

1. Datos Generales de la asignatura

Nombre de la asignatura:	SEGURIDAD EN INFRAESTRUCTURA
Clave de la asignatura:	SDI-2201
SATCA¹:	2 - 3 - 5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura
<p>El contar con una infraestructura de Tecnologías de Información (TI) flexible, confiable, segura y administrable puede ayudar a una institución y/o empresa a conseguir sus objetivos de salvaguardar la información, así como los sistemas, y poder ofrecer una ventaja competitiva de sus servicios a sus usuarios.</p> <p>La información, los equipos y los servicios, que como cualquier sistema de cómputo descansa en una infraestructura de hardware, están propensos a sufrir los embates de usuarios malintencionados o problemas de administración.</p> <p>Es decir, que si una infraestructura de TI no se implementa correctamente, las empresas pueden enfrentar problemas de conectividad, disponibilidad, productividad y seguridad, como pueden ser interrupciones y vulneraciones del sistema.</p> <p>En general, es muy importante contar con una infraestructura debidamente implementada y configurada que pueda ser un factor fundamental para saber si una empresa, institución o negocio es confiable o no.</p> <p>Por lo que es de vital importancia proveer al estudiante del conocimiento, habilidades, destrezas y herramientas para planificar y prevenir la mayoría de los posibles riesgos y amenazas en los sistemas, conociendo y aplicando los procedimientos y políticas para una administración segura de la infraestructura de TI.</p>
Intención didáctica
<p>El alumno conocerá metodologías de control y protección a los recursos vitales de una empresa o institución. Proporcionando seguridad a los datos, aplicaciones, servicios y al hardware de la infraestructura de TI de la empresa o institución. Conociendo normas y estándares y aplicando las mejores prácticas recomendadas para este fin.</p>

3. Participantes en el diseño y seguimiento curricular del programa

	Participantes	Observaciones

¹ Sistema de Asignación y Transferencia de Créditos Académicos

Lugar y fecha de elaboración o revisión		
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 ITIC. Heirán Hernández Esquivel	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
El estudiante conocerá metodologías de encriptamiento, así como herramientas utilizadas para el análisis y detección de vulnerabilidades de servicios e infraestructura de TI. Además de analizar los riesgos, conocerá y aplicará las recomendaciones de estándares para proteger y asegurar los recursos computacionales de la organización o empresa.

5. Competencias previas

<ul style="list-style-type: none"> • Seleccionar, clasificar y analizar información. • Conocimiento de protocolos de redes computacionales. • Conocimientos de redes y 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. • Conocer la administración de S.O. virtualizado.
--

6. Temario

No.	Temas	Subtemas
1	Introducción	<ol style="list-style-type: none"> 1. Objetivos de la seguridad informática. 2. Conceptos de amenazas, vulnerabilidades, riesgos y controles. 3. Fundamentos de seguridad de la información <ul style="list-style-type: none"> • Cifrado simétrico y asimétrico • Algoritmos de verificación de integridad 4. Introducción al ethical hacking

2	Métodos de ataques, técnicas y protección	<ol style="list-style-type: none"> 1. Técnicas y protección de descifrado de contraseñas 2. Técnicas y protección de ingeniería social 3. Ataques y protección a nivel de red 4. Ataques y protección de aplicaciones web 5. Ataques y protección en Wireless 6. Ataques y protección en dispositivos móviles 7. Ataques y protección en internet de las cosas
3	Análisis y detección de vulnerabilidades	<ol style="list-style-type: none"> 1. Análisis de Riesgos <ol style="list-style-type: none"> a. Cualitativo b. Cuantitativo 2. Amenazas y protección de cómputo en la nube (CC, cloud computing) 3. Definición y técnicas de pruebas de penetración 4. Herramientas (monitoreo)
4	Fundamentos de virtualización	<ol style="list-style-type: none"> 1. Máquinas virtuales 2. Hipervisores 3. Creación de escenario integrador

7. Actividades de aprendizaje de los temas

Tema 1. Introducción	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Conocerá y aplica los conceptos y objetivos de la seguridad informática. - Conocerá los conceptos e identifica las diferencias entre amenaza, vulnerabilidad y riesgo. - Conocerá las técnicas de cifrado de la información. <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocerá los conceptos fundamentales de la seguridad informática. 	<ol style="list-style-type: none"> 1. Documentarse en todos los conceptos de seguridad informática, aclarando las diferencias entre algunos conceptos. 2. Investigará y conocerá las técnicas de cifrado. 3. Investigará acerca de ethical hacking o hackeo ético.

Tema 2. Métodos de ataques, técnicas y protección	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Conocerá las técnicas utilizadas para encontrar contraseñas. - Conocerá las técnicas más utilizadas para protección de activos de los sistemas de información. - Conocerá las técnicas utilizadas para protección dispositivos móviles. <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocerá los métodos y técnicas utilizadas para la protección de los activos de una empresa o institución. 	<ol style="list-style-type: none"> 1. Investigar e implementar las tácticas y técnicas utilizadas para encontrar contraseñas. 2. Investigar e implementar las tácticas y técnicas utilizadas, para proteger la información y datos de los sistemas informáticos. 3. Investigar e implementar las tácticas y técnicas utilizadas, para proteger la información sensible de los dispositivos móviles.
Tema 3. Análisis y detección de vulnerabilidades	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Conocerá los conceptos básicos del análisis de riesgos. - Conocerá las amenazas existentes en el ambiente de CC. - Conocerá la definición y técnicas utilizadas en las pruebas de intentos de intrusión a los sistemas. - Conocerá algunas herramientas que permiten sensor o monitorear el estado de los sistemas de cómputo. <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocerá y analizará las técnicas, métodos y normas utilizadas para analizar riesgos, detectar y proporcionar seguridad en 	<ol style="list-style-type: none"> 1. Investigar y conocer acerca de la norma internacional ISO 27001. 2. Investigar y conocer las tipos de amenaza que pueden afectar a los sistemas de CC. 3. Investigar, conocer e implementar las técnicas y metodologías aplicadas a la protección de datos del CC. 4. Investigar, conocer e implementar algunas de las técnicas utilizadas para pentest a los sistemas. 5. Investigar, conocer e implementar algunas de las herramientas de monitoreo de los sistemas.

<p>plataformas de CC, así como saber acerca de pentest y monitoreo de sistemas.</p>	
<p>Tema 4. Fundamentos de virtualización</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</p> <ul style="list-style-type: none"> - Conocerá la definición y concepto de máquinas virtuales y sistemas virtualizados. - Conocerá de plataformas de virtualización e hipervisores más populares. - Conocerá acerca de un escenario que integre los sistemas virtualizados. <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocerá e implementará la integración de sistemas, previamente creados en plataformas de virtualización. 	<ol style="list-style-type: none"> 1. Investigar, conocer e implementar la virtualización de sistemas. 2. Investigar, conocer e implementar hipervisores. 3. Investigar e implementar la integración de plataformas de sistemas virtualizados, así como servicios.

8. Práctica(s)

<ul style="list-style-type: none"> - Investigar sobre conceptos de vulnerabilidad, amenaza, riesgos y controles en la seguridad informática. - Investigar y conocer acerca de la norma Internacional ISO 27001, así como otras normas asociadas al análisis de riesgos. - Investigar e implementar el cifrado de datos utilizando algoritmos de cifrado simétrico y asimétrico. - Investigar e implementar la protección a los servicios y datos de los sistemas de redes contra ataques cibernéticos. - Aplicar actualizaciones y recomendaciones para un SO seguro en ambientes móviles. - Instalar y configurar un sistema de virtualización sobre un sistema host (unix/Windows). - Instalar y configurar un sistema de hipervisor para administrar, de manera remota plataformas virtualizadas.

9. Proyecto de asignatura

Llevar a cabo la instalación, configuración e integración de servicios y aplicaciones entre los sistemas de plataformas virtuales, configurando medidas de seguridad, tanto para las máquinas virtuales como para los servicios de la infraestructura.

10. Evaluación por competencias

- En un laboratorio de especialidad, elaborar las prácticas y documentación para su evaluación.
- En un sistema Linux Kali/Parrot, instalar y configurar los servicios necesarios para asegurar los servicios y datos, contra ataques cibernéticos.
- Elaborar pruebas de conexión remotas seguras entre un dispositivo móvil y aplicaciones.
- Instalar, configurar e integrar plataformas virtuales y servicios.

11. Fuentes de información

- [1] EC-COUNCIL. "Network Defense Essentials", EC-COUNCIL OFFICIAL CURRICULA. 2022. <https://www.eccouncil.org/official/> (accedido agosto 2022)
- [2] EC-COUNCIL. "Ethical Hacking Essentials", EC-COUNCIL OFFICIAL CURRICULA. 2022. <https://www.eccouncil.org/official/> (accedido agosto 2022)
- [3] IBM. <https://www.ibm.com/mx-es/topics/infrastructure> (accedido agosto 2022)
- [4] Amazon, aws. https://docs.aws.amazon.com/es_es/wellarchitected/latest/security-pillar/infrastructure-protection.html (accedido agosto 2022)
- [5] Tevault Donald. Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Kindle Edition, 2018.
- [6] Miroshnikov Andrei. Windows Security Monitoring: Scenarios and Patterns. Ed. Wiley. 2018
- [7] Nemeth Evi, Snyder Garth. Unix and Linux system administration. Kindle Edition, 2017.
- [8] Sivarajan Santhosh. Getting Started with Windows Server Security. Kindle Edition, 2015.
- [9] Estándar internacional iso27000. <http://www.iso27000.es> (accedido agosto 2022).
- [10] Cert coordination Center, "Análisis de un sistema comprometido". <https://www.sei.cmu.edu/about/divisions/cert/index.cfm> (accedido agosto 2022).

- [11] Sitio dedicado a la seguridad, Universidad Nacional Autónoma de México. <http://www.seguridad.unam.mx> (accedido agosto 2022).
- [12] Carnegie Mellon University, Software engineering Institute: Recuperación de sistemas comprometidos: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496739> (accedido agosto 2022)
- [13] "Citrix Hypervisor | Open Source Server Virtualization". Citrix Hypervisor | Open Source Server Virtualization. <https://xenserver.org/> (accedido agosto 2022).
- [14] "What is ESXI? | Bare Metal Hypervisor | ESX | VMware". VMware. <https://www.vmware.com/mx/products/esxi-and-esx.html> (accedido agosto 2022).
- [15] "Open Source Cloud Computing Infrastructure - OpenStack". OpenStack. <https://www.openstack.org/> (accedido agosto 2022).
- [16] [Defensa en profundidad - Wikipedia, la enciclopedia libre](#) (accedido agosto 2022)