1. Datos Generales de la asignatura

Nombre de la asignatura:	**SEGURIDAD EN SERVICIOS**
Clave de la asignatura:	SDI-2204
SATCA[1]:	2 - 3 - 5
Carrera:	Ingeniería en Sistemas Computacionales.

2. Presentación

Caracterización de la asignatura
La seguridad de los servicios en red es esencial para proteger la información y la imagen o prestigio de una empresa o institución, así como también impedir actividades o accesos no autorizados. El objetivo general es proteger la infraestructura de TI y los datos de la red frente a amenazas externas e internas. La administración de seguridad en los servicios de red no sólo implica el mantener al día las políticas y procedimientos de seguridad establecidos, sino la realización de auditorías, mediante pruebas de penetración y desempeño a los servicios, protocolos y aplicaciones de la red. También es importante comenzar a conocer cómo se lleva a cabo la presentación de datos validos ante un proceso legal mediante la informática forense.
Intención didáctica
El alumno conocerá elementos para llevar a cabo un análisis de riesgos y su implementación en los servicios de red, establecidos en la organización y las diferentes técnicas para obtener información en un crimen digital.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Morelia, 30 de agosto de 2022.	Dr. Heberto Ferreira Medina Dr. Anastacio Antolino Hernández Dr. Juan Carlos Olivares Rojas MSC. Juan Jesús Ruiz Lagunas ISC. Rubén Lara Bárcenas	Diseño Curricular basado en Competencias del Módulo de “Seguridad en infraestructura y servicios”.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El alumno conocerá metodologías de análisis de riesgos, elaboración de procedimientos y políticas de seguridad, para su uso e implementación de la red dentro de la organización, así como llevar a cabo pruebas de penetración y vulnerabilidades de los servicios en red. Además, se analizará e implementaran diferentes metodologías para la informática forense.

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Capacidad de análisis y síntesis.
- Capacidad deductiva e inductiva.
- Conocimientos de redes u servicios.
- Observar el escenario problema e identificar oportunidades de desarrollo de proyectos generando ideas innovadoras de la aplicación de la investigación en su área profesional.

6. Temario

No.	Temas	Subtemas
1	**Introducción**	1. Definición y objetivos de servicios y microservicios (Contenedores) 2. Arquitecturas y plataformas (utilizadas para montar servicios y contenedores) 3. Servicios • Autenticación • Autorización • Contabilidad 4. Normas y estándares de servicios.
2	**Análisis de riesgos en servicios de red**	1. Arquitectura de servicios confiables 2. Monitoreo y reconocimiento 3. Herramientas administrativas 4. Rendimiento y resiliencia
3	**Pruebas de penetración** (**Pentesting**)	1. Antecedentes, conceptos y ética 2. Aspectos legales (legislación) 3. Herramientas 4. Escaneo 5. Metodologías
4	**Introducción a la informática forense**	1. Fundamentos de informática forense 2. Proceso de investigación de informática forense 3. Analizar discos duros y sistemas de archivos 4. Adquisición y duplicación de datos 5. Defensa ante técnicas antiforenses

7. Actividades de aprendizaje de los temas

Tema 1: Introducción	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá la definición y objetivos de servicios, microservicios y contenedores. - Investigará las diferentes arquitecturas, plataformas y estándares para brindar servicios de red. Genéricas: - Conocerá los conceptos de seguridad en redes y servicios de red.	1. Documentarse en todos los conceptos de seguridad en redes y servicios de red. 2. Investigar las normas y plataformas para montar servicios de red. 3. Investigar sobre la virtualización y crear un escenario para probar diferentes servicios de red.
Tema 2: Análisis de riesgos en servicios de red	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá la arquitectura para implementar servicios de red seguros. - Implementara diferentes herramientas para monitoreo y reconocimiento. - Revisará que el rendimiento de los servicios de red se conserve y sea resiliente. Genéricas: - Implementara servicios confiables y resilientes, así como diferentes herramientas administrativas para supervisión.	1. Implementar diferentes servicios de red en el escenario previo. 2. Instalar y configurar diferentes herramientas de monitoreo y supervisión para los diferentes servicios de red. 3. Comprobar el rendimiento y capacidad de recuperación de los diferentes servicios.
Tema 3: Pruebas de penetración (Pentesting)	

Competencias	Actividades de aprendizaje
Específica(s): - Conocerá los términos, antecedentes y ética del Pentesting. - Implementará las diferentes metodologías y herramientas de pruebas de penetración. - Analizará los resultados del escaneo y aplicara correcciones sobre los servicios de red. Genéricas: - Configurará de forma correcta los servicios de red de acuerdo a los resultados de las pruebas de penetración.	1. Realizar las pruebas de penetración suficientes sobre los servicios de red para garantizar el rendimiento correcto e integridad de la información. 2. Llevar a cabo hacking ético para vulnerar servidores.
Introducción a la informática forense	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá los elementos básicos de la informática forense - Implementará y utilizará diferentes herramientas para analizar discos duros y sistemas de archivos. - Utilizará diferentes técnicas para conservar datos contundentes ante un posible ataque. Genéricas: - Usará métodos, técnicas y obtendrá información relevante durante un crimen digital	1- Realizar análisis forense ataques a los servicios configurados en el escenario anterior 2- Conservar y presentar datos relevantes de los diferentes ataques 3- Implementar los cambios necesarios para evitar ataque en los servicios de red

8. Práctica(s)

- Implementar servicios de red en los servidores, para ser utilizados como laboratorio para pruebas de vulnerabilidad y poder ser analizados de manera posterior.
- Reconocer y escanear servicios y vulnerabilidades en la red.
- Vulnerar los servicios con baja seguridad para lograr acceso a los servidores.
- Elaborar reportes e informes de la auditoria de seguridad llevada a cabo con las herramientas de Pentesting.
- Realizar documentación con informe sobre los datos recabados durante el análisis forense

9. Proyecto de asignatura

- Crear un escenario con diferentes servidores y servicios de red.
- Realizar Pentesting a los servicios de red.
- Generar informes de rendimiento y monitoreo de los diferentes servicios.
- Aplicar correcciones a los servicios de red para tener diferentes resultados en nuevas pruebas de penetración.
- Mostrar el análisis forense de las pruebas de penetración iniciales.

10. Evaluación por competencias

- Elaboración de prácticas y su evaluación.
- Proyecto de configuración, monitoreo, pentesting y análisis forense
- Aplicar esquemas de seguridad en servicios de red para disminuir las amenazas.

11. Fuentes de información

[1] EC-COUNCIL. “Digital Forensics Essentials”, EC-COUNCIL OFFICIAL CURRICULA 2022 https://www.eccouncil.org/official/ (accedido agosto 2022).

[2] IBM. https://www.ibm.com/mx-es/topics/infrastructure (accedido agosto 2022).

[3] EC-COUNCIL. “Ethical Hacking Essentials”, EC-COUNCIL OFFICIAL CURRICULA. 2022. https://www.eccouncil.org/official/ (accedido agosto 2022)

[4] Amazon, aws. https://docs.aws.amazon.com/es_es/wellarchitected/latest/security-pillar/infrastructure-protection.html (accedido agosto 2022)

[5] NIST, National Institute of Standards and Technology, NIST SP 800-123, Guide to General Server Security. 2022.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

[6] SANS, SysAdmin Audit, Networking and Security Institute. Políticas de seguridad para servidores. 2022. https://www.sans.org/information-security-policy/ (accedido agosto 2022).

[7] Sitio dedicado a la seguridad, Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx (accedido agosto 2022).

[8] Seguridad de servicios web – Documentación de IBM 2022. https://www.ibm.com/docs/es/was-liberty/base?topic=applications-web-services-security (accedido agosto 2022).

[9] Seguridad para los servicios básicos. 2022. https://docs.oracle.com/es-ww/iaas/Content/Security/Concepts/security_core_services.htm (accedido agosto 2022).

[10] Seguridad de los servicios - WCF | Microsoft Docs. 2022. https://docs.microsoft.com/es-es/dotnet/framework/wcf/securing-services. (accedido agosto 2022).

[11] Cisco Soluciones de Seguridad. 2022. https://www.cisco.com/site/mx/es/products/security/index.html (accedido agosto 2022).

[12] "Home - Docker". Docker. https://www.docker.com/ (accedido el 30 de agosto de 2022).

[13] "Contenedores". Kubernetes. https://kubernetes.io/es/docs/concepts/containers/ (accedido el 30 de agosto de 2022).

[14] Scarfone K., Mell P., (2007) Guide to Intrusion Detection and Prevention Systems (IDPS), NIST. https://csrc.nist.gov/publications/detail/sp/800-94/final (accedido el 30 de agosto de 2022).

[15] Tim Grance (2003) Guide to Information Technology Security Services (IDPS), NIST. https://csrc.nist.gov/publications/detail/sp/800-35/final (accedido el 30 de agosto de 2022).