1. Datos Generales de la asignatura

Nombre de la asignatura:	Gestión de amenazas
Clave de la asignatura:	CSF-2101
SATCA[1]:	3 – 2 – 5
Carrera:	Ingeniería en Informática

2. Presentación

Caracterización de la asignatura
Esta asignatura es la primera de las materias que conforman el área de la especialidad y aporta al perfil del egresado los conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario. Permite seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes. También aplica normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información. Así como también realizar actividades de auditoría y consultoría relacionadas con la función informática. Esta materia estudia proteger los sistemas de información y en redes; dar respuesta a eventos de seguridad; proteger sistemas de riesgos de ciberseguridad, amenazas y vulnerabilidades.
Intención didáctica
La asignatura se encuentra organizada en cinco temas. El primer tema explica qué es la ciberseguridad, también analiza qué son los datos de una organización y por qué deben protegerse; quiénes son los atacantes cibernéticos y lo que quieren. En general se ven todos los conceptos elementales para que se entienda el por qué es importante implementar ciberseguridad en una organización. El segundo tema, aborda la estructura del mundo de la ciberseguridad y el motivo por el que sigue creciendo, analizando el rol de los delincuentes cibernéticos y sus motivaciones. En el tercer tema se analizan las dimensiones del cubo de destrezas de ciberseguridad, que incluye los tres principios de seguridad informática. Los profesionales en ciberseguridad hacen referencia a los tres principios como la Tríada de CID. La segunda

[1] Sistema de Asignación y Transferencia de Créditos Académicos

dimensión identifica los tres estados de información o de datos. La tercera dimensión del cubo identifica los poderes de los hechiceros que proporcionan protección. Estos poderes son las tres categorías de mecanismos de las medidas de ciberseguridad. También se analiza el modelo de ciberseguridad de ISO. El modelo representa un marco de trabajo internacional para estandarizar la administración de los sistemas de información.

También, se examinan los ataques más comunes a la ciberseguridad.

El cuarto tema analiza los cuatro pasos del proceso de control de acceso como lo son: identificación, autenticación, autorización y responsabilidad. Además, también se describen los diversos modelos de control de acceso y los tipos de control de acceso. Se analizan de las diversas maneras en que los usuarios enmascaran los datos como lo son la ofuscación de datos y la esteganografía.

También se revisan los tipos de controles de integridad de datos utilizados, por ejemplo los algoritmos de hash, la técnica de “salting” y el código de autenticación de mensajes de hash. El uso de firmas y certificados digitales incorpora los controles de integridad de datos para proporcionar a los usuarios una manera de verificar la autenticación de mensajes y documentos. Por último se finaliza con un análisis de las aplicaciones de integridad de la base de datos. Tener un sistema de integridad de datos bien controlado y bien definido permite aumentar la estabilidad, el rendimiento y la capacidad de mantenimiento de un sistema de base de datos.

En el quinto tema comienza explicando el concepto de los cinco nueves. Muchos sectores deben mantener los mayores estándares de disponibilidad dado que el tiempo de inactividad puede significar literalmente una diferencia entre la vida y la muerte.

En este tema, se analizan diversos enfoques que las organizaciones pueden adoptar para cumplir sus objetivos de disponibilidad. También se hace un análisis de la recuperabilidad y la capacidad de un servidor, una red o un centro de datos para recuperarse rápidamente y continuar con la operación.

También se analizan las tecnologías, los procesos y los procedimientos que los paladines cibernéticos utilizan para proteger los sistemas, dispositivos y datos que conforman la infraestructura de red. La protección de los dispositivos es una tarea fundamental para la seguridad de la red. Implica la implementación de métodos comprobados de protección física de los dispositivos de red. Algunos de estos métodos implican el acceso administrativo seguro, el mantenimiento de las contraseñas y la implementación de comunicaciones seguras.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Revisión del 26 al 30 de abril del 2021 por parte del Tecnológico Nacional de México Campus Lerdo.	Representantes de los Institutos Tecnológicos Superiores de: Instituto Tecnológico Superior de Lerdo.	Reunión para el Análisis y Diseño por competencias de la Especialidad de "Ciberseguriad".

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Analiza y evalúa el mundo de la ciberseguridad, conociendo e identificando todas las posibles amenazas y aplica adecuadamente las técnicas y metodologías de seguridad informática para proteger sistemas de información y en redes.

5. Competencias previas

- Conceptos básicos de redes

6. Temario

No.	Temas	Subtemas
1.	Introducción a la ciberseguridad	1.1 La necesidad de la ciberseguridad 1.2 Ataques, conceptos y técnicas 1.3 Protección de sus datos y su privacidad 1.4 Protección de la organización
2.	La ciberseguridad	2.1 El mundo de la ciberseguridad 2.2 Los delincuentes cibernéticos frente a los héroes cibernéticos 2.3 Amenazas 2.4 El lado obscuro de la ciberseguridad 2.5 Creación de más héroes
3.	El cubo de destrezas de ciberseguridad	3.1 El cubo de destrezas de ciberseguridad 3.2 Triada de CID 3.3 Estados de los datos 3.4 Contramedidas de ciberseguridad 3.5 Marco de trabajo para la administración de la seguridad de TI 3.6 Malware y código malicioso 3.7 Uso de trucos

		3.8 Ataques
4.	El arte de proteger los secretos y de garantizar la integridad	4.1 Criptografía 4.2 Controles de acceso 4.3 Ocultamiento de datos 4.4 Tipos de controles de integridad de datos 4.5 Firmas digitales 4.6 Certificados 4.7 Aplicación de la integridad de la base de datos
5.	La regla de las cinco 9s y la protección	5.1 Alta disponibilidad 5.2 Medidas para mejorar la disponibilidad 5.3 Respuestas ante los incidentes 5.4 Recuperación tras un desastre 5.5 Defensa de sistemas y dispositivos 5.6 Protección del servidor 5.7 Protección de la red 5.8 Seguridad física

7. Actividades de aprendizaje de los temas

Introducción a la ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): • Aprenderá los aspectos básicos de estar seguro en línea, así como los diferentes tipos de malware y ataques, y cómo las organizaciones se protegen contra ellos. Genéricas: • Capacidad de abstracción, análisis y síntesis. • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Compromiso con la calidad.	• Realizar una búsqueda de las opciones de trabajo en el área de ciberseguridad • Realizar una comparación de datos con un hash. • Aprender a crear y almacenar contraseñas seguras. • Conocer los diferentes respaldos de datos en un almacenamiento externo. • Describir su propio comportamiento riesgoso en línea.
La ciberseguridad	
Competencias	Actividades de aprendizaje

Específica(s): • Analizar el rol de los delincuentes cibernéticos y sus motivaciones y examinar los ataques más comunes a la ciberseguridad. Genéricas: • Capacidad de abstracción, análisis y síntesis. • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Compromiso con la calidad.	• Identificar mediante modelo de un mundo cibernético los diferentes roles que tienen los delincuentes en la red • Conocer la comunicación que existe en un mundo cibernético • Mediante ejemplos llevar a cabo la identificación de amenazas
El cubo de destrezas de ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar el cubo de las destrezas de la ciberseguriad, así como el modelo de la ciberseguridad ISO • Identificar las amenazas de malware y de código malicioso • Examinar los ataques más comunes a la ciberseguridad Genéricas: • Capacidad de abstracción, análisis y síntesis. • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Compromiso con la calidad.	• Conocer el mundo de los profesionales en el área de ciberseguridad • Conocer el cifrado de archivos y datos • Conocer la autenticación, autorización y auditoria • Identifica los controles de integridad de datos y archivos • Diferenciar los protocolos WEP/WPA2 PSK/WPA2 RADIUS • Clasificar la amenazas y vulnerabilidades
El arte de proteger los secretos y de garantizar la integridad	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar los cuatro pasos del proceso de control de acceso: identificación, autenticación, autorización y responsabilidad. Además de describir los diversos modelos de control de acceso y los tipos de control de acceso. • Analizar los tipos de controles de integridad de datos utilizado	• Describir el modo de transporte de VPN • Describir el modo de túneles VPN • Definir y saber cómo usar la esteganografia • Clasifica los diferentes tipos de decodificación de contraseñas • Describir la importancia del uso de firmas digitales

• Aplicar el uso de firmas y certificados digitales Genéricas: • Capacidad de abstracción, análisis y síntesis. • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Compromiso con la calidad.	
La regla de las cinco 9s y la protección	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar diversos enfoques que las organizaciones pueden adoptar para cumplir sus objetivos de disponibilidad • Analizar las tecnologías, los procesos y los procedimientos se utilizan para proteger los sistemas, dispositivos y datos que conforman la infraestructura de red. Genéricas: • Capacidad de abstracción, análisis y síntesis. • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Compromiso con la calidad.	• Clasificar los Firewalls que se pueden implementar en un servidor y ACL del router

8. Práctica(s)

- Búsqueda de trabajo en el área de ciberseguridad
- Comparar datos con un hash
- Crear y almacenar contraseñas seguras
- Crear respaldo de datos en un almacenamiento externo
- Descubrir su propio comportamiento riesgoso en línea
- Creación de un mundo cibernético
- La comunicación de un mundo cibernético
- Identificación de amenazas
- Explorar el mundo de los profesionales en el área de ciberseguridad
- Explorar el cifrado de archivos y datos
- Explorar la autenticación, autorización y auditoria

- Usar los controles de integridad de datos y archivos
- Configurar los protocolos WEP/WPA2 PSK/WPA2 RADIUS
- Detección de amenazas y vulnerabilidades
- Configuración del modo de transporte de VPN
- Configuración del modo de túneles VPN
- Uso de la esteganografía
- Decodificación de contraseñas
- Uso de firmas digitales
- Firewalls del servidor y ACL del router

9. Proyecto de asignatura

Configurar un router, cargar y descargar archivos mediante FTP, conectarse de manera segura a un sitio remoto mediante una VPN y asegurar un router.

10. Evaluación por competencias

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

- Evaluación diagnóstica.
- Investigación en diversas fuentes de información.
- Desarrollo de actividad(es) y reporte de prácticas.
- Exposición de temas específicos.
- Exámenes teóricos - prácticos que demuestre parte del conocimiento adquirido durante la asignatura.

11. Fuentes de información

- Stuppi, J., Santos, O.; (2015), *CCNA Security 210-260;* Ciscopress.com
- Chan, B. (2020); *Seguridad Cibernética*
- Sallis, E.; Caracciolo, C.; Rodríguez M. (2010) *Ethical Hacking. Un enfoque metodológico para profesionales.* Alfaomega
- Bejtlich, R. (2016); *The Practice of network security monitoring: Understanding incident detection and response*
- Rodriguez, N. (2020); *¡Ciber-conciénciate!: Ni sabemos toda la verdad ni somos conscientes del verdadero peligro que nos acecha.* Independently published
- Sing, S. (1999);*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Fourth Estate y Doubleday

- Mitnick, K. (2017); *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.* Little, Brown and Company
- Hadnagy, C. (2018); *Social Engineering: The Science of Human Hacking.*Wiley