómo se lleva a cabo una auditoría informática en el mundo real. A través de una serie de ejercicios prácticos, comprenderás los conceptos fundamentales, las metodologías y las herramientas utilizadas por los auditores informáticos para evaluar la seguridad, la eficiencia y la integridad de los sistemas de información.

Cada práctica te sumergirá en un aspecto específico del proceso de auditoría, desde la planificación inicial hasta la presentación de resultados. Te animamos a ser proactivo, investigar más allá de lo que se presenta aquí y discutir tus hallazgos con tus compañeros y profesor.

Práctica 1: Introducción a la Auditoría Informática y su Planeación

Objetivo:

Comprender la importancia de la auditoría informática y sus objetivos, así como iniciar el proceso de planificación de una auditoría.

Fundamento Teórico:

La **auditoría informática** es un proceso sistemático para evaluar la seguridad, el control y la eficacia de los sistemas de información de una organización. Su objetivo principal es asegurar la **confiabilidad, integridad y disponibilidad** de la información, identificando riesgos y proponiendo mejoras. La **planeación** es la primera y crucial etapa, donde se definen el alcance, los objetivos, los recursos y el cronograma de la auditoría.

Actividades:

1. **Investigación y Discusión:**
   - Investiga sobre al menos tres marcos de trabajo o estándares de auditoría informática (ej. COBIT, ISO 27001, ITIL).
   - Discute en grupo: ¿Cuáles son las principales diferencias entre ellos? ¿En qué tipo de organizaciones aplicarías cada uno y por qué?
2. **Definición de Escenario:**
   - Imagina que eres el auditor informático de una empresa ficticia (ej. una startup de desarrollo de software, un banco pequeño, una cadena de supermercados).
   - Describe brevemente la empresa: su tamaño, sector, principales sistemas informáticos (ej. ERP, CRM, sitio web, base de datos de clientes).
3. **Primeros Pasos de Planeación:**
   - Basándote en el escenario anterior, define un **objetivo** claro para tu auditoría informática (ej. "Evaluar la seguridad de la información sensible de los clientes", "Verificar la disponibilidad de los sistemas críticos de la empresa").

- Establece el **alcance** de la auditoría: ¿Qué sistemas, procesos o departamentos serán incluidos? ¿Cuáles no?
- Identifica al menos **tres riesgos potenciales** que podrías encontrar en los sistemas de la empresa ficticia, relacionados con la seguridad, la disponibilidad o la integridad de la información.

Entregables:

- Un breve reporte (1-2 páginas) con la investigación y discusión sobre los marcos de trabajo.
- Una descripción detallada de la empresa ficticia, el objetivo y el alcance de la auditoría.
- Una lista de los tres riesgos potenciales identificados para tu empresa ficticia.

Practica 2: Reconocimiento de la Red (Scanning y Enumeración)

Objetivo General:
Desarrollar habilidades para identificar y mapear los dispositivos, servicios y topología presentes en una red local utilizando herramientas de escaneo y análisis, como parte del proceso de recopilación de información previa a una auditoría o prueba de penetración.

Objetivos Específicos:

- Comprender las fases de reconocimiento pasivo y activo en un entorno de red.
- Utilizar herramientas como Nmap, Netdiscover, y Wireshark para identificar dispositivos, puertos abiertos y servicios activos.
- Elaborar un mapa de red básico con base en los resultados del reconocimiento.

Contexto:
Eres parte del equipo de seguridad informática de una empresa ficticia. Se te ha solicitado realizar una auditoría inicial de la red para identificar los activos conectados y evaluar su exposición.

Requisitos Previos:

- Conocimiento básico de direcciones IP y subredes.
- Familiaridad con comandos de terminal (Linux/Windows).
- Tener acceso a una red local simulada (puede usarse VirtualBox con varias VMs conectadas en red interna).

Herramientas Recomendadas:

- Nmap – Escaneo de puertos y detección de servicios.
- Netdiscover – Descubrimiento de hosts en la red local.
- Wireshark – Captura y análisis de tráfico de red.
- IP Scanner - Fing.
- Escenario en TryHackMe o red virtualizada.

Actividades a Realizar:

1. **Descubrimiento de Hosts (Reconocimiento Pasivo y Activo):**
   - Utiliza Netdiscover o arp-scan para identificar los dispositivos conectados a la red.
   - Ejecuta un ping sweep con Nmap:

nmap -sn 192.168.1.0/24

2. **Identificación de Puertos y Servicios:**
   - Escanea los dispositivos identificados con Nmap para conocer los puertos abiertos y los servicios activos. Ejemplo:

nmap -sS -sV -O 192.168.1.105

   - Documenta servicios como HTTP, FTP, SSH, SMB, etc., encontrados en los dispositivos.

3. **Captura de Tráfico (opcional):**
   - Usa Wireshark para capturar tráfico y analizar paquetes que muestren actividad interesante (ARP, DNS, HTTP, etc.).

4. **Documentación:**
   - Crea un mapa lógico de red (puede hacerse en herramientas como draw.io, Lucidchart, o papel).
   - Llena una tabla como la siguiente:

IP	MAC	Sistema Operativo	Puertos Abiertos	Servicios Identificados
192.168.1.105	00:0C:29:...	Linux 5.x	22, 80	SSH, HTTP

Entrega Esperada:

- **Informe en PDF** con los siguientes elementos:
  - Introducción breve al reconocimiento de red.
  - Herramientas utilizadas y justificación.
  - Capturas de pantalla de los comandos y resultados obtenidos.
  - Tabla de dispositivos identificados.
  - Mapa lógico de red.
  - Conclusiones y recomendaciones básicas.

Criterios de Evaluación:

Criterio	Puntos
Identificación completa de dispositivos	25 pts
Uso adecuado de herramientas	20 pts
Precisión en el análisis de servicios	20 pts
Mapa lógico claro y organizado	15 pts
Presentación del informe y redacción	10 pts
Conclusiones razonadas	10 pts
Total	**100 pts**

Práctica 3: Recopilación de Información y Análisis Preliminar

Objetivo:

Aprender a recopilar información relevante y realizar un análisis inicial para identificar áreas de interés durante la auditoría.

Fundamento Teórico:

La **recopilación de información** es vital para entender el entorno a auditar. Incluye la revisión de documentación (políticas, procedimientos, diagramas de red), entrevistas con personal clave, observación de procesos y el uso de herramientas para escanear y mapear sistemas. El **análisis preliminar** ayuda a refinar el plan de auditoría, enfocándose en los puntos más críticos.

Actividades:

1. **Revisión Documental (Simulada):**
    - Supón que tienes acceso a la siguiente "documentación" de tu empresa ficticia:
        - Una "Política de Contraseñas" muy básica.
        - Un "Diagrama de Red Simplificado" (con servidores, estaciones de trabajo y un router).
        - Un "Procedimiento de Respaldo de Información" genérico.
    - Analiza cada documento y anota al menos dos puntos débiles o áreas de mejora en cada uno desde la perspectiva de la seguridad y el control.
2. **Diseño de Entrevista:**
    - Prepara una lista de 5-7 preguntas clave que le harías a los siguientes perfiles dentro de tu empresa ficticia:
        - Gerente de TI
        - Un usuario final (empleado)
        - Un administrador de bases de datos
    - Las preguntas deben buscar entender cómo se maneja la información, la seguridad y los procedimientos diarios.
3. **Herramientas de Reconocimiento (Teórico/Simulado):**
    - Investiga sobre al menos dos herramientas de "reconocimiento" o "mapeo de red".
    - Describe brevemente qué tipo de información te permitirían obtener y cómo te ayudarían en tu auditoría. No es necesario usarlas, solo comprender su función.

Entregables:

- Un documento con el análisis de los "documentos" simulados, indicando puntos débiles.
- La lista de preguntas diseñadas para las entrevistas.
- Una breve descripción de las herramientas de reconocimiento investigadas y su utilidad en la auditoría.

Práctica 4: Evaluación de Controles y Pruebas de Seguridad

Objetivo:

Aplicar técnicas para evaluar la efectividad de los controles internos y realizar pruebas de seguridad en sistemas de información.

Fundamento Teórico:

Los **controles internos** son las medidas implementadas por la organización para mitigar riesgos. La auditoría verifica si estos controles son adecuados y operan efectivamente. Las **pruebas de seguridad** (ej. pruebas de penetración, análisis de vulnerabilidades) buscan activamente debilidades en los sistemas.

Actividades:

1. **Evaluación de Controles (Checklist):**
    - Crea una lista de verificación (checklist) de 10 puntos para evaluar los controles de acceso lógico en tu empresa ficticia. Considera aspectos como: complejidad de contraseñas, bloqueo de cuentas, políticas de privilegios mínimos, gestión de usuarios, etc.
    - Para cada punto, indica si es un control *preventivo*, *detectivo* o *correctivo*.
2. **Escenario de Prueba de Penetración (Simulado):**
    - Imagina que vas a realizar una prueba de penetración "caja negra" (sin conocimiento previo de la infraestructura interna) sobre el sitio web público de tu empresa ficticia.
    - Describe al menos tres tipos de ataques que intentarías simular (ej. inyección SQL, Cross-Site Scripting (XSS), fuerza bruta en formularios de login).
    - Para cada ataque, explica brevemente qué buscarías y qué impacto tendría si fuera exitoso.
3. **Análisis de Registros (Logs) - Concepto:**
    - Investiga qué son los "logs" o registros de eventos en un sistema operativo o aplicación.
    - Explica cómo un auditor informático podría utilizar los logs para identificar actividades sospechosas o fallos de seguridad. Menciona al menos dos tipos de eventos que buscarías en un log para detectar una anomalía.

Entregables:

- La checklist de evaluación de controles de acceso lógico, incluyendo el tipo de control.
- Una descripción del escenario de prueba de penetración simulado, con los tipos de ataques y sus impactos.
- Una explicación sobre el uso de logs en auditoría y ejemplos de eventos a buscar.

Práctica 5: Análisis de Vulnerabilidades y Gestión de Riesgos

Objetivo:

Identificar vulnerabilidades en sistemas, comprender su impacto y proponer recomendaciones para la gestión de riesgos.

Fundamento Teórico:

Una **vulnerabilidad** es una debilidad en un sistema que podría ser explotada por una amenaza. El **análisis de vulnerabilidades** es el proceso de identificar estas debilidades. La **gestión de riesgos** implica identificar, evaluar y tratar los riesgos para minimizarlos a un nivel aceptable.

Actividades:

1. **Identificación de Vulnerabilidades (Caso Práctico Pequeño):**
    - Lee el siguiente escenario: "Una empresa utiliza un sistema de gestión de documentos que no requiere autenticación fuerte para acceder a archivos internos si se conoce la URL directa del documento."
    - Identifica al menos dos vulnerabilidades presentes en este escenario.
    - Clasifica estas vulnerabilidades (ej. de configuración, de diseño, de desarrollo).
2. **Impacto y Probabilidad (Matriz de Riesgos Simplificada):**
    - Selecciona dos de los riesgos identificados en la Práctica 1 o 3.
    - Para cada riesgo, estima su **probabilidad** de ocurrencia (Baja, Media, Alta) y su **impacto** (Bajo, Medio, Alto) en la organización.
    - Crea una pequeña "matriz de riesgos" (puede ser una tabla simple) donde los clasifiques.
3. **Recomendaciones y Plan de Mitigación:**
    - Para cada una de las dos vulnerabilidades identificadas en el punto 1 de esta práctica, propone al menos dos **recomendaciones** concretas para mitigarlas.
    - Para cada recomendación, indica si es una medida de control *preventiva*, *detectiva* o *correctiva*.

Entregables:

- Análisis de vulnerabilidades del caso práctico, con su clasificación.
- La matriz de riesgos simplificada con la probabilidad e impacto de los riesgos seleccionados.
- Las recomendaciones de mitigación para las vulnerabilidades identificadas, indicando el tipo de control.

Proyecto Final: Auditoría Informática Integral

Objetivo del Proyecto

El objetivo del proyecto final es que los estudiantes apliquen de manera práctica todos los conocimientos adquiridos durante el curso de Auditoría Informática, mediante la realización de una auditoría completa en un entorno real. Esto incluye identificar las vulnerabilidades, evaluar los controles existentes, la planificación, ejecución, análisis de resultados, y presentación de un informe detallado con hallazgos y recomendaciones.

Descripción del Proyecto

Los estudiantes deberán llevar a cabo una auditoría informática integral en una empresa real. El proyecto se dividirá en las siguientes fases:

1. **Planificación de la Auditoría**
   - **Definición del alcance**: Determinar qué áreas de la infraestructura de TI serán auditadas, como redes, sistemas operativos, aplicaciones, bases de datos, y políticas de seguridad.
   - **Identificación de riesgos**: Evaluar los posibles riesgos asociados a las áreas seleccionadas.
   - **Asignación de roles**: Si el proyecto se realiza en equipo, definir los roles y responsabilidades de cada miembro.
   - **Cronograma:** Establecer un cronograma detallado de las actividades a realizar.

2. **Ejecución de la Auditoría**
   - **Recolección de datos**: Utilizar herramientas de auditoría para recopilar información relevante sobre la infraestructura de TI, incluyendo configuraciones de red, políticas de seguridad, control de accesos, y administración de sistemas operativos.
   - **Análisis de vulnerabilidades**: Identificar vulnerabilidades y debilidades en las áreas auditadas, utilizando técnicas de pruebas de penetración, revisión de configuraciones, y análisis de logs.
   - **Evaluación de controles internos**: Revisar la efectividad de los controles internos y su cumplimiento con normativas y estándares relevantes.

3. **Pruebas de Vulnerabilidad:**
   - **Escaneo de vulnerabilidades: Realizar escaneos de vulnerabilidades utilizando herramientas especializadas.**
   - **Pruebas de penetración: Realizar pruebas de penetración para evaluar la resistencia de los sistemas a ataques.**

4. Análisis de Resultados

- **Interpretación de datos**: Analizar los datos recolectados para identificar patrones, anomalías, y áreas de riesgo.
- **Detección de fallos de seguridad**: Priorizar los hallazgos en función de su impacto y probabilidad de ocurrencia.
- **Revisión de cumplimiento normativo**: Verificar que las políticas y procedimientos de la empresa cumplen con las regulaciones y estándares aplicables.

5. Elaboración del Informe de Auditoría

- **Estructura del informe**: El informe debe incluir una introducción, el alcance de la auditoría, los métodos utilizados, los hallazgos identificados, un análisis detallado de los mismos, y recomendaciones.
- **Recomendaciones**: Proponer medidas correctivas para mitigar los riesgos y mejorar la seguridad y eficiencia de la infraestructura de TI.
- **Presentación de hallazgos**: Preparar una presentación para exponer los resultados de la auditoría ante un panel (puede incluir al instructor y otros estudiantes).

6. Presentación Final

- **Presentación del proyecto**: Los estudiantes presentarán y defenderán su informe de auditoría ante el grupo, respondiendo preguntas y justificando sus hallazgos y recomendaciones.
- **Retroalimentación**: El grupo proporcionará comentarios y evaluaciones sobre la calidad del informe, la efectividad de la presentación, y la solidez del análisis.

Criterios de Evaluación

- **Rigor y exhaustividad**: Evaluación de la profundidad y detalle con el que se realizó la auditoría.
- **Relevancia de los hallazgos**: Identificación y análisis de las principales vulnerabilidades y riesgos.
- **Calidad del informe**: Claridad, estructura, y contenido del informe de auditoría.
- **Propuestas de mejora**: Viabilidad y efectividad de las recomendaciones propuestas.
- **Defensa oral**: Habilidad para presentar y defender el proyecto ante el grupo, demostrando comprensión del proceso de auditoría.

Entrega

- **Fecha límite**: Los estudiantes deben entregar el informe final en formato digital una semana antes de la presentación.
- **Formato**: El informe debe estar redactado en un documento estructurado Word y la presentación en PowerPoint u otra herramienta equivalente.

Recursos

- **Herramientas de auditoría**: Se proporcionarán herramientas como Wireshark, Nessus, Nmap, y SQL Server Audit, entre otras.

Consideraciones Adicionales:

- **Ética:** Los estudiantes deben respetar la confidencialidad de la información a la que tengan acceso durante la auditoría.

Este proyecto final permite a los estudiantes integrar y aplicar todos los conocimientos adquiridos, desarrollando habilidades críticas para desempeñarse en el campo de la auditoría informática.