MÓDULO DE ESPECIALIDAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

Ciberseguridad Y Redes Empresariales

Módulo de especialidad para el plan ISIC-2010-224 de la carrera de Ingeniería en Sistemas Computacionales, que tiene como objetivo proporcionar las competencias necesarias para que el (la) alumno(a) sea capaz de dar solución a problemas de interconectividad, así como Identificar y proteger los sistemas informáticos de amenazas que los comprometan.

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE JIQUILPAN

NOMBRE DE LA ESPECIALIDAD: **CIBERSEGURIDAD y REDES EMPRESARIALES.**

CLAVE DE LA ESPECIALIDAD: **ISIE-CSR-2024-01**

PARA LA CARRERA: **INGENIERÍA EN SISTEMAS COMPUTACIONALES.**

CLAVE DEL PLAN: **ISIC-2010-224**

FECHA DE INICIO: **ENERO 2024**

VIGENCIA: **3 AÑOS**

Jiquilpan Michoacán, Agosto 2023

ESPECIALIDAD: **CIBERSEGURIDAD Y REDES EMPRESARIALES.**

CLAVE DE LA ESPECIALIDAD: **ISIE-CSR-2024-01**

FECHA DE INICIO: **ENERO 2024**

VIGENCIA: **3 AÑOS**

OBJETIVO:

Al finalizar el módulo el (la) alumno(a) será capaz de dar solución a problemas de interconectividad, así como Identificar y proteger los sistemas informáticos de amenazas que los comprometan.

PERFIL DE LA ESPECIALIDAD:

El Ingeniero(a) en Sistemas Computacionales tendrá la misión de detectar y satisfacer las necesidades organizacionales relacionadas con la interconectividad y el uso de la información, protegiéndola del uso mal intencionado de la misma. Desarrollará la capacidad para recabar y organizar los datos de los procesos necesarios, en base a las tecnologías informáticas para el buen funcionamiento de la organización, en el cumplimiento de sus objetivos.

Tendrá una preparación integral en el campo teórico, práctico, metodológico y de las tecnologías actuales de interconectividad, pentesting y hacking ético, independientemente de la organización; contando con una disposición para el trabajo grupal e interdisciplinario.

Además, el módulo de especialidad ofrece la oportunidad de certificarse en CCNA (Cisco Certified Networking Associate) y/o EJTP (eLearnSecurity Junior Penetration Tester)

ASIGNATURAS DE LA ESPECIALIDAD:

No.	Asignatura	Créditos	Clave
1	Introducción a las redes empresariales y automatización.	2-3-5	CSD-2401
2	Conmutación en redes empresariales.	2-3-5	CSD-2402
3	Redes empresariales y automatización con IoT.	2-3-5	CSD-2403
4	Ciberseguridad y Ethical Hacking.	2-3-5	CSD-2404
5	Ciberseguridad y Pentesting.	2-3-5	CSD-2405

COMPETENCIAS ESPECÍFICAS Y GENÉRICAS DE LAS ASIGNATURAS:

El módulo de especialidad de Ciberseguridad y Redes empresariales, aporta al perfil de egreso las siguientes competencias específicas:

- Analizar las tecnologías básicas de redes con la finalidad de ayudar a desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones.
- Aplicar normas y estándares vigentes, que permitan un correcto diseño de la red.
- Seleccionar los dispositivos óptimos para garantizar el funcionamiento de una red.
- Planificar y direccionar dispositivos en una red LAN/WAN.
- Capacidad para analizar protocolos de enrutamiento identificando las características principales que puedan resolver problemáticas de comunicación entre redes diversas.
- Capacidad para implementar soluciones de enrutamiento en redes LAN y WAN, configurando rutas estáticas y/o protocolos de ruteo dinámicos.
- Seleccionar la configuración de ruteo apropiada de acuerdo a las necesidades de comunicación de las organizaciones.
- Optimizar los recursos de red eligiendo protocolos de ruteo que trabajen con máscaras de subred de longitud variable, e IPv6.
- Configurar un switch para que funcione en una red diseñada para admitir transmisiones de voz, video y datos.
- Configurar las VLAN y enlaces troncales en los switches en una topología de red conmutada.

- Configurar y explicar el VTP en los switches en una red convergente.
- Describir los componentes y la operación básica de las LAN inalámbricas.
- Implementar soluciones de seguridad Informática dentro de entornos locales.
- Planificar entornos híbridos para el cómputo actual.
- Identificar los ataques que se presentan dentro de un entrono de red de datos.
- Conocer las herramientas que se utilizan para la protección de la información.
- Implementar Smart Firewalls como medida de protección informática.
- Analizar el estado de seuridad de un sistema informático en la organización.
- Diseña protocolos de operación para la prevención de delitos cibernéticos.
- Diseña esquemas de seguridad para dispositivos móviles.
- Aplica diferentes alternativas de seguridad para proteger servidores de red.
- Conocimiento de pruebas de penetración de sistemas de información.
- Diseña y desarrolla pruebas de software que permitan evaluar el funcionamiento de una aplicación.
- Conocimiento para proteger la seguridad y privacidad digital.
- Conocimiento para poder realizar un peritaje informático.
- Conocimiento para realizar una informática forense.
- Conocimiento para asegurar dispositivos móviles.
- Diseña estrategias para asegurar servidores de red.
- Diseña estrategias para mantener la seguridad e integridad de los datos en una red.
- Emplear controles que permitan la detección de intrusiones y amenazas de acuerdo con normas y estándares internacionales.

A su vez, este módulo de especialidad aporta las siguientes competencias genéricas al perfil del egresado:

Competencias instrumentales:

- Capacidad de análisis y síntesis.
- Capacidad de organizar y planificar.
- Comunicación oral y escrita.
- Habilidad para buscar y analizar información proveniente de fuentes diversas.

- Solución de problemas.
- Toma de decisiones.
- Habilidades de gestión de información

Competencias interpersonales:

- Capacidad crítica y autocrítica.
- Trabajo en equipo.
- Capacidad de comunicación interdisciplinaria.
- Compromiso ético.
- Habilidades interpersonales.

Competencias sistémicas:

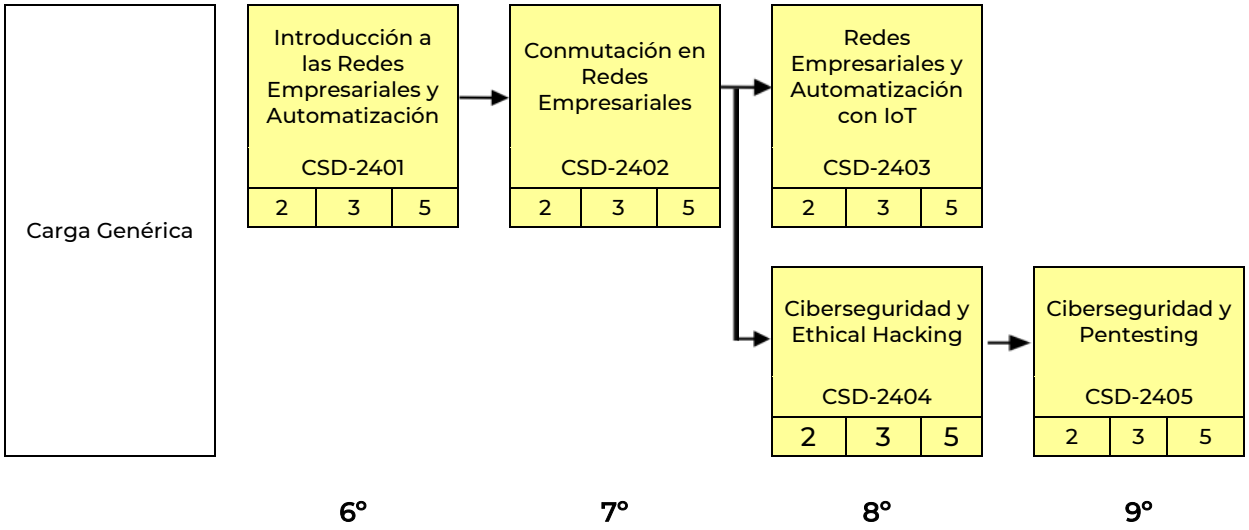
- Capacidad de aplicar los conocimientos en la práctica.
- Habilidades de investigación.
- Capacidad de aprender.
- Capacidad de generar nuevas ideas (creatividad).
- Capacidad de adaptarse a nuevas situaciones.
- Liderazgo.
- Habilidad para trabajar en forma autónoma.
- Búsqueda del logro.
- Capacidad para diseñar y gestionar proyectos.
- Iniciativa y espíritu emprendedor.
- Preocupación por la calidad.
- Conocimiento de culturas y costumbres de diversas organizaciones.
- Habilidad en el uso de Tecnologías de la información y de la comunicación.

CONTENIDOS TEMÁTICOS DE LAS ASIGNATURAS:

Asignatura	Temas
Introducción a las Redes Empresariales y Automatización.	1. Las Redes Hoy. 2. Dispositivos Capa 2 (DCE). 3. Protocolos y Modelos. 4. Direccionamiento IP referencia e IPv6. 5. Capa de Aplicación.
Conmutación, Enrutamiento en Redes Empresariales y PyMEs.	• Configuración y conceptos básicos. • VLAN, Enrutamiento entre VLAN. • Conceptos STP y EtherChannel. • DHCP. • Conceptos y Configuración WLAN • Enrutamiento Estático
Redes Empresariales y Automatización con IOT´s.	1. Introducción al escalamiento de redes. 2. Redes inalámbricas. 3. Conceptos avanzados de protocolos de ruteo. 4. Sistemas operativos de dispositivos de comunicaciones.
Ciberseguridad y Ethical Hacking	1. Ethical Hacking. 2. Criptología. 3. Obtención de Información 4. Ingeniera Social 5. Vulnerabilidades 6. Metasploit
Ciberseguridad y Pentesting	1. Pentesting Wifi 2. Pentesting OWASP 3. SQL, DNS. 4. Ciberpratullaje 5. Estrategias de Ciberdefensa Pymes 6. Certificación

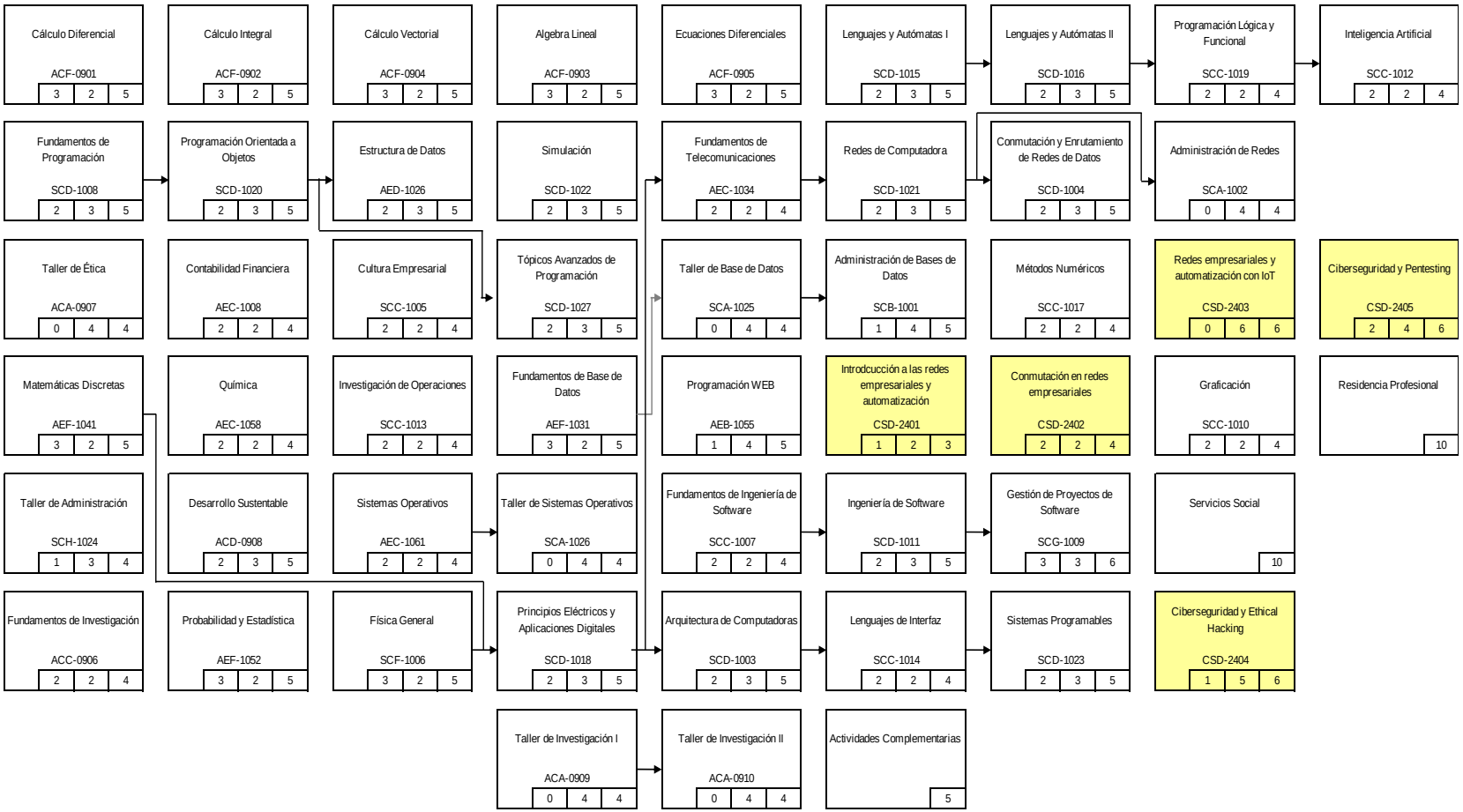
MAPA CURRICULAR DEL MÓDULO:

Las asignaturas del módulo de especialidad se ofrecen a partir del sexto semestre y concluyen en el noveno como se indica a continuación:



Ingeniería en Sistemas Computacionales

ISIC-2010-224



1	2	3	4	5	6	7	8	9
27	28	27	33	31	32	29	34	20

Genéricas	211
Residencias	10
Servicio Social	10
Otros	5
Especialidad	25
Total de Créditos	**261**

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Introducción a las Redes Empresariales y Automatización.**
Clave de la asignatura:	**CSD-2401**
SATCA[1]:	**2-3-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

El programa de la asignatura Introducción a las Redes y Cómputo en la nube utilizando IPv6, está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para:

- Aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área de sistemas computacionales con un enfoque interdisciplinario.
- Aplicar normas, marcos de referencia, estándares de calidad y seguridad vigentes en el ámbito de desarrollo y gestión de tecnologías y sistemas de información.
- Administrar dispositivos de comunicación y configuración de protocolos de red que intervienen en el funcionamiento y desempeño de una red de datos.

Ea Esta materia se centra en el aprendizaje de los aspectos fundamentales de redes. En ella aprenderá las habilidades prácticas y conceptuales que constituyen la base para entender los conceptos básicos. Para la cual, comparará la comunicación humana con la de red y observará las semejanzas. Después, se analizan los tipos de dispositivos de capa 2 su funcionalidad e implementación. Se familiarizará con las Organizaciones de Estándares, modelos de referencia y las bases de capa de red asi como los protocolos de comunicaciones IPv4 e IPv6. Define el direccionamiento de la red dependiendo de los requerimientos del entorno, y por último basado en

la Capa de Aplicación desarrolla una arquitectura en la cual se visualice en conjunto el total de competencias adquiridas. En esta materia, adquirirá experiencia usando las herramientas y utilidades de redes, como simuladores y analizadores de protocolos, para explorar las redes de datos. Estas herramientas lo ayudarán a comprender cómo fluyen los datos en una red, así como los factores que influyen en el desempeño de la misma. Esta materia se incluye dentro del módulo de especialidad para la carrera de Ingeniería en Informática, denominado Redes De Datos, Cómputo en la Nube e Ipv6, debido a que requiere de los conocimientos y habilidades que proporcionan materias tales como Redes de computadora, Conmutación y Enrutamiento de Redes de Datos y Administración de Redes. A su vez esta materia proporciona bases necesarias para la asignatura Conmutación, enrutamiento y redes inalámbricas, complementando los conocimientos necesarios para lograr que la (el) alumna(o) desarrolle competencias efectivas en un ambiente real de comunicaciones basadas en IP.
Intención didáctica
• La (el) estudiante aprenderá de los aspectos básicos de redes. • Aprenderá las habilidades prácticas y conceptuales que constituyen la base para entender lo básico de las redes. • Comparará la comunicación humana con la de red y observará las semejanzas entre ambas. • Recibirá una introducción a los dos modelos principales para planificar e implementar redes: OSI y TCP/IP. • Obtendrá la comprensión del enfoque de capas de las redes. • Examinará las capas OSI y TCP/IP en detalle para comprender sus funciones y servicios. • Se familiarizará con los diversos dispositivos de red y los esquemas de direccionamiento de red tanto en IPv4 e IPv6. • Descubrirá los tipos de medios utilizados para transportar datos a través de la red. • Podrá crear redes LAN simples, realizar configuraciones básicas de switches, e implementar esquemas de direccionamiento IP.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones

Instituto Tecnológico de Jiquilpan. 8 de mayo de 2023	Ing. David Lira Leyva. Lic. José Manuel Padilla Aguilar. Lic. José Odiseo López Calderón Lic. Ricardo Murguia Rivas Ing. Jorge Alberto Rivera Guerra	Reunión de elaboración curricular de las especialidades de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Describir como afectan las redes la forma en que interactuamos, aprendemos, trabajamos y jugamos. • Analizar la forma en que las redes permiten la comunicación, local, cobertura amplia, en la Nube y Nube Hibrida. • Explicar el uso de los dispositivos de red. • Describir el impacto de BYOD (Bring Your Own Device), de la colaboración en línea, del video y de la computación en la nube en una red empresarial. • Describir las características básicas de los métodos de control de acceso al medio en las topologías LAN. • Describir la importancia de la transición de los protocolos IPv4 a Ipv6.

5. Competencias previas

- Conocer el entorno, conceptos básicos y características de las redes, para aplicar medios de transmisión y protocolos.
- Conocer la estructura de la arquitectura del modelo TCP/IP, y OSI como modelo de referencia para redes.
- Aplicar las funciones de las capas del modelo OSI y TCP/IP. Seleccionar y aplicar el uso de herramientas de análisis de red, para examinar la forma en que funcionan las aplicaciones de usuario.
- Seleccionar y manejar los medios Ethernet adecuados en una red de computadoras.

6. Temario

No.	Temas	Subtemas
1	**Las Redes Hoy.**	1.1 Introducción a las redes. 1.2 Las Redes afectan nuestras vidas. 1.3 Conectados globalmente. 1.3.1 Las redes en la actualidad. 1.3.2 Provisión de recursos en una red. 1.4 Tipos comunes de redes. 1.4.1 Componentes de redes. 1.4.2 LAN y WAN. 1.4.3 Internet. 1.4.4 Internets y extranets. 1.5 La red como plataforma. 1.5.1 Redes convergentes. 1.5.2 Red confiable. 1.6 El cambiante entorno de red. 1.6.1 Tendencias de red. 1.6.2 Computación en la nube 1.6.3 Seguridad de red.
2	**Dispositivos Capa 2**	2.1 Intrducción. 2.1.1 Sistema Operativo 2.2 Métodos de Acceso. 2.2.1 Consola. 2.2.2 Ssh. 2.2.3 Telnet. 2.3 Capa Física 2.3.1 Propósito de la Capa Física. 2.3.2 Medios de comunicación. 2.4 Capa de Enalce de Datos 2.4.1 Propósito de la Capa de Enlace. 2.4.2 Topologías. 2.4.3 Marco de Enlace de Datos.
		3.1 Las Reglas. 3.1.1 Protocolos. 3.1.2 Organizaciones de Estándares. 3.1.3 Modelos de Referencia. 3.1.4 Acceso a Datos.

3	**Protocolos y Modelos.**	3.2. Conmutación Ethernet. 3.2.1 Funcionamiento de Ethernet. 3.2.2 Direcciones MAC de Ethernet. 3.2.3 Tabla de Direcciones MAC. 3.2.4 Velocidad de Cambio y reenvío. 3.3 Capa de Red. 3.3.1 Caracterísitcas. 3.3.2 Paquete IPv4. 3.3.3 Paquete IPv6. 3.4 ICMP 3.4.1 Introducción. 3.4.2 Mensajes ICMP. 3.6 Capa de Transporte. 3.6.1 Transporte de Datos. 3.6.2 Descripción TCP/UDP. 3.6.3
4	**Direccionamiento IP IPv4-IPv6**	4.1 Direccionamiento IPv4. 4.1.1 Estructura de Direcciones. 4.1.2 IPv4 Unicast, Broadcast y Multicast. 4.1.3 Tipos de direcciones IPv4. 4.1.4 Subredes. 4.1.5 VLSM. 4.3 Direccionamiento IPv6. 4.3.1 Problemas de IPv4. 4.3.2 Representación. 4.3.3 Tipos de direcciones IPv6. 4.3.4 Subred una red IPv6.
5	**Capa de Aplicación**	5.1 Introducción. 5.2 Solicitud, presentación y sesión. 5.3 Servicios de direccionamiento IPv4 e IPv6. 5.4 Servicios para compartir archivos usando IPv4 e IPv6.

7. Actividades de aprendizaje de los temas

Unidad I Las Redes Hoy.	
Competencias	Actividades de aprendizaje
Específica(s):	

La (el) estudiante comparará la comunicación humana con la de red y observará las semejanzas entre ambas. Se familiarizará con los diversos dispositivos de red y los esquemas de direccionamiento de red IPv4 e IPv6. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de análisis, síntesis y abstracción. • Capacidad de trabajo en equipo.	• Investigar de forma individual y analizar de manera grupal los conceptos básicos de las redes y características en diferentes fuentes de información confiables, y presentar los resultados en una plenaria. • Presentación en clase, debates y práctica con su instructor • Realizar prácticas de laboratorio que usan equipos de redes, dentro del aula de networking. • Evaluación mediante software de simulación (Packet Tracer), posteriormente presentar problemas reales para la solución en equipos físicos. • Plantear problemáticas empresariales al grupo para su estudio y solución.
Unidad II Dispositivos Capa 2.	
Competencias	Actividades de aprendizaje
Específica(s): Explicar los diferentes dispositivos de Capa 2 su comportamiento, maneras de administración, tipos de medios para interconexión entre dichos dispositivos y los IOS de cada dispositivo. Genéricas: • Capacidad de comunicación oral y escrita.	• Investigar de forma individual los tipos de dispositivos capa 2 y sus formas de trabajar o como tratan la información que les llega de capa 3 y capa 1. • Realizar prácticas de laboratorio para conocer los diferentes medios de

• Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de análisis, síntesis y abstracción. • Capacidad de trabajo en equipo.	comunicación entre dispositivos. • Investigar y discutir en grupo las diferencias entre los tipos de dispositivos capa 2 y los IOS. • Realizar una interconexión y analizar el comportamiento de las comunicaciones utilizando el protocolo IPv4/IPv6. • Analizar las ofertas del mercado que ofrecen el cómputo en la Nube y visualizar en que situaciones se puede aplicar. • Investigar la funcionalidad y comportamiento de la Nube Hibrida.
Unidad III Protocolos y Modelos.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer las Organizaciones que rigen la parte de los estándares, ubicar los Modelos de Referencia para las comunicaciones y como se logra la interacción entre dispositivos y EndUser. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación.	• Realizar de manera individual mapas mentales que muestren las Organizaciones y sus Estandáres. • Investigar de manera individual la conmutación Ethernet y realizar una presentación ante el grupo. • Configurar una red LAN, para visualizar el comportamiento de conmutación Ethernet, utilizando como protocolo de comunicaciones IPv4/IPv6.

• Capacidad de análisis, síntesis y abstracción. • Capacidad de trabajo en equipo.	• Evaluación mediante software de simulación. (Packet Tracer). • Plantear problemáticas empresariales al grupo para su estudio y solución.
Unidad IV Direccionamiento IPv4-IPv6	
Competencias	Actividades de aprendizaje
Específica(s): Describir la estructura de una dirección IPv4 e IPv6, el propósito de la máscara de subred y el prefijo de red. Comparar las características y los usos de las direcciones IPv4 unicast, broadcast y multicast. Explicar la necesidad de direccionamiento IPv6, tipos de direcciones IPv6 y representación de una dirección IPv6. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de análisis, síntesis y abstracción. • Capacidad de trabajo en equipo.	• Investigar y discutir en grupo las diferencias entre IPV4 e IPV6. • Determinar la porción de red de la dirección de host y explicar la función de la máscara de subred/ el prefijo de red en IPv4/IPv6. • Calcular los componentes de direccionamiento adecuados de acuerdo con la información de la dirección IPv4 e IPv6 y los criterios de diseño. • Realizar prácticas de laboratorio que usan equipos de redes, dentro del aula de networking. • Evaluación mediante software de simulación (Packet Tracer). • Plantear problemáticas empresariales al grupo para su estudio y solución.
Unidad V Capa de Aplicación	

Competencias	Actividades de aprendizaje
Específica(s): Explicar la forma en que las funciones de la capa de aplicación, de la capa de sesión y de la capa de presentación operan conjuntamente para proporcionar servicios de red a las aplicaciones de usuario final. Describir los protocolos de la capa de aplicación comunes que proporcionan servicios de Internet a usuarios finales. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de análisis, síntesis y abstracción. • Capacidad de trabajo en equipo.	• Investigar los protocolos de capa de aplicación que proporcionan servicios de direccionamiento IP, incluso: DNS y DHCP, para IPv4/IPv6. • Analizar la forma en que los datos se transfieren a través de la red, desde que se abre una aplicación hasta que se reciben los datos, en IPv4/IPv6. • Utilizar los comandos show básicos para verificar la configuración y el estado de una interfaz de los dispositivos.

8. Práctica(s)

1. **Investigación de oportunidades laborales de TI y redes.**

En esta práctica de laboratorio, realizará cierta búsqueda laboral orientada en la Web, para descubrir qué tipos de empleos relacionados con TI y redes de computadoras se encuentran disponibles, qué tipo de aptitudes y certificaciones necesitará y las escalas salariales asociadas con los diversos puestos.

2. **Establecimiento de una sesión de consola con dispositivos de capa 2.**

Aprenderá cómo acceder a un dispositivo Capa 2, a través de una conexión local directa al puerto de consola mediante un programa de emulación de

terminal. También aprenderá a configurar los parámetros del puerto serie para la conexión de consola de Tera Term.

3. **Investigación de estándares de redes.**

Con la ayuda de motores de búsqueda como Google, investigue las organizaciones sin fines de lucro que son responsables de establecer estándares internacionales para Internet y el desarrollo de tecnologías de Internet.

4. **Identificación de dispositivos y cableado de red**

Como parte del personal de soporte de red, debe poder identificar distintos equipos de red. También debe comprender la función de los equipos en la parte apropiada de la red. En esta práctica de laboratorio, tendrá acceso a dispositivos y a medios de red. Identificará el tipo y las características de los equipos y los medios de red, utilizar un protocolo de comunicaciones para probar las comunicaciones entre usuarios finales.

5. **Observación del protocolo ARP mediante la CLI de Windows, la CLI del IOS y Wireshark.**

En esta práctica de laboratorio, utilizará los comandos ARP tanto en los routers Windows como Cisco para visualizar la tabla ARP. También borrará la caché ARP y agregará entradas ARP estáticas.

6. **Visualización de tablas de enrutamiento de host.**

La o el estudiante mostrará y examinará la información en la tabla de enrutamiento de host de la PC utilizando los comandos netstat –r y route print. Asimismo, determinará la forma en que la PC enrutará paquetes según la dirección de destino.

7. **Identificación de direcciones IPv4.**

El direccionamiento es una función importante de los protocolos de la capa de red, porque permite la comunicación de datos entre hosts en la misma red o en redes diferentes. En esta práctica de laboratorio, examinará la estructura de las direcciones del protocolo de Internet versión 4 (IPv4). Identificará los diversos tipos de direcciones IPv4 y los componentes que ayudan a formar la dirección, como la porción de red, la porción de host y la máscara de subred.

8. **Identificación de direcciones IPv6.**

Esta práctica se centra en las direcciones IPv6 y los componentes de la dirección. En la parte 1, identificará los tipos de direcciones IPv6 y, en la parte 2, verá las configuraciones de IPv6 en una PC. En la parte 3, practicará la abreviatura de direcciones IPv6 y, en la parte 4, identificará las partes del prefijo de red IPv6 haciendo foco en las direcciones unicast globales.

9. **Analizar las opciones del cómputo en la Nube.**

Esta práctica se centra en conocer que es el cómputo en la Nube, analizar la pertinencia de su implementación dentro del entorno de las corporaciones, identificar la tecnología de Nube Hibrida, y la pertinencia de su implementación.

9. Proyecto de asignatura

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

Fundamentación:

La asignatura está fundamentada en la aplicación de los estándares vigentes para el diseño de una red LAN/WAN, cómputo en la Nube y Nube Hibrida con respecto al análisis y selección de dispositivos, la planificación de la instalación y direccionamiento de los mismos. El docente propondrá en clase junto con las y los alumnos los proyectos factibles a desarrollar. Estos pueden establecerse de acuerdo a empresas o instituciones que existen en el entorno, como son el diseño de una red LAN/WAN para un hospital, institución educativa, productora de calzado, fábricas de productos manufacturados, hoteles, etc.

Planeación:

El desarrollo del proyecto puede planearse en función de la realización de las siguientes actividades: la recopilación de los requerimientos de interconexión, el diseño de la propuesta de interconexión considerando y aplicando las tecnologías vigentes, haciendo énfasis en los elementos de la red a utilizar, la función que estos desempeñan; la siguiente actividad es el direccionamiento de los dispositivos empleando los direccionamiento de red más adecuados (IPV4 e IPV6). Finalmente la (el) alumna(o) realizará e instalará en forma de prototipo su propuesta. En esta parte la (el) alumna(o) elaborará un plan de acción y tiempos para elaborar el proyecto.

Ejecución:
Para la realización del proyecto, éste se podrá realizar en forma individual o grupal según lo determine el docente. El trabajar en equipo fomenta en la (el) alumna(o) las competencias interpersonales. Para el desarrollo la (el) alumna(o) trabajará en coordinación con el docente mostrando los avances de su trabajo según lo planeado. El docente prestará atención a la (al) alumna(o) en el avance que este muestre de su proyecto y asesorará según lo requiera la (el) alumna(o) o el grupo. Para esto la (el) alumna(o) trabajará con herramientas de software para el diseño de la red, Simulador de redes.

Evaluación:
Los criterios para la evaluación del proyecto que se proponen son:
Trabajo en equipo e individual: 10%
Entrega en tiempo y forma de los avances 10%
La propuesta tendrá un valor 10%
Diseño e implantación virtual 30%
Implantación física 30%
Exposición de las propuesta 10%

10. Evaluación por competencias

- Reportes de trabajos de investigación.
- Reportes de prácticas.
- Exámenes prácticos y escritos.
- Ensayos sobre los diferentes temas de la asignatura.
- Evidencias de participación individual y grupal.
- Proyecto integrador final.
- Presentación del proyecto.

11. Fuentes de información

Allan;Lorenz Reid (Jim;Schmidt, Cheryl.). (2019). Introducción al enrutamiento y la conmutación en la empresa. Pearson Education.

Odom, W. (2013). *Cisco CCNA Routing Switching 200-120 Official Cert Guide Library*. Indianapolis: Pearson Education.
Odom, W. (2014). *Cisco CCNA Routing and Switching 200-120 Official Cert Simulator Library*. Indianapolis: Pearson Education.
Rivard, E. (2014). *Cisco CCNA Routing and Switching 200-120 Flash Cards and Exam Practice Pack*. Indianapolis, Indiana: Pearson Education.
Sequera, A., & Tiso, J. (2014). *Cisco CCNA Routing and Switching 200-120 Foundation Learning Guide Library*. Indianapolis, Indiana: Pearson Education.

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Conmutación en Redes Empresariales.**
Clave de la asignatura:	**CSD-2402**
SATCA[2]:	**2-3-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura
Esta asignatura ha sido creada en base a la necesidad de formar profesionistas altamente capacitados para diseñar e implementar soluciones avanzadas en redes de datos para cualquier tamaño de organización. Esta asignatura aporta al perfil del Ingeniero en Informática las capacidades básicas para el diseño, implementación y administración de redes de datos LAN y WLAN. La importancia de esta asignatura radica en la necesidad que tienen las organizaciones de optimizar sus procesos empleando redes de datos. El objetivo es desarrollar un conocimiento ligado a la manera en que un conmutador, un ruteador y los dispositivos inalámbricos soportan las tareas cotidianas en las organizaciones. De tal manera, el profesionista será capaz de aprovechar las tecnologías de información, así como administrar los dispositivos de red que soportan dichas tecnologías.
Intención didáctica
El temario de esta asignatura se organiza en seis unidades. • En la primera unidad se verá la configuración de dispositivos utilizando las mejores prácticas de seguridad, configurar los ajustes iniciales en un conmutador Cisco y configurar los ajustes básicos en un enrutador para enrutar entre dos redes conectadas directamente, usando CLI.

[2] Sistema de Asignación y Transferencia de Créditos Académicos

• En la segunda unidad se implementarán VLAN y enlaces troncales en una red conmutada. Se explicará el propósito de las VLAN en una red conmutada y como un conmutador reenvía tramas basadas en la configuración de VLAN en un entorno de conmutadores múltiples.

• En la tercera unidad se estudiarán los conceptos básicos de STP. Explicar como STP permite la redundancia en una red de capa 2, Explicar cómo opera STP en una red conmutada simple y como funciona Rapid PVST +.
Solucionar problemas de EtherChannel en enlaces conmutados

• En la cuarta unidad se implementará DHCPv4 para operar múltiples LAN y explicar cómo opera DHCPv4 en una red de pequeñas y medianas empresas.
Configurar la asignación dinámica de direcciones de redes IPv6 y explicar como un host IPv6 puede adquirir su configuración IPv6.

• En la unidad cinco se analizarán los conceptos de WLAN, explicar cómo las WLAN permiten la conectividad de red. Explicar cómo WLC usa CAPWAP para administrar múltiples AP. Y describir las amenazas y mecanismos de seguridad de WLAN.

Y por último la unidad seis se explicará cómo los enrutadores usan la información en paquetes para tomar decisiones de reenvío, configurar los ajustes básicos en un enrutador. Explicar cómo los enrutadores determinan la mejor ruta y reenvían paquetes al destino. Comparar los conceptos de enrutamiento estático y dinámico.

En el transcurso de las actividades programadas es muy importante que la o el estudiante aprenda a valorar las actividades que lleva a cabo y entienda que está construyendo su desempeño profesional y actúe acorde a ello; de igual manera, aprecie la importancia del conocimiento y los hábitos de trabajo; desarrolle la precisión y la curiosidad, la puntualidad, el entusiasmo y el interés, la tenacidad, la flexibilidad, la autonomía y el trabajo en equipo.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Jiquilpan. 8 de mayo de 2023	Ing. David Lira Leyva. Lic. José Manuel Padilla Aguilar. Lic. José Odiseo López Calderón Lic. Ricardo Murguia Rivas Ing. Jorge Alberto Rivera Guerra	Reunión de elaboración curricular de las especialidades de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Analizar las tecnologías básicas de redes con la finalidad de ayudar a desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones. • Aplicar normas y estándares vigentes, que permitan un correcto diseño de la red. • Seleccionar los dispositivos óptimos para garantizar el funcionamiento de una red. • Planificar y direccionar dispositivos en una red WLAN. • Desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones utilizando un simulador de redes, así como el laboratorio de redes. • El objetivo de este curso es presentar los conceptos y tecnologías básicos de red. El curso ayudará a la (al) alumna(o) a configurar la funcionalidad avanzada en enrutadores y conmutadores. También podrá realizar la solución básica de problemas de estos componentes. Con las mejores prácticas de seguridad, solucionará y resolverá problemas comunes de protocolo en redes IPv4 e IPv6.

5. Competencias previas

- Explicar la forma en que las redes afectan nuestra vida diaria.
- Explicarla forma en que se utilizan los dispositivos host y de red.
- Comparar las características de los tipos comunes de redes.
- Identifique algunas amenazas y soluciones de seguridad básicas para todas las redes.
- Explique la forma en que las tendencias, como BYOD, la colaboración en línea, la comunicación de video y la computación en la nube, están cambiando el modo en que interactuamos

6.Temario

No.	Temas	Subtemas
1	Configuración y conceptos básicos.	1.1 Introducción. 1.2 Configuración básica de un conmutador. 1.3 Configuración básica de un enrutador. 1.4 Dominios de switching. 1.4.1 Dominios de colisiones. 1.4.2 Dominios de broadcast.
2	VLAN, Enrutamiento entre VLAN.	2.1 Introducción a las VLANs 2.2 Reenvio de Tramas. 2.2.1 Cambio de Dominios 2.2.2 Descripción general de VLAN 2.2.3 VLAN nativas y etiquetado de 802.1Q 2.3 Configuración de VLAN 2.3.1 Protocolo de enlace troncal dinámico. 2.3.2 VLAN de voz. 2.4 Operación de enrutamiento entre VLAN. 2.5 Enrutamiento Inter-VLAN y Router-on-a-Stick. 2.6 Enrutamiento entre VLAN utilizando conmutadores capa 3

3	Conceptos STP y EtherChannel.	3.1 Introducción a STP. 3.1.1 Proposito de STP. 3.1.2 Operaciones de STP. 3.1.3 Evolución de STP. 3.2 Introducción EtherChannel. 3.2.1 Proposito de EtherChannel. 3.2.2 Operación de EtherChannel. 3.2.3 Configuración de EtherChannel. 3.3 Verificar y Solucionar Problemas de STP. 3.4 Verificar y Solucionar Problemas de EtherChannel.
4	DHCP.	4.1 Introducción al DHCP. 4.2 Configuración de DHCPv4. 4.2.1 Verificar operación del servidor DHCP en el IOS. 4.3 SLAAC y DHCPv6. 4.3.1 Asignación de GUA IPv6. 4.3.2 SLAAC. 4.3.3 DHCPv6. 4.3.4 Configuración del Servidor DHCPv6.
5	Conceptos y Configuración WLAN.	5.1 Introducción a la Tecnología Inalámbrica (WLAN). 5.1.1 Componentes de WLAN. 5.1.2 Operación de WLAN. 5.1.3 Operación CAPWAP. 5.2 Configuración de WLAN. 5.2.1 WLAN de sitio Remoto. 5.2.2 Entorno WLC. 5.2.3 Configuración de un entorno WLC.
6	Enrutamiento Estático	.1 Introducción 6.1.1 Determinar la Ruta. 6.1.2 Reenvío de paquetes. 6.1.3 Tabla de Enrutamiento. 6.2 Enrutamiento Estatico 6.2.1 Rutas Estáticas. 6.2.2 Configurar rutas estáticas predeterminadas.

		6.2.3 Configurar rutas estaticas flotantes.

7. Actividades de aprendizaje de los temas

Unidad I. Configuración y conceptos básicos.	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) comprenderá la forma en que se transmite la información en una red conmutada; aprenderá a configurar y solucionar problemas de comunicación en redes LAN. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de trabajo en equipo.	• Describir la convergencia de datos, voz y video en el contexto de las redes conmutadas. • Identificar la terminología de las redes conmutadas. • Identificar los métodos de reenvió de tramas. • Describa la función de la transmisión de unidifusión, difusión y multidifusión en una red conmutada. • Identificar los ataques de seguridad • Verificar la configuración de capa 2 de un puerto de switch conectado a una estación terminal.
Unidad II. VLAN, enrutamiento entre VLAN	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) aprenderá a segmentar la LAN utilizando VLANs, configurando características de seguridad y protocolos, además será capaz de solucionar problemas de enrutamiento entre VLAN en dispositivos de capa 3. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita.	• Explicar la finalidad de las VLAN en una red conmutada. • Investigar el proceso de implementación de una VLAN. • Configuración de redes VLAN. • Configuración de enlaces troncales. • Resolución de problemas de implementación de

• Habilidad en el uso de tecnologías de información y comunicación. • Capacidad de generar nuevas ideas.	VLAN (utilizando simulador de redes). • Resolución de problemas de implementación de VLAN (laboratorio de redes). • implementación de seguridad de VLAN. • Identificar los tipos de routing entre VLAN. • Configuración de routing entre VLAN con router-on-a-stick
Unidad III. Conceptos STP y EtherChannel	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) aprenderá a administrar varias rutas para que no se produzcan bucles de capa 2. Genéricas: • Habilidades de investigación. • Capacidad de aplicar los conocimientos en la práctica. • Reto de habilidades de integración. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad de aprender • Capacidad de generar nuevas ideas (creatividad).	• Analizar los protocolos utilizados para administrar formas de redundancia • Utilizar Internet para investigar STP • Explicar el propósito del protocolo STP. • Explicar el funcionamiento de la agregación de enlaces en un entorno de LAN conmutada
Unidad IV. DHCP.	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) será capaz de administrar el direccionamiento IP utilizando DHCPv4. Y DHCPv6	• Identificar los pasos del funcionamiento de DHCPv4

Genéricas: • Habilidades de investigación. • Capacidad de aplicar los conocimientos en la práctica. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas • Capacidad de generar nuevas ideas (creatividad).	• Configuración de DHCPv4 mediante el IOS de cisco. • Identificar los pasos del funcionamiento de DHCPv6.
Unidad V Conceptos y configuración WLAN	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) será capaz de Identificar y describir los componentes necesarios para la operación de una WLAN y realizar su configuración básica. Genéricas: • Habilidades de investigación. • Capacidad de aplicar los conocimientos en la práctica. • Reto de habilidades de integración. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Capacidad de aprender. • Capacidad de generar nuevas ideas (creatividad).	• Describir los estándares 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac • Realizar un modelo a escala que incluya los componentes de una estructura inalámbrica para describir sus funciones y la manera en la que se interrelacionan. • Realizar prácticas de laboratorio de configuración básica de una red inalámbrica

Unidad VI Enrutamiento Estatico	
Competencias	Actividades de aprendizaje
Específica(s): La (el) alumna(o) aprenderá a configurar el enrutamiento estático y solucionar problemas de enrutamiento en la red. Genéricas: • Habilidades de investigación. • Capacidad de aplicar los conocimientos en la práctica. • Reto de habilidades de integración. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad de aprender • Capacidad de generar nuevas ideas (creatividad).	• Identificar las ventajas y desventajas de enrutamiento estático. • Identificar el tipo de ruta estática. • Configuración de rutas estáticas y predeterminadas IPv4. • Diseño e implementación de un esquema de direccionamiento VLSM. • Determinar la dirección y el prefijo de red resumida. • Configuración de la sumarización de ruta IPv4. • Cálculo y configuración de la sumarización de ruta IPv6. • Configuración de una ruta estática flotante. • Resolución de problemas de rutas estáticas. • Resolución de problemas de sumarización de ruta y VLSM.

8. Práctica(s)

1. **Configuración del enrutador básico.** Cableará el equipo y completará las configuraciones básicas y la configuración de la interfaz IPv4 en el enrutador. Luego usará SSH para conectarse al enrutador de forma remota y utilizará los comandos IOS para recuperar información del dispositivo para responder preguntas sobre el enrutador. 2. **Implemente VLAN y enlaces troncales en un switch.** Construya la red y configure los ajustes básicos del dispositivo Crear VLAN y asignar puertos de conmutador

Configure un enlace troncal 802.1Q entre los conmutadores

3. **Configuración de VLANs.**

En esta actividad, hay dos switches completamente configurados. Usted es responsable de asignar el direccionamiento IP a una interfaz virtual de switch, configurar las VLAN, asignar las VLAN a las interfaces, configurar enlaces troncales e implementar medidas de seguridad básicas en un tercer switch.

4. **Ruteo entre VLANs.**

En esta actividad, demostrará y reforzará su capacidad para implementar el enrutamiento entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces.

5. **Ruteo entre VLANs y rutas estáticas.**

En esta actividad, demostrará y reforzará su habilidad para configurar ruteadores destinados a la comunicación entre VLAN, al igual que rutas estáticas para llegar a destinos fuera de su red.

6. **Implementar EtherChannel**

Se le ha asignado la tarea de diseñar una implementación EtherChannel para una empresa que desea mejorar el rendimiento de los enlaces troncales del conmutador. Intentará varias formas diferentes de implementar los enlaces EtherChannel para evaluar cuál es el mejor para la empresa. Construirá la topología, configurará puertos troncales e implementará LACP y PAgP EtherChannels.

7. **Implementar DHCPv4**

Como técnico de red de su empresa, tiene la tarea de configurar un enrutador Cisco como un servidor DHCP para proporcionar una asignación dinámica de direcciones a los clientes en la red. También debe configurar el enrutador perimetral como cliente DHCP para que reciba una dirección IP de la red ISP. Debido a que el servidor está centralizado, deberá configurar los dos enrutadores LAN para retransmitir el tráfico DHCP entre las LAN y el enrutador que sirve como servidor DHCP.

8. **Configurar DHCPv6.**

En este laboratorio, completará los siguientes objetivos:
Parte 1: construir la red y configurar los ajustes básicos del dispositivo
Parte 2: Verificar la asignación de dirección SLAAC desde R1
Parte 3: configurar y verificar un servidor DHCPv6 sin estado en R1
Parte 4: configurar y verificar un servidor DHCPv6 con estado en R1

Parte 5: configurar y verificar un relé DHCPv6 en R2

9. **Configuración de seguridad del conmutador**

En este laboratorio, usted:
Asegure los puertos no utilizados
Implementar seguridad portuaria
Mitigar los ataques de salto de VLAN
Mitigar los ataques de DHCP
Mitigar los ataques ARP
Mitigar los ataques STP
Verifique la configuración de seguridad del conmutador

10. **Configuración de WLAN**

En esta actividad, configurará un enrutador doméstico inalámbrico y una red basada en WLC. Implementará tanto la seguridad WPA2-PSK como la WPA2-Enterprise.

11. **Configure rutas IPv4 e IPv6 estáticas y predeterminadas**

En esta actividad de resumen de Packet Tracer, configurará rutas estáticas, predeterminadas y flotantes para los protocolos IPv4 e IPv6

9. Proyecto de asignatura

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

Fundamento:
El constante uso de la tecnología para resolver la problemática de comunicación en las organizaciones, busca mantener una conectividad constante en sus redes de datos. La optimización de recursos de red, así como la rápida convergencia entre ruteadores, coloca a las organizaciones en un alto nivel de competitividad a nivel nacional y/o internacional.
En base al conocimiento y habilidades adquiridas, podrán resolverse problemáticas de interconectividad de redes, como puede ser una necesidad en una escuela, alguna empresa de servicios financieros, empresas de manufactura, etc.

Planeación:
El proyecto a realizar deberá integrar fases de análisis de áreas, requerimientos de visibilidad de información, requerimientos de seguridad, identificación de grupos y subredes. Posteriormente se planteará la fase de diseño de la red, con diferentes alternativas como propuestas.

Desarrollo:
El docente organizará los grupos que desarrollarán las propuestas de configuración de la red, las y los alumnos trabajarán en equipo para identificar las necesidades, analizar los requerimientos, realizar la propuesta de comunicación, diseñar virtualmente la solución e implantar una solución física.
Las y Los alumnos serán capaces de determinar la cantidad de subredes necesarias, la cantidad de direcciones IP por cada subred, diseñando el esquema de direccionamiento adecuado utilizando VLSM. La (el) alumna(o) será capaz de determinar el protocolo de enrutamiento más adecuado para la problemática que le sea presentada, de acuerdo a las necesidades de comunicación, seguridad y de visibilidad de información dentro de la empresa.
Considerando un identificador de red IPv4 (de una red privada preferentemente), la (el) alumna(o) deberá hacer una correcta administración de red y subredes basándose en VLSM. Se pueden tener "N" subredes y "M" direcciones IP por subred. La interconectividad deberá lograrse entre todos los nodos que integran las subredes, configurando los diferentes ruteadores de acuerdo al número de subredes elegidas. Este proyecto deberá realizarse con un simulador de redes e instalar la configuración en el laboratorio de redes.

Evaluación:
Los criterios para la evaluación del proyecto que se proponen son:
Trabajo en equipo e individual: 20%
La propuesta tendrá un valor 20%
Diseño e implantación virtual 30%
Implantación física 30%

10. Evaluación por competencias

- Reportes de trabajos de investigación.
- Reportes de prácticas.
- Exámenes prácticos y escritos.
- Ensayos sobre los diferentes temas de la asignatura.
- Evidencias de participación individual y grupal.
- Proyecto integrador final.
- Presentación del proyecto.

11. Fuentes de información

Odom, W. (2013). *Cisco CCNA Routing Switching 200-120 Official Cert Guide Library*. Indianapolis: Pearson Education.
Odom, W. (2014). *Cisco CCNA Routing and Switching 200-120 Official Cert Simulator Library*. Indianapolis: Pearson Education.
Rivard, E. (2014). *Cisco CCNA Routing and Switching 200-120 Flash Cards and Exam Practice Pack*. Indianapolis, Indiana: Pearson Education.
Sequera, A., & Tiso, J. (2014). *Cisco CCNA Routing and Switching 200-120 Foundation Learning Guide Library*. Indianapolis, Indiana: Pearson Education.

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Redes Empresariales y Automatización.**
Clave de la asignatura:	**CSD-2403**
SATCA[3]:	**2-3-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura
Para integrar los elementos que conforman el plan de estudios de esta asignatura, se considera la importancia del área de telecomunicaciones que actualmente está teniendo en todas las áreas de nuestro entorno. Realizando el análisis de los aspectos que se deben considerar para establecer una comunicación y administración adecuada entre los elementos que conforman las redes de comunicaciones, se consideraron aspectos de heterogeneidad, seguridad, métodos de interconexión, para proporcionar las herramientas que permitan integrar conocimientos que se aplican en un ambiente red empresarial. El programa de la asignatura, está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para: • Aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario. • Aplicar normas, marcos de referencia, estándares de calidad y seguridad vigentes en el ámbito de desarrollo y gestión de tecnologías y sistemas de información. • Crear y administrar redes de comunicación que contemplen el diseño, selección, instalación y mantenimiento para la operación de equipos de cómputo aprovechando los avances tecnológicos a su alcance y que se adapten a las necesidades empresariales. • Además se integran competencias del área de redes de datos en el proceso de formación profesional durante la carrera, además de tener

implicaciones no sólo para aprender conceptos científicos y tecnológicos, sino también, para formar actitudes y valores de compromiso humano y social inherentes a su práctica profesional en un mundo en el cual la comunicación va más allá de conectar máquinas, sino comunicar a personas y colocar la tecnología al alcance del usuario final, para que su vida productiva sea atractiva.
Intención didáctica
Se organiza el temario agrupando los contenidos de la asignatura en cuatro unidades, distribuyendo los conceptos teóricos que ayudan a lograr el adecuado entendimiento e interpretación de las prácticas que se realizarán a lo largo del curso, lo cual permitirá el óptimo desarrollo y alcance de las competencias que esta asignatura proporciona. En la primera unidad se abarcan las Redes Empresariales, la necesidad de utilizar información ubicada en diferentes ubicaciones geograficas, la necesidad de lograr la interconectividad a nivel de redes de cobertura amplia, elección de protocolos de redes que permitan dicha comuicación. En la segunda unidad se cubre el tema de la Gestion de la Red, donde es importante conocer un protocolo para la administración de la red y las tecnicás para generar los archivos log donde se puede visializar el comportamiento dentro de la red. En la tercera unidad se presentan conceptos avanzados en el Diseño de la Red, dentro de los alcances de esta unidad se cubren las opciones de un diseño de red jerárquico, que en su funcionalidad permite aislar problemas. En la cuarta unidad contemplará la Virtualización de Red, que ofrece nuevas opciones de arquitecturas a la red Empresarial, utilizando el Cómputo en la Nube o bien la Nube Hibrida, todo con el enfoque de que en algunas ocasiones no hay necesidad de adquirir equipamiento.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones

Instituto Tecnológico de Jiquilpan. 8 de mayo de 2023	Ing. David Lira Leyva. Lic. José Manuel Padilla Aguilar. Lic. José Odiseo López Calderón Lic. Ricardo Murguia Rivas Ing. Jorge Alberto Rivera Guerra	Reunión de elaboración curricular de las especialidades de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Describir y conocer las Redes Empresariales. • Describir funcionalidad y configurar el protocolo de administración de la red. • Describir los diferentes tipos de Diseño de la Red, para la adecuada implementación.. • Describir los conceptos de la automatización y virtualización en la Redes Empresariales.

5. Competencias previas

- Analizar las tecnologías básicas de redes con la finalidad de ayudar a desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones, previendo su pertinencia al crecimiento de una Red Empresarial.
- Aplicar normas y estándares vigentes, que permitan un correcto diseño de la red.
- Seleccionar los dispositivos óptimos para garantizar el funcionamiento de una red.
- Planificar y direccionar dispositivos en una red LAN/WAN
- Desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones utilizando el simulador y el laboratorio de redes.

6. Temario

No.	Temas	Subtemas
1	Redes Empresariales	1.1 Introducción a Redes Empresariales 1.1.1. Introducción al Protocolo de Comunicaciones OSPF. 1.1.2. OSPF Área Única 1.1.3. Configuración OSPF v2 de Área Única. 1.2 Conceptos de WAN 1.2.1. Proposito de las WAN. 1.2.2. Operaciones de WAN. 1.2.3 Conectividad WAN Moderna. 1.2.4. Conectividad Basada en Internet
2	Gestión de Red.	2.1 Introducción a la Gestión de Red. 2.1.1. Descubrimiento de Dispositivos CDP. 2.1.2. Descubrimiento de Dispositivos LLDP. 2.2 Protocolo NTP. 2.2.1. Operación NTP. 2.2.2. Configuración NTP. 2.2.3. Verificar NTP. 2.3 Protocolo SNMP 2.3.1. Operación SNMP. 2.3.2. Versiones SNMP. 2.3.3. Escenario SNMP. 2.3.4. Navegador SNMP. 2.4 Mantenimiento de Syslog 2.4.1. Operación Syslog. 2.4.2. Formato Syslog. 2.5. Mantenimeinto al Archivo de configuración de los Dispositivos. 2.6. Gestión de imagen IOS
		3.1. Red Jerárqica. 3.1.1. Diseño de Tres y Dos Niveles.

3	Diseño de Red	3.1.2. Rol de Redes Conmutadas. 3.2. Red Escalable. 3.2.1. Diseño para Escalabilidad. 3.2.2. Reducir el Tamaño del Dominio de la Falla. 3.3. Hardware Capa 2. 3.3.1. Plataformas. 3.3.2. Densidad. 3.3.3. POE. 3.3.4. Multicapa. 3.4. Hardware Capa 3. 3.3.5. Plataformas. 3.3.6. Factores de Forma.
4	Virtualización de Red.	4.1 Cómputo en la Nube. 4.1.1. Descripción. 4.1.2. Servicios en la Nube. 4.1.3. Modelos en la Nube 4.2 Virtualización. 4.2.1. Servidores Dedicados. 4.2.2. Virtualización del Servidor. 4.2.3. Ventajas. 4.2.4 Capas de Abstracción. 4.3. Redes Definidas por Software. 4.4. Automatización de Red.

7. Actividades de aprendizaje de los temas

Unidad I. Redes Empresariales.	
Competencias	Actividades de aprendizaje
Específica(s): • Describir la Red Empresarial. • Manejo del Concepto de la WAN. • Conocer el protocolo OSPF. • Implementación del protocolo OSPF en un entrono de WAN, utilizando IPV4/IPv6. • Conceptualización de conectividad utilizando INTERNET	• Realizar una investigación sobre el concepto de Redes Empresariales, características y necesidades. • Realizar una plenaría en clases para compartir y discutir sobre el concepto de Red Empresarial.

Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo.	• Identificar los tipos de tecnología WAN. • configuración, administración y resolución de problemas de agregación de canales.
Unidad II. Gestión de Red.	
Competencias	Actividades de aprendizaje
Específica(s): • Identificar y describir los componentes necesarios para la gestión de todos los elementos que integran la Red. • Configurar los componenetes que permitan gestionar los elementos de la Red. Genéricas: • Habilidad para realizar proyectos en equipo o grupos de trabajo. Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo.	• Describir el comportamiento de los protocolos estandar para administrar los componentes de una Red • Realizar un modelo a escala que incluya los componentes de una estructura Red para describir sus funciones y la manera en la que se interrelacionan. • Realizar prácticas de laboratorio de configuración de red, habilitar los protocolos que permitan la gestion del total de los componentes que integran la Red. • Actualizar un sistema operativo de los diferentes dispositivos que integran la Red.
Unidad III. Diseño de Red.	
Competencias	Actividades de aprendizaje

Específica(s): • El diseño de una red que permita el aislar problemas y resolverlos sin afectar a diferentes áreas. • Describir el uso de la red jerárquica. • Selección de hardware adecuado para la red jerárquica. • Describir los problemas de implementación de una red redundante. • Describir el propósito y el funcionamiento de los protocolos de redundancia primer salto. • Describir la técnica de agregación de enlaces. • Configurar la agregación de enlaces en dispositivos de comunicaciones. Genéricas: • Habilidad para realizar proyectos en equipo o grupos de trabajo. Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo.	• Realizar un diseño jerárquico de una red. • Configurar un switch para que funcione en una red diseñada para admitir trasmisiones de voz, video y datos. • Investigar de forma individual y analizar de manera grupal que es STP, sus tipos y características en diferentes fuentes de información confiables, y presentar los resultados en una plenaria. • Realizar prácticas de laboratorio de configuración de STP. • Realizar prácticas de configuración, administración y resolución de problemas de agregación de enlaces.
Unidad IV. Virtualización de Red.	
Competencias	Actividades de aprendizaje
Específica(s): • Entender las convenciones de la virtualización. • Administrar los recursos de la red y usar técnicas de	• Instalar un servidor con dos máquinas Virtuales que permitan usar distintos servicios por ejemplo DHCP y WEB.

virtualización para aprovechar al máximo los recursos físicos. • Entender el beneficio de los servicios en la Nube. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo.	• Crear una red LAN/WAN para implementar servicio de virtualización en ambos sentidos. • Analizar servicios en la Nube.

8. Práctica(s)

1.- Diseño de una red con modelo Jerárquico LAN/WAN.

- Identificar las áreas de oportunidad para realizar el proyecto.
- Identificar las capas del modelo jerárquico: Núcleo, Distribución y Acceso.
- Selección de los Dispositivos a utilizar en cada una de las capas.
- Seleccione de acuerdo al diseó el protocolo de ruteo a utilizar en la WAN.

2.- Configuración básica de OSPF área única.

- Verificar la configuración de OSPF
- Propagación de ruta predeterminada.
- Verificar OSPF y ruta predeterminada.

3.- Gestión de la Red de OSPF área única.

- Gestion de CDP y LLDP.
- Integrar un servidor para que los dispositivos trabajen el NTP.
- Visualizar el protocolo SNMP.
- Habilitar el Syslog enviando los Log al servidor que funciona como NTP.

4.- Gestión del IOS.

- Descargue la versión del IOS de un Switch.
- Descargue la versión del IOS de un Router.

- Descargue una versión reciente de IOS e inyectela en un Switch.
- Descargue una versión reciente de IOS e inyectela en un Router.
-

5.- Diseñar una red.

En esta práctica se cubrirán los objetivos del diseño de red en capas.

- Diseñar una red que cumpla con las capas de Acceso, Distribución y Nucleo.
- Documentar el funcionamiento del diseño.

9. Proyecto de asignatura

- **Fundamentación:**

El proyecto fomenta actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración entre las y los estudiantes. Permite relacionar los contenidos de esta asignatura con las demás del plan de estudios para desarrollar una visión interdisciplinaria en la y el estudiante. Finalmente facilitar el contacto directo con materiales e instrumentos, al llevar a cabo actividades prácticas, para contribuir a la formación de las competencias para el trabajo experimental.

Los proyectos a desarrollar pueden ser para empresas manufactureras, educativas, hospitalarias, hoteleras, que desean disponer de su información en toda la empresa y los espacios permiten instalaciones y configuraciones de red de computadoras de forma física e inalámbrica, además de establecer la configuración de conmutación de acuerdo a las necesidades y requisitos de disponibilidad de información dentro de la organización u empresa.

- **Planeación:**

Para pequeñas y medianas empresas, la comunicación digital con datos, voz y video es esencial para la supervivencia de la empresa. En consecuencia, una LAN con un diseño jerárquico es un requisito fundamental para hacer negocios en el presente. La (el) estudiante debe ser capaz de diseñar e implantar una LAN bien diseñada y seleccionar los dispositivos apropiados para admitir las especificaciones de las redes de una empresa pequeña o mediana, considerando en ellas tecnologías inalámbricas.

Por lo cual la (el) estudiante a partir de una necesidad real antes planteada realizará una propuesta considerando las tecnologías aprendidas en clase. La propuesta contendrá los requerimientos de información y de disponibilidad de la empresa u organización, el análisis de espacios, selección y cotización

de equipo, diseño de configuración. Ofreciendo las alternativas vigentes del Computo en la Nube y Nube Hibrida.

- **Desarrollo**:

En esta materia, la (el) alumna(o) comenzará a explorar la arquitectura de las LAN conmutadas y algunos de los principios que se utilizan para diseñar una red jerárquica. La, (el) alumna(o) aprenderá sobre las redes convergentes. También aprenderá cómo seleccionar el switch correcto para una red jerárquica y qué switches son los apropiados para cada capa de red. Las actividades y los laboratorios confirman y refuerzan su aprendizaje.
El objetivo del proyecto es comprender cómo se interconectan y configuran los switchs para brindar acceso a la red a los usuarios de la LAN. Este curso también enseña cómo integrar dispositivos inalámbricos a la LAN.
El docente podrá integrar equipos o de forma individual indicar la necesidad de una propuesta de red, orientará a la y al estudiante sobre sus dudas y lo estimulará a investigar y pensar de forma crítica de acuerdo a las necesidades del proyecto. La (el) alumna(o) por su parte entregará y sus avances en tiempo y forma.

- **Evaluación:**

Evaluación: Los criterios para la evaluación del proyecto que se proponen son:

- Trabajo en equipo e individual: 20%
- La propuesta tendrá un valor 20%
- Diseño de propuestas y pruebas pertinentes 60%

10. Evaluación por competencias

La evaluación de la asignatura debe de ser continua, sumativa y formativa, por lo que debe de considerarse el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Capacidad de análisis, síntesis, abstracción, de organizar y planificar, comprobado mediante las evidencias de aprendizaje tales como: Reportes, ensayos y prácticas, solución de ejercicios extra clase, actividades de investigación, elaboración de modelos o prototipos.
- Resolución de problemas con apoyo de software.
- Exámenes escritos y prácticos para comprobar la adquisición de conocimientos.

11. Fuentes de información

Allan;Lorenz Reid (Jim;Schmidt, Cheryl.). (2019). *Introducción al enrutamiento y la conmutación en la empresa*. Pearson Education.

Odom, W. (2013). *Cisco CCNA Routing Switching 200-120 Official Cert Guide Library*. Indianapolis: Pearson Education.

Odom, W. (2014). *Cisco CCNA Routing and Switching 200-120 Official Cert Simulator Library*. Indianapolis: Pearson Education.

Rivard, E. (2014). *Cisco CCNA Routing and Switching 200-120 Flash Cards and Exam Practice Pack*. Indianapolis, Indiana: Pearson Education.

Sequera, A., & Tiso, J. (2014). *Cisco CCNA Routing and Switching 200-120 Foundation Learning Guide Library*. Indianapolis, Indiana: Pearson Education.

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Ciberseguridad y Ethical Hacking.**
Clave de la asignatura:	**CSD-2404**
SATCA[4]:	**1-4-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

El programa de la asignatura está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para:

- Aplicar conocimientos científicos y tecnológicos con el objetivo de mejorar la ciberseguridad de los sistemas informáticos de empresas y organizaciones.
- Aplicar normas, marcos de referencia, estándares de calidad y seguridad vigentes en el ámbito de desarrollo y gestión de tecnologías y redes empresariales.
- Crear y administrar redes de comunicación que contemplen el diseño, selección, instalación y mantenimiento para la operación de equipos de cómputo aprovechando los avances tecnológicos a su alcance y que se adapten a las necesidades empresariales.
- Además se integran competencias del área de redes de datos en el proceso de formación profesional durante la carrera, además de tener implicaciones no sólo para aprender conceptos científicos y tecnológicos, sino también, para formar actitudes y valores de compromiso humano y social inherentes a su práctica profesional en un mundo en el cual la comunicación va más allá de conectar máquinas, sino comunicar a personas y colocar la tecnología al alcance del usuario final, para que su vida productiva sea atractiva.
- Esta materia está centrada en obtener los beneficios al utilizar el Hacking Ético, ya que ayuda a evaluar y reforzar sus sistemas de

[4] Sistema de Asignación y Transferencia de Créditos Académicos

seguridad. En ella aprenderá a realizar ciberataques supervisados con el fin de medir el nivel de seguridad y descubrir las vulnerabilidades del sistema, los errores y los protocolos de ciberseguridad, reforzar las políticas, así como el darle un mayor valor, como también reducir los costos de inversión, al implementar herramientas y sistemas de defensa más eficaces.
Intención didáctica
El (La) estudiante aprenderá los beneficios al utilizar el hacking ético para evaluar y reforzar sus sistemas de seguridad. • Descubrir vulnerabilidades uno de los beneficios de la ciberseguridad y el hacking ético, es que con los ciberataques realizados por profesionales del hacking ético se pueden identificar las debilidades del sistema y, de esta manera, aplicar acciones correctivas para eliminarlas y evitar los riesgos que suponen en materia de ciberseguridad. Algunas de las vulnerabilidades habituales son de inyección SQL, de desbordamientos de buffer o de Cross Site Scripting (XSS), entre otras. • Refuerza las políticas de ciberseguridad, otro de los beneficios de la ciberseguridad y el hacking ético, se puede medir si la política de ciberseguridad de la empresa es la adecuada y si los usuarios la están cumpliendo de forma correcta, y poder garantizar un alto nivel de ciberseguridad en el negocio. • Aporta valor a la ciberseguridad, gracias al hacking ético, la empresa puede dar valor a la ciberseguridad, ya que empiezan a ser conscientes de la importancia que tiene la seguridad de sus sistemas. • Reduce los costes de inversión, también destaca como beneficio, que la información que aporta el Hackeo Ético permite definir de forma eficiente las medidas necesarias para eliminar vulnerabilidades e implementar las herramientas y sistemas de defensa más eficaces.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones

Instituto Tecnológico de Jiquilpan. 8 de mayo de 2023	Ing. David Lira Leyva. Lic. José Manuel Padilla Aguilar. Lic. José Odiseo López Calderón Lic. Ricardo Murguia Rivas Ing. Jorge Alberto Rivera Guerra	Reunión de elaboración curricular de las especialidades de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones. • Ser capaz de permanecer eficaz dentro de un medio cambiante, así como a la hora de enfrentarse con nuevas tareas, retos y personas. • Conocer las tendencias actuales en técnicas de ciberataque. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros.

5. Competencias previas

- Conocimientos en programación, redes y sistemas operativos.
- Habilidad para identificar y explotar vulnerabilidades en sistemas informáticos.
- Conocimiento de las técnicas y herramientas utilizadas por los hackers malintencionados para realizar ataques.
- Capacidad para realizar pruebas de penetración y evaluaciones de riesgos de forma sistemática y rigurosa.
- Conocimiento de las leyes y regulaciones relacionadas con la seguridad informática y la privacidad de los datos.
- Manejo de criptografía.

6. Temario

No.	Temas	Subtemas
1	Ethical Hacking.	1.1 Penetration Testing 1.1.1 Terminología 1.1.2 Equipos Rojo, Azul 1.2 Instalación del Laboratorio 1.3 Comandos basicos Kali linux 1.4 Configuración Kali 1.5 Nmap
2	Criptología.	2.1 Definición 2.2 Historia 2.3 Tipos de claves Criptograficas 2.3.1 Simétrica 2.3.2 Asimétrica 2.3.2 Híbrida 2.4 Algositmos Hash 2.4.1 Hash para detectar Malware 2.5 SHA2 2.5.1 SHA2-224 2.5.2 SHA2-256 2.5.3 SHA2-384 2.5.4 SHA2-512 2.6 SHA3 2.7 KDF 2.7.1 Argon2 2.7.2 scrytp 2.7.3 bcrypt 2.7.4 PBKDF2 2.8 Enriptación 2.8.1 AES 2.8.2 DES 2.9 Kerberos 2.10 Esteganografía
		3.1 Utilizando Internet 3.2 Google dorks 3.3 OSINT

3	Obtención de Información	3.3 Shodan 3.4 Maltego 3.5 Nmap 3.6 Wireshark 3.7 tcpdump
4	Ingeniera Social.	4.1 Pretexting 4.2 Phishing 4.3 Social Engineering toolkit 4.4 Gosphish 4.5 WifiPhisher
5	Vulnerabilidades.	5.1 Vulnerabilidades con Nmap Scrypting 5.2 OpenVas 5.3 Nessus 5.4 Exploit Database
6	Metasploit.	6.1 Metasploit framework 6.2 Instalación y actualización 6.2.1 Metasploitable 6.3 Utilización de diversos métodos, shells y payloads 6.4 Creación de troyanos 6.4.1 Con uso de Vulnerabilidades 6.4.2 Con backdoor 6.4.5 Incrustados en archivos, imágenes, etc 6.4.6 Con encriptación 6.5 Comandos en Metasploit 6.6 Apoderandose del equipo 6.7 Escalando Privilegios 6.8 Agregando modulos 6.8.1 Exploit-DB 6.8.2 Rapid7 6.8.3 0day.today 6.9 MSFVenom

7. Actividades de aprendizaje de los temas

Unidad I. Ethical Hacking.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita.	• Conocer los papeles en los que operan los equipos Rojo y Azul. • Realizar instalaciones de los entornos controlados para realizar el pentesting. • Realizar la instalación de herramientas para el pentesting.

• Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.	

Unidad II. Criptología.

Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema	• Conocer los diferentes algoritmos de encriptación que existen. • Realizar programación de alto nivel para aplicar los algoritmos de encriptación para encriptar y desencriptar todos los algoritmos. • Aplicar técnicas de esteganografía para ocultar y revelar información.

informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.	
Unidad III. Obtención de la información.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético.	• Conocer las diferentes técnicas de obtención de información, ya sea referente a un dispositivo o a una persona. • Utilizar las herramientas de uso publico y privado para la obtenion de información y vulnerabilidades de equipos y personas.

• Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.	
Unidad IV. Ingeniera social.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales.	• Conocer las diferentes técnicas de ingenieria social. • Realizar campañas de phising mediante correo electronico e

• Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de	instalación de malware en dispositivos tanto móviles como de escritorio o portatiles.

sistemas y en la aplicación de herramientas de seguridad.	

Unidad V. Vulnerabilidades	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción.	• Conocer las diferentes técnicas de escaneo de vulnerabilidades para permitir su detección. • Analizar algunas vulnerabilidades de distintos tipos de sistemas y ver cómo estas pueden ser explotadas por software malicioso. • Desarrollar técnicas y métodos de protección ante vulnerabilidades de distintos tipos de sistemas. • Conocer las herramientas para poder realizar un análisis de vulnerabilidades a fondo.

• Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.	
Unidad VI. Metasploit.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas.	• Desarrollar técnicas de penetración e intrusión en equipos utilizando Backdoor. • Desarrollar técnicas y métodos de protección ante vulnerabilidades de distintos tipos de sistemas. • Crear diferentes virus triyanos e instalarlos en el entorno controlado del laboratorio y determinar como puede ser protegido. • Realizar la penetración en un equipo de laboratorio utilizando los troyanos y ver la manera de protegerlo.

• Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. Genéricas: • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.	

8. Práctica(s)

1.- Instalacion y configiuración de los eqipos a utilizar en el laboratorio. • Instalar los servidores: Windows, Linux, Metasploitable, OWASP, etc. • Instalar el quipo para penetración con Kali Linux. • Utilizar Nmap para explorar la red y los equipos. • Generar equipo de trabajo como son el Rojo y el Azul. **2.- Encriptación.** • Realizar un programa en un lenguaje de alto nivel para hacer encriptación con: ○ Los diferentes métodos vistos en clase.

- Utilizar los diferentes programas de encriptación para realizar esteganografia con:
  - Audio
  - Imagen
  - Video
- Realizar desencriptado con Kerberos.

3.- Obtención de la información.

- Realizar búsquedas con Google dorks sobre un tema en especifíco.
- Utilizar la red OSINT para investigar a personas.
- Utilizar la red Shodan para encontrar MAC adress de diversos dispositivos
- Realizar búsqueda avanzada con NMAP
- Capturar y analizar tráfico de la red del laboratorio

4.- Ingenieria Social.

- Realizar Pretexting
- Hacer una campaña de phising con las diversas herramientas disponibkles.
- Utilizar la herramienta incorporada SET en Kali Linux para realiar phising con emal y demás.
- Utilizar WifiPhiser para la obtencion de información del usuario, y capturar sus datos.

5.- Vulnerabilidades.

- Utilizar NMAP para encontrar las vulnerabilidades de los equipos de la red.
- Instalar OpenVas para detectar vulnerabilidades de los eqipos.
- Instalar y configurar la herramienta Nessus para la detección de vulnerabiliades en los equpos del laboratorio.
- Utilizar la base de datos de la red Exploit DB para la interpretacion de los voletines de seguridad.

6. Metasploit

- Instalar y configurar la herramienta Metasploit
- Crear virus triyanos
- Utilizar las Vulnerabilidades encotradas de los equipos para hacer pruebas de penetración.
- Crear virus triyanos con ecnriptación a nivel de se indectados por los antivirus y firewalls.
- Tomar control de los equipos y escalar los privilegios del usuario

- Instalar y configurar MSFVenom para crear backdoors y tomar control de los diferentes equipos.

9. Proyecto de asignatura

- **Fundamentación:**

El proyecto fomenta actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración entre las y los estudiantes. Permite relacionar los contenidos de esta asignatura con las demás del plan de estudios para desarrollar una visión interdisciplinaria en la y el estudiante. Finalmente facilitar el contacto directo con materiales e instrumentos, al llevar a cabo actividades prácticas, para contribuir a la formación de las competencias para el trabajo experimental.
Los proyectos a desarrollar pueden ser para empresas manufactureras, educativas, hospitalarias, hoteleras, que desean disponer de su información en toda la empresa y los espacios permiten instalaciones y configuraciones de red de computadoras de forma física e inalámbrica, además de establecer la configuración de conmutación de acuerdo a las necesidades y requisitos de disponibilidad de información dentro de la organización u empresa.

Cabe destacar que durante las pruebas de penetración a sistemas tanto infomáticos como de redes inalámbricas y cableadas se realizara en un entorno controlado y privado dentro del laboratio, utilizando hackin ethico en todo momento.

- **Planeación:**

Llevar a cabo la instalación de diversos servidores de red, como por ejemplo, Windows Server, Ubuntu, Kali, Metasploitable, OWASP, etc que contengan varios servicios por ejemplo DNS, SQL, etc para que sean en ellos donde se lleven a cabo las pruebas de pentración.

Tambien instalar una de red o varias Wifi en donde se lleven a cabo las prubeas de captura de la contraseña.

Utilizar dispositivos móviles como smartphones para realizar las pruebas de hackcing ethico.

- **Desarrollo:**

En esta materia, la (el) alumna(o) comenzará a generarse un criterio de la importancia de ser pentester y a aplicar los conocimiento de hacking ethico. Desarrollara la habilidad para poder determinar en que algoritmo de encriptación común se encuentra una clave y como proteger ante una amenaza.
Dentro del laboratorio se formaran grupos de estudiantes en los cuales dividiran en Equipo Rojo y Equipo Azul para hacer una simulación de un ataque y de respueta ante un hackeo.

- **Evaluación:**

Evaluación: Los criterios para la evaluación del proyecto que se proponen son:

- Trabajo en equipo e individual: 20%
- La propuesta tendrá un valor 20%
- Diseño de propuestas y pruebas pertinentes 60%

10. Evaluación por competencias

La evaluación de la asignatura debe de ser continua, sumativa y formativa, por lo que debe de considerarse el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Capacidad de análisis, síntesis, abstracción, de organizar y planificar, comprobado mediante las evidencias de aprendizaje tales como: Reportes, ensayos y prácticas, solución de ejercicios extra clase, actividades de investigación, elaboración de modelos o prototipos.
- Resolución de problemas con apoyo de software.
- Exámenes escritos y prácticos para comprobar la adquisición de conocimientos.

11. Fuentes de información

- R. MESSIER, CEH V11 CERTIFIED ETHICAL HACKER STUDY GUIDE. [S.l.]: WILEYSYBEX, 2021.
- S. McClure, J. Scambray and G. Kurtz, Hacking exposed. Berkeley, Calif.: Osborne/McGraw-Hill, 1999.
- R. Luppicini and B. Abu-Shaqra, The changing scope of technoethics in contemporary society. IGI Global, 2018.

- Leonhardt F, "Auditing, Penetration Testing And Ethical Hacking". World Scientific Publishing Co, 2010. Available from: Scopus®, Ipswich, MA.
- Himma K, Tavani H, "Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking". Handbook Of Information & Computer Ethics [serial online]. January 2008;:191. Available from: Complementary Index, Ipswich, MA.
- Vignesh R, Rohini K. "Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security". International Journal Of Engineering And Technology(UAE) [serial online]. January 1, 2018;7(3.27 Special Issue 27):196-199.
- Berger H, Jones A. "Cyber security & ethical hacking for SMEs". ACM International Conference Proceeding Series [serial online]. July 25, 2016;Part F130520(Proceedings of the 11th International Knowledge Management in Organizations Conference on the Changing Face of Knowledge Management Impacting Society, KMO 2016.
- Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. "Ethical hacking: The need for cyber security". IEEE International Conference On Power, Control, Signals And Instrumentation Engineering, ICPCSI 2017 [serial online]. June 20, 2018;(IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017):1602-1606.
- Molina F. "La evolución de las técnicas de 'hacking' ético". Red Seguridad: Revista Especializada En Seguridad Informática, Protección De Datos Y Comunicaciones[serial online]. 2015;(. 68):62.
- K. Mitnick and W. Simon, El arte de la intrusion. RA-MA S.A., 2007. [11] ?tefan I, Ramona M. MALWARE FOR MOBILE DEVICES AND THEIR SECURITY. Fiabilitate ?i Durabilitate, Vol 1, Iss 21, Pp 267-272 (2018) [serial online]. 2018;(21):267.
- M. Sikorski and A. Honig, Practical malware analysis. San Francisco, 2012.
- D. Stuttard, M. Pinto and J. Pauli, The web application hacker's handbook. Indianapolis, Ind.: John Wiley & Sons, 2012.

1. Datos Generales de la asignatura

Nombre de la asignatura:	**Ciberseguridad y Pentesting.**
Clave de la asignatura:	**CSD-2405**
SATCA[5]:	**1-4-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

El programa de la asignatura está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para:

- Aplicar conocimientos científicos y tecnológicos con el objetivo de mejorar la ciberseguridad de los sistemas informáticos de empresas y organizaciones.
- Aplicar normas, marcos de referencia, estándares de calidad y seguridad vigentes en el ámbito de desarrollo y gestión de tecnologías y redes empresariales.
- Crear y administrar redes de comunicación que contemplen el diseño, selección, instalación y mantenimiento para la operación de equipos de cómputo aprovechando los avances tecnológicos a su alcance y que se adapten a las necesidades empresariales.
- Además se integran competencias del área de redes de datos en el proceso de formación profesional durante la carrera, además de tener implicaciones no sólo para aprender conceptos científicos y tecnológicos, sino también, para formar actitudes y valores de compromiso humano y social inherentes a su práctica profesional en un mundo en el cual la comunicación va más allá de conectar máquinas, sino comunicar a personas y colocar la tecnología al alcance del usuario final, para que su vida productiva sea atractiva.

Esta materia está centrada en obtener los beneficios al utilizar el Hacking Ético, ya que ayuda a evaluar y reforzar sus sistemas de seguridad. En ella

[5] Sistema de Asignación y Transferencia de Créditos Académicos

aprenderá a realizar ciberataques supervisados con el fin de medir el nivel de seguridad y descubrir las vulnerabilidades del sistema, los errores y los protocolos de ciberseguridad, reforzar las políticas, así como el darle un mayor valor, como también reducir los costos de inversión, al implementar herramientas y sistemas de defensa más eficaces.

Intención didáctica

El (La) estudiante aprenderá los beneficios al utilizar el hacking ético para evaluar y reforzar sus sistemas de seguridad.

- Descubrir vulnerabilidades uno de los beneficios de la ciberseguridad y el hacking ético, es que con los ciberataques realizados por profesionales del hacking ético se pueden identificar las debilidades del sistema y, de esta manera, aplicar acciones correctivas para eliminarlas y evitar los riesgos que suponen en materia de ciberseguridad. Algunas de las vulnerabilidades habituales son de inyección SQL, de desbordamientos de buffer o de Cross Site Scripting (XSS), entre otras.
- Refuerza las políticas de ciberseguridad, otro de los beneficios de la ciberseguridad y el hacking ético, se puede medir si la política de ciberseguridad de la empresa es la adecuada y si los usuarios la están cumpliendo de forma correcta, y poder garantizar un alto nivel de ciberseguridad en el negocio.
- Aporta valor a la ciberseguridad, gracias al hacking ético, la empresa puede dar valor a la ciberseguridad, ya que empiezan a ser conscientes de la importancia que tiene la seguridad de sus sistemas.

Reduce los costes de inversión, también destaca como beneficio, que la información que aporta el Hackeo Ético permite definir de forma eficiente las medidas necesarias para eliminar vulnerabilidades e implementar las herramientas y sistemas de defensa más eficaces.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Jiquilpan. 8 de mayo de 2023	Ing. David Lira Leyva. Lic. José Manuel Padilla Aguilar. Lic. José Odiseo López Calderón Lic. Ricardo Murguia Rivas Ing. Jorge Alberto Rivera Guerra	Reunión de elaboración curricular de las especialidades de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. • Que los estudiantes sepan comunicar sus conclusiones y los conocimientos razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. • Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. • Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones. • Ser capaz de permanecer eficaz dentro de un medio cambiante, así como a la hora de enfrentarse con nuevas tareas, retos y personas. • Ser capaz de proponer soluciones imaginativas y originales así como ser capaz de promover la innovación e identificación de alternativas contrapuestas a los métodos y enfoques tradicionales en el ámbito de la ciberseguridad. • Conocer y aplicar métodos de protección en sistemas tecnológicos industriales y sociales avanzados. • Ser capaz de integrarse en equipos de trabajo o investigación multidisciplinares de manera eficaz y colaborativa.

- Conocer las tendencias actuales en técnicas de ciberataque.
- Comprender, aplicar y evaluar técnicas de hacking ético.
- Comprender, aplicar y evaluar la gestión de la seguridad de sistemas altamente seguras por su naturaleza o criticidad.
- Analizar e identificar las vulnerabilidades de un sistema informático, y ser.

5. Competencias previas

- Conocimientos en programación, redes y sistemas operativos.
- Habilidad para identificar y explotar vulnerabilidades en sistemas informáticos.
- Conocimiento de las técnicas y herramientas utilizadas por los hackers malintencionados para realizar ataques.
- Capacidad para realizar pruebas de penetración y evaluaciones de riesgos de forma sistemática y rigurosa.
- Conocimiento de las leyes y regulaciones relacionadas con la seguridad informática y la privacidad de los datos.
- Manejo de criptografía.

6. Temario

No.	Temas	Subtemas
1	Pentesting Wifi.	1.1 Requerimeintos técnicos 1.2 Arquitectura WiFi 1.3 Protocolos de seguirdad WEP, WPA, WPA2, WPA3 1.4 Tipos de Ataques 1.5 Wifiphiser 1.6 Aircrack.ng 1.6.1 Airodump-ng 1.6.2 Airplay-ng 1.7 Airgeddon 1.7.1 The Evil 1.7.2 Twin attack 1.8 Wifite
		2.1 Proyecto OWASP 2.2 Instalación y configuración 2.3 Burp Suite 2.3.1 Herramientas

2	Pentesting OWASP.	2.3.2 Proxy, Target, Scanner, Pepeater, Intruder, Sequencer, Decoder, Comparer, Extender, Hydra, Medusa, Ncrack, Jhon the ripper, Hasch Cat 2.4 Arquitectura de una aplicación web 2.5 Lenguajes de desarrollo de aplicaiones web 2.5.1 Python, Ruby, Java, ASP.net, Php 2.6 Protocolo HTTP 2.6.1 Solicitudes y Respuestas 2.7 Ataques comunes 2.7.1 inclusion attacks (LFI/RFI) 2.7.2 Cross-Site Request Forgery (CSRF) 2.7.3 Cross-Site Scripting (XSS) 2.7.4 SQL injection 2.8 Ataque a aplicaciones web 2.8.1 Nikto 2.8.2 SQlmap 2.8.3 Backdoor con PHP
3	SQL, DNS.	3.1 Acceso anonimo a la red 3.1.1 FreeVPN 3.1.2 Tor 3.1.3 ProxyChains 3.1 SQL 3.1.1 Ataque a contraseñas 3.1.2 Backdoor con sql injection 3.1.3 Denegación del servicio 3.2 DNS 3.2.1 Obtención de Información 3.2.2 Denegación del servicio
		4.1 Ciberpatrullaje. 4.1.1 Inspección de medidas de seguridad en el entorno. 4.2 Que activos debo de proteger.

4	Ciberpratullaje y CiberDefensa.	4.3 Activos vulnerables dentro de la organización. 4.4 Estrategias de ciberdefensas. 4.4.1 Modelos protección de la seguridad. 4.5 ¿Cómo protegerme? 4.6 Modelos de ciberdefensas. 4.7 Ciberdefensa personal. 4.7.1 Esquemas de protección de seguridad informática personal. 4.7.2 Contramedidas de protección. 4.7.3 Software y herramientas de protección. 4.8 Ciberdefensa organizacional. 4.8.1 ¿Cómo proteger mi organización? 4.8.2 Modelos de protección en capas. 4.8.3 Medidas para proteger los activos organizacionales.
5	Certificación.	5.1 Instalación y configuración del laboratorio 5.1.1 Kali linux 5.1.2 Windows servers 5.1.3 Metasploitable 5.2 Fundamentos y descripción de la certificación eJPT 5.3 Herramientas para la certificación 5.3.1 Burp suite 5.3.2 Target y Proxy 5.3.3 Foxy Proxy 5.3.4 CA Certificate 5.3.5 Intruder, Sniper 5.3.6 Battery Ram 5.3.7 Intruder: Pichfork 5.3.8 Intruder: Cluster Bomb 5.3.9 Repeater 5.3.10 Decoder y Comparer 5.3.11 Hydra, Jhon the Ripper 5.4 Elaboración del Informe

		5.4.1 Post-reporte de pentesting 5.4.2 Estructura de reporte de pentesting 5.4.3 Redacción de metodología 5.4.4 Redacción sobre Recomendaciones

7. Actividades de aprendizaje de los temas

Unidad I. Pentesting Wifi.	
Competencias	Actividades de aprendizaje
Específica(s): • Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización. • Capacidad para diseñar estrategias, políticas y normativas de ciberseguridad corporativa. • Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información. • Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red. • Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral.	• Realiazar la instalación de varias redes Wifi con los diferentes protocolos de seguridad y realizar pruebas de hacking ethico. • Utilizar las diversas herramientas para obtener la contraseña de una red wifi. • Aplicar los conocimientos para proteger las redes wifi de intrusiones.

• Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos. • Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes • Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa. • Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo • Capacidad de realizar un trabajo o proyecto individual integrando y relacionando las competencias adquiridas en las distintas asignaturas del máster, junto con la capacidad de defenderlo en público ante un grupo de personas expertas en el tema del trabajo. Genéricas: • Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa.	

• Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización. • Dotar al alumno de la capacidad de diseñar e implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas. • Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad. Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de	

aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia.	
Unidad II. Pentesting OWASP.	
Competencias	Actividades de aprendizaje
Específica(s): • Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización. • Capacidad para diseñar estrategias, políticas y normativas de ciberseguridad corporativa. • Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información. • Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red. • Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral. • Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos.	• Instalar el servidor del proyecto OWASP. • Instalar las diferentes herramientas para las pruebas de penetración de sitios y servidores web. • Realizar ataques a los servidores instalados en el laboratorio. • Proteger mediante los conocimientos adquiridos a los servidores y servicios Web.

• Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes • Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa. • Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo • Capacidad de realizar un trabajo o proyecto individual integrando y relacionando las competencias adquiridas en las distintas asignaturas del máster, junto con la capacidad de defenderlo en público ante un grupo de personas expertas en el tema del trabajo. Genéricas: • Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa. • Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus	

consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización. • Dotar al alumno de la capacidad de diseñar e implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas. • Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad. Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia.	

Unidad III. SQL, DNS.	
Competencias	Actividades de aprendizaje
Específica(s): • Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización. • Capacidad para diseñar estrategias, políticas y normativas de ciberseguridad corporativa. • Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información. • Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red. • Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral. • Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos. • Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de	• Realizar la instalación de por lo menos 2 servidores SQL, uno con Sql Server y otro con MySql. • Utilizar las técnicas de penetración aprendidas para hacer pentesting y hacking ethico a los servidores. • Utilizando los conocimeintos adquiridos preparar a los quipos Rojo y Azul para simular un ataque y respuesta.

detección y de respuesta a incidentes • Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa. • Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo • Capacidad de realizar un trabajo o proyecto individual integrando y relacionando las competencias adquiridas en las distintas asignaturas del máster, junto con la capacidad de defenderlo en público ante un grupo de personas expertas en el tema del trabajo. Genéricas: • Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa. • Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis	

y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización. • Dotar al alumno de la capacidad de diseñar e implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas. • Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad. Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia.	
Unidad IV. Ciberpratullaje y CiberDefensa.	
Competencias	Actividades de aprendizaje
Específica(s):	

• Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización. • Capacidad para diseñar estrategias, políticas y normativas de ciberseguridad corporativa. • Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información. • Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red. • Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral. • Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos. • Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes • Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad,	• Comprobar la capacidad de una empresa en ciberseguridad. • Proactividad o ser capaz de anteponerse ante las posibles amenazas. • Realizar un plan de acción preventivo en seguridad informática. • Permitir la continuidad de un servicio o producto. • Conocer las diferentes técnicas de escaneo de vulnerabilidades para permitir su detección. • Analizar algunas vulnerabilidades de distintos tipos de sistemas y ver cómo estas pueden ser explotadas por software malicioso. • Desarrollar técnicas y métodos de protección ante vulnerabilidades de distintos tipos de sistemas.

incluyendo análisis de malware, análisis forense e ingeniería inversa. • Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo • Capacidad de realizar un trabajo o proyecto individual integrando y relacionando las competencias adquiridas en las distintas asignaturas del máster, junto con la capacidad de defenderlo en público ante un grupo de personas expertas en el tema del trabajo. Genéricas: • Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa. • Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o	

eliminar sus impactos hacer resiliente a la organización. • Dotar al alumno de la capacidad de diseñar e implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas. • Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad. Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia.	

Unidad V. Certificación.	
Competencias	Actividades de aprendizaje
Específica(s): • Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un	• Utilizando el laboratorio controlado de pentesting, realizar simulaciones de ataque y defenza con los equipos Rojo y Azul para

sistema de ciberseguridad en una organización. • Capacidad para diseñar estrategias, políticas y normativas de ciberseguridad corporativa. • Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información. • Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red. • Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral. • Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos. • Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes • Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa.	estudiar a fondo todos los conocimientos adquiridos y preparase para la certificación EJTP.

• Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo • Capacidad de realizar un trabajo o proyecto individual integrando y relacionando las competencias adquiridas en las distintas asignaturas del máster, junto con la capacidad de defenderlo en público ante un grupo de personas expertas en el tema del trabajo. Genéricas: • Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa. • Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización. • Dotar al alumno de la capacidad de diseñar e	

implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas. • Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad. • Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia.	

8. Práctica(s)

1.- Pentesting Wifi. • Instalar y configurar por lo menos 2 redes wifi en el laboratorio. • Instalar y Configurar WifiPhiser para crear un access point falso y obetener información de los usuarios conectados. • Instalar y configurar o en su caso actuklizar las herramientas de la Suite Aircrack • Instalar y configurar la herramienta Airgeddon.

- Actualizar la herramienta Wifite para obtener las contraseñas de la redes wifi del laboratorio

2.- OWASP.

- Instalar y configurar el servidor web en los diversos servidores del laboratorio.
- Levantar el servidor del proyecto OWASP para realizar pruebas de pentesting web
- Obetener contraseñas de los servidores que se encuentren en la red del laboratorio.
- Realizar ataques a los diferentes entornos de servidores web como Python, Ruby, Java, ASP.net, Php, etc
- Realizar pruebas de penetración con Cross-Site
- Instalar y configurar por lo menos 2 diferntes servidores SQL
- Realiar pruebas de penetración con SQL injection en los servidores
- Utilizando la herramienta Nikto, hacer un ataque a un sitio web
- Realizar ataque de Backdoor y apoderarse del servidor web php

3.- SQL, DNS.

- Configurar el equipo de penetración Kali para tener acceso anonimo a la Web
- Instalar y configurar VPN
- Acceder a la Deep Web mediante Tor
- Configurar ProxyChains para un acceso más seguro y navegar por la deep web
- Atacar al servidor SQL mediante la obtencion de Contraseñas por medio de las herramientas
- Planear el uso de las herramientas de denegación del servicio DNS para atacar un servidor DNS
- Cambiar las tablas de DNS para desvio de sitio web

4.- Ciberpatrullaje y CiberDefensa.

- Instalar y configirar las herramientas de ciberpatrullaje
- Proteger los equipos del laboratorio mediante antivirus y firewalls
- Realizar prácticas de pentetración y defenza entre los equpos Rojo y Azul
- Instalación de medidas de proteccion en los dispositivos móviles

5.- Certificación.

- Instalación y configuración del laboratorio.

- Instalación de certificados Web en los servidores
- Mediante la herramienta Intruder y Sniper realizar pruebas de penetración.
- Obtener las contraseñas de los equipos en la red mediante Hydra Jhon de Ripper etc.
- Realizar un reporte de Pentesting que este conforme a los estandares internacionales
-

9. Proyecto de asignatura

- **Fundamentación:**

El proyecto fomenta actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración entre las y los estudiantes. Permite relacionar los contenidos de esta asignatura con las demás del plan de estudios para desarrollar una visión interdisciplinaria en la y el estudiante. Finalmente facilitar el contacto directo con materiales e instrumentos, al llevar a cabo actividades prácticas, para contribuir a la formación de las competencias para el trabajo experimental.
Los proyectos a desarrollar pueden ser para empresas manufactureras, educativas, hospitalarias, hoteleras, que desean disponer de su información en toda la empresa y los espacios permiten instalaciones y configuraciones de red de computadoras de forma física e inalámbrica, además de establecer la configuración de conmutación de acuerdo a las necesidades y requisitos de disponibilidad de información dentro de la organización u empresa.

- **Planeación:**

Llevar a cabo la instalación de diversos servidores de red, como por ejemplo, Windows Server, Ubuntu, Kali, Metasploitable, OWASP, etc que contengan varios servicios por ejemplo DNS, SQL, etc para que sean en ellos donde se lleven a cabo las pruebas de pentración.

Tambien instalar una de red o varias Wifi en donde se lleven a cabo las prubeas de captura de la contraseña.

Utilizar dispositivos móviles como smartphones para realizar las pruebas de hackcing ethico.

Realizar ataques a los servidores web utilizando las diversas técnicas de penetración.

Realizar ataques a los servidores SQL y DNS para denegar el servicio y tener control de los mismos.

Hacer unos de las diversas herramientas para realizar CiberPatrullaje y poder dar respuesta ante un ataque.

Mediante todos los conocimientos adquiridos de CiberSeguridad, instalar el entorno necesario con equipos y deversos sistemas para poder llevar a cabo las prácticas necesarias para la atacar y dar respuesta y brindar un informe.

Utilizando el laboratorio realizar un estudio a fondo para la certificación EJTP.

- **Desarrollo**:

En esta materia, la (el) alumna(o) comenzará a generarse un criterio de la importancia de ser pentester y a aplicar los conocimiento de hacking ethico. Desarrollara la habilidad para poder determinar en que algoritmo de encriptación común se encuentra una clave y como proteger ante una amenaza.

Dentro del laboratorio se formaran grupos de estudiantes en los cuales dividiran en Equipo Rojo y Equipo Azul para hacer una simulación de un ataque y de respueta ante un hackeo.

- **Evaluación:**

Evaluación: Los criterios para la evaluación del proyecto que se proponen son:

- Trabajo en equipo e individual: 20%
- La propuesta tendrá un valor 20%
- Diseño de propuestas y pruebas pertinentes 60%

10. Evaluación por competencias

La evaluación de la asignatura debe de ser continua, sumativa y formativa, por lo que debe de considerarse el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Capacidad de análisis, síntesis, abstracción, de organizar y planificar, comprobado mediante las evidencias de aprendizaje tales como: Reportes, ensayos y prácticas, solución de ejercicios extra clase, actividades de investigación, elaboración de modelos o prototipos.
- Resolución de problemas con apoyo de software.
- Exámenes escritos y prácticos para comprobar la adquisición de conocimientos.

11. Fuentes de información

- R. MESSIER, CEH V11 CERTIFIED ETHICAL HACKER STUDY GUIDE. [S.l.]: WILEYSYBEX, 2021.
- S. McClure, J. Scambray and G. Kurtz, Hacking exposed. Berkeley, Calif.: Osborne/McGraw-Hill, 1999.
- R. Luppicini and B. Abu-Shaqra, The changing scope of technoethics in contemporary society. IGI Global, 2018.
- Leonhardt F, "Auditing, Penetration Testing And Ethical Hacking". World Scientific Publishing Co, 2010. Available from: Scopus®, Ipswich, MA.
- Himma K, Tavani H, "Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking". Handbook Of Information & Computer Ethics [serial online]. January 2008;:191. Available from: Complementary Index, Ipswich, MA.
- Vignesh R, Rohini K. "Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security". International Journal Of Engineering And Technology(UAE) [serial online]. January 1, 2018;7(3.27 Special Issue 27):196-199.
- Berger H, Jones A. "Cyber security & ethical hacking for SMEs". ACM International Conference Proceeding Series [serial online]. July 25, 2016;Part F130520(Proceedings of the 11th International Knowledge Management in Organizations Conference on the Changing Face of Knowledge Management Impacting Society, KMO 2016.
- Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. "Ethical hacking: The need for cyber security". IEEE International Conference On Power, Control, Signals And Instrumentation Engineering, ICPCSI 2017 [serial online]. June 20, 2018;(IEEE International Conference on Power,

Control, Signals and Instrumentation Engineering, ICPCSI 2017):1602-1606.

- Molina F. "La evolución de las técnicas de 'hacking' ético". Red Seguridad: Revista Especializada En Seguridad Informática, Protección De Datos Y Comunicaciones[serial online]. 2015;(. 68):62.
- K. Mitnick and W. Simon, El arte de la intrusion. RA-MA S.A., 2007. [11] ?tefan I, Ramona M. MALWARE FOR MOBILE DEVICES AND THEIR SECURITY. Fiabilitate ?i Durabilitate, Vol 1, Iss 21, Pp 267-272 (2018) [serial online]. 2018;(21):267.
- M. Sikorski and A. Honig, Practical malware analysis. San Francisco, 2012.
- D. Stuttard, M. Pinto and J. Pauli, The web application hacker's handbook. Indianapolis, Ind.: John Wiley & Sons, 2012.