1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad y Virtualización
Clave de la asignatura:	DEB-2203
SATCA[1]:	1-4-5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad de analizar, instalar y administrar software para la virtualización, conociendo los diferentes Riesgos y Amenazas en la red.

Proporciona soporte a otras asignaturas directamente vinculadas con desempeños profesionales; se ubica en el séptimo semestre de la trayectoria escolar, después de la materia de redes de computadoras y a la par de conmutación y enrutamiento de redes de datos, Proporciona al estudiante las competencias necesarias para abordar el estudio de cualquier software de virtualización.
En esta asignatura se inicia desde los conceptos básicos de seguridad en redes, como también los conceptos básicos de virtualización, para después dar paso a la instalación y administración de diferentes aplicaciones virtualizadas; así como el conocimiento y manejo de firewall.

Intención didáctica

La asignatura está organizada en cuatro temas:

El primer tema, se centra en definir los conceptos de seguridad y virtualización, también se conocen el Software de seguridad en la red y en la virtualización como también los Riesgos y Amenazas considerando los aspectos legales, delitos informáticos, el código penal que los rige, así como también la integridad de archivos y auditoria.

El segundo, aborda el trabajo con máquinas virtuales utilizando software para virtualización en diferentes plataformas. Instalando servidores y escritorios virtuales donde se realiza el establecimiento de un Host Físico, Instalación de un Cliente Virtual, Administración de un Cliente Virtual, Monitoreo de Recursos Virtuales, Administración de Usuarios y Escritorios Remotos así como la Exportación e Importación de Máquinas Virtuales.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El tercer tema, tiene como objetivo la seguridad redes a través de la implementación de un Firewall, en el cual se deben de conocer sus componentes y las diferentes arquitecturas que existen. También la configuración de diferentes dispositivos en la red para la seguridad de la misma.

El cuarto tema se presenta las tendencias de la seguridad en tecnologías de las redes de computadoras, así como las cuestiones de auditoria y hacking ético.

La importancia de la asignatura se centra en conocer e implementar distintos mecanismos de seguridad en la red así como de instalar diferentes aplicaciones de virtualización, para lo cual se recomienda generar aplicaciones demostrativas en cada tema visto en clase generando un proyecto integrador poniendo atención en los avances de los estudiantes.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Tlaxiaco Oaxaca, 16 de agosto de 2021.	Nancy Ortiz Mariano Astrid Mildred García Hernández Lucia Sánchez Vásquez Jorge Cruz Pérez	Reunión de integración de asignaturas para la carrera de Ingeniería en Sistemas Computacionales.

4. Competencia(s) a desarrollar

Competencia(s) específica(s)de la asignatura
Competencia Genérica: ✓ Virtualiza, configura y administra sistemas de seguridad para mantener la confiabilidad e integridad de cualquier sistema de información. **Competencias Específicas:** ✓ Comprende los aspectos del software en la red y la virtualización para la seguridad informática. ✓ Identifica los diferentes riesgos y amenazas así como el contexto legal en el cual incurren para la red y la virtualización. ✓ Realiza virtualización de aplicaciones en un equipo de cómputo para lograr aprovechar los recursos del hardware y software. ✓ Instala, administra y exporta plataformas virtuales para lograr que sean más eficientes los recursos de una red de computadoras.

- ✓ Aplica soluciones sobre vulnerabilidades dentro de los sistemas informáticos.

5. Competencias previas

- ✓ Identifica los componentes de un sistema de red.
- ✓ Conoce el protocolo de conexión TCP/IP
- ✓ Utilizar normas y estándares de la industria para diseñar e integrar soluciones de red dentro de las organizaciones.
- ✓ Seleccionar, conocer y usar adecuadamente los diferentes sistemas operativos.
- ✓ Aplicar normas y estándares oficiales vigentes que permitan un correcto diseño de red.
- ✓ Utilizar metodologías para el análisis de requerimientos, planeación, diseño e instalación de una red.

6. Temario

No.	Temas	Subtemas
1	Introducción a la seguridad	1.1.- Conceptos 1.1.1.-Gestión de la información 1.1.2.-Administración de la seguridad 1.2.- Políticas de seguridad. 1.2.1.-Principios de la seguridad. 1.2.2.-Amenazas, ataques y vulnerabilidades. 1.3- Recopilación de la información 1.3.1.-Mecanismos de la seguridad. 1.3.2.-Metodologías de la evaluación de la seguridad. 1.4.- Integridad de archivos y auditoria. 1.4.1- Aspectos legales 1.4.3.- Código penal
2	Servidores y Escritores Virtuales	2.1.- Ambiente virtual 2.1.1.-Arquitectura física 2.1.2.- Trabajo con Máquinas Virtuales. 2.1.3.- Software para virtualización. 2.2.-Mejoras con la virtualización 2.3.-Virtualización del software y Hardware. 2.3.1.-Almacenamiento

		2.3.2.-Redes 2.3.3.-Escritorio 2.3.4.-Aplicaciones 2.4.-Vistualizacion de S.O. 2.4.1- Instalación de un Cliente Virtual 2.4.2.- Administración de un Cliente Virtual 2.4.3.-Monitoreo de Recursos Virtuales 2.4.4.-Administración de Usuarios y Escritorios Remotos. 2.4.5.-Exportación e Importación de Máquinas Virtuales.
3	Seguridad en la LAN	3.1.-Redes de computadoras 3.1.1.-Evaluación de la red 3.2.-Seguridad perimetral 3.2.1.-Configuración de firewall empresarial. 3.2.2.-Monitoreo de la red 3.2.3.-Protección de la red de área local. 3.3.-Seguridad de las aplicaciones web 3.3.1.-Seguridad de los servidores 3.4.-Tipos de respaldo 3.5.-Antivirus y antispam 3.5.1.-Criptografía 3.5.2.-Algoritmo hash 3.5.3.-Firma digital 3.7.-Seguridad en el host
4	Tendencias en seguridad	4.1.-Seguridad de la nube 4.1.1.-Auditoria de los mecanismos de seguridad 4.1.2.-Continuidad del negocio 4.1.3.-Documentación 4.1.4.-Roles y responsabilidades 4.1.5.-Capacitación de usuarios 4.1.6.-Seguridad en dispositivos móviles 4.2.-Hacking ético 4.2.1.-Computo forense 4.2.2.-Inteligencia de amenazas 4.2.3.-Herramientas de hackers

7. Actividades de aprendizaje de los temas

Introducción a la seguridad	
Competencias	Actividades de aprendizaje
Específica(s): ✓ Comprende los aspectos del software en la red para la seguridad informática. ✓ Identifica los diferentes riesgos y amenazas así como el contexto legal en el cual incurren en una red de datos. Genéricas: ✓ Capacidad de análisis y síntesis ✓ Capacidad de organizar información ✓ Comunicación oral y escrita ✓ Habilidad para buscar y analizar información proveniente de fuentes diversas ✓ Trabajo en equipo ✓ Habilidades de investigación ✓ Capacidad de aprender	✓ Investigar los conceptos de seguridad y virtualización. ✓ Definir software de seguridad en la red. ✓ Examinar el diagrama de la Visión Global de la seguridad para conocer los elementos que la conforman. ✓ Investigar los tipos de riesgos ✓ Identificar los riesgos dentro de un sistema informático. ✓ Hacer un cuadro comparativo sobre el pirateo informático. ✓ Diferenciar los tipos del pirateo informático ✓ Distinguir los diferentes delitos informáticos ✓ Elaborar un ensayo sobre los tipos de delitos informáticos ✓ Discutir el código penal en clase de acuerdo a los tipos de delitos informáticos.
Servidores y Escritores Virtuales	
Competencias	Actividades de aprendizaje
Específica(s): ✓ Realiza virtualización de aplicaciones en un equipo de cómputo para lograr aprovechar los recursos del hardware y software. ✓ Instala, administra y exporta plataformas virtuales para lograr que sean más eficientes los recursos de una red de computadoras. Genéricas: ✓ Solución de problemas	✓ Trabajar con máquinas virtuales ✓ Instalar software de virtualización ✓ Trabajar con plataformas para virtualización. ✓ Establecer un Host Físico. ✓ Instalar y administrar un Cliente Virtual. ✓ Monitorear Recursos Virtuales. ✓ Administrar Usuarios y Escritorios Remotos. ✓ Exportar e importar Máquinas Virtuales.

✓ Confidencialidad de la información. ✓ Trabajo en equipo ✓ Habilidades interpersonales ✓ Capacidad de generar nuevas ideas ✓ Habilidad para trabajar en forma autónoma	
Seguridad en la LAN	
Competencias	Actividades de aprendizaje
Específica(s): ✓ Aplica soluciones sobre vulnerabilidades dentro de una LAN. Genéricas: ✓ Capacidad de análisis y síntesis ✓ Capacidad de organizar información ✓ Solución de problemas ✓ Trabajo en equipo ✓ Habilidades interpersonales ✓ Habilidades de investigación ✓ Capacidad de aprender ✓ Habilidad para trabajar en forma ✓ autónoma	✓ Identifica que es un firewall. ✓ Identifica cuales son los componentes y arquitecturas de un firewall. ✓ Elige una arquitectura de firewall en base al cuadro comparativo realizado. ✓ En equipo instala y configura una arquitectura de firewall. ✓ Elabora un reporte acerca del funcionamiento de la arquitectura de firewall. ✓ Investiga la forma de configurar puertos en un switch. ✓ Configuración de puertos en un switch. ✓ Investiga el funcionamiento de un antivirus. ✓ Configura un antivirus en un sistema operativo.
Tendencias en seguridad en TI	
Específica(s): ✓ Utiliza herramientas para realizar auditorías de seguridad. Genéricas: ✓ Capacidad de análisis y síntesis ✓ Capacidad de organizar información ✓ Solución de problemas ✓ Trabajo en equipo ✓ Habilidades interpersonales ✓ Habilidades de investigación ✓ Capacidad de aprender ✓ Habilidad para trabajar en forma autónoma	✓ Investiga los conceptos de seguridad en la nube ✓ Investiga diferentes herramientas para auditoria. ✓ Implementa herramienta de administración de redes para encontrar fallas de seguridad. ✓ Investiga los diferentes tipos de hacking. ✓ Define que es el cómputo forense. ✓ Implementa herramientas de auditoria para observar fallas en la seguridad de un objetivo destino.

8. Práctica(s)

1. Instalar Software de virtualización en un equipo de trabajo
2. Crear una computadora cloud personal
3. Ejecute Linux sobre Windows (o viceversa)
4. Migrar máquinas virtuales desde la línea de comando.
5. Haga una copia de seguridad de un sistema operativo completo
6. Intercepción de mensajes y escaneo de puertos
7. Implementación de un Firewall.
8. Instalar un clúster de máquinas virtuales.
9. Configurar puertos de seguridad en un switch.
10. Utilizar la herramienta wireshark para monitorear una red.
11. Utilizar la herramienta nmap para conocer la información de un host.
12. Utilizar ultrasurf para saltar un servicio de dhcp.
13. Configurar un clúster de alta disponibilidad.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual

se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y especificas a desarrollar.

- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

La evaluación debe ser permanente y continua. Se debe hacer una evaluación diagnóstica, formativa y sumativa. Se debe aplicar la autoevaluación, coevaluación y heteroevaluación.

Se debe generar un portafolio de evidencias, de preferencia en formato digital.

Instrumentos

- ✓ Guía de problemas de programación
- ✓ Examen(teóricos y prácticos)
- ✓ Reportes de prácticas
- ✓ Resúmenes
- ✓ Preguntas guiadas
- ✓ plenaria
- ✓ Cuadro comparativo

Herramientas

- ✓ Rúbrica
- ✓ Lista de cotejo

- ✓ Matriz de valoración
- ✓ Guía de observación

11. Fuentes de información

Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://elibro.net/es/lc/tlaxiaco/titulos/62452

Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://elibro.net/es/lc/tlaxiaco/titulos/40458

Gómez Vieites, Á. (2015). Auditoría de seguridad informática. RA-MA Editorial. https://elibro.net/es/lc/tlaxiaco/titulos/62464

Elizondo Callejas, R. A. (2015). Informática 2. Grupo Editorial Patria. https://elibro.net/es/lc/tlaxiaco/titulos/39507

Chicano Tejada, E. (2015). Gestión de incidentes de seguridad informática (MF0488_3). IC Editorial. https://elibro.net/es/lc/tlaxiaco/titulos/44101

Giménez Albacete, J. F. (2015). Seguridad en equipos informáticos (MF0486_3). IC Editorial. https://elibro.net/es/lc/tlaxiaco/titulos/44137

Sizemore, G. Medd, J. y Dekens, L. (2016). VMware vSphere PowerCLI Reference: Automating vSphere Administration (2nd. ed.). Wiley. https://elibro.net/es/lc/tlaxiaco/titulos/180418

Shackleford, D. (2013). Virtualization Security: Protecting Virtualized Environments. Wiley. https://elibro.net/es/lc/tlaxiaco/titulos/183102

Hosken, M. (2016). VMware Software-Defined Storage: A Design Guide to the Policy-Driven, Software-Defined Storage Era. Wiley. https://elibro.net/es/lc/tlaxiaco/titulos/177229

Ariganello, E. y Barrientos Sevilla, E. (2015). Redes Cisco: guía de estudio para la certificación CCNP Routing y Switching (3a. ed.). RA-MA Editorial. https://elibro.net/es/lc/tlaxiaco/titulos/106474

Soria Guzmán, I., Briones Medina, F., Cabañes Martínez, E., Miranda, A., Serralde Ruiz, J. M., & Wolf, G. (2016). Ética hacker, seguridad y vigilancia.

Grant, Joe (2019). Hackeo Ético: Guia complete para principiantes para aprender y comprender el concepto de hacking ético