1. Datos Generales de la asignatura

Nombre de la asignatura:	**Introducción a la Ciberseguridad**
Clave de la asignatura:	XXXX
SATCA[1]:	**2-3-5**
Carrera:	**Ingeniería en Tecnologías de la Información y telecomunicaciones**

2. Presentación

Caracterización de la asignatura

Este curso explora las tendencias cibernéticas, las amenazas y cómo permanecer seguro en el ciberespacio a fin de proteger los datos personales y empresariales.

Este le brindará conocimientos básicos y de concientización en habilidades específicas solicitadas como: pruebas de penetración, cibercrimen, privacidad de datos, firewall, arquitectura de seguridad, entre otros.

La materia provee al alumno las bases para:
- Conocer los elementos de identificación, protección, detección, respuesta y recuperación ante una amenaza en ciberseguridad y alinear los recursos que ofrecen
las tecnologías de la información.
- Dirigir desde una visión integral la gestión de los procesos asociados a seguridad de la información para prevenir ataques por IP.
- Saber cómo optimizar los flujos de gestión operativa de red con base en las vulnerabilidades de la dirección MAC y ataques de la infraestructura.
- Conocer cómo proteger los datos sensibles frente a las amenazas que pueden materializarse por parte de los adversarios usando sistemas contra hacking.
- Tener conocimiento de las principales herramientas, metodologías y servicios más adecuados para el resguardo de información en bases de datos.

Intención didáctica

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Este curso está diseñado para explorar la ciberseguridad como especialización potencial en una carrera de TI.

El material del curso lo ayudará a desarrollar las aptitudes necesarias para realizar lo siguiente:

- Comprender la importancia del comportamiento en línea seguro.
- Describir los diferentes tipos de malware y ataques.
- Describir las estrategias de protección que usan las organizaciones contra los ataques

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Estudios Superiores de Zamora en Agosto de 2021.	Integrantes de las Academias de Ingeniería en Sistemas Computacionales e Ingeniería en Tecnologías de la Información y Comunicaciones.	Elaboración de las nuevas especialidades para los planes de estudio 2010.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Competencias específicas Desarrollar la capacidad de análisis, diseño y evaluación de sistemas usando diferentes tecnologías de comunicaciones, dispositivos, y software de programación para ciberseguridad. **Competencias genéricas** **Competencias instrumentales:** - Capacidad de abstracción, análisis y síntesis. - Conocimiento sobre el área de estudio y la profesión. - Capacidad de comunicación oral y escrita. - Habilidades en el uso de las tecnologías de la información y de la comunicación. - Habilidades para buscar, procesar y analizar información, procedente de

fuentes
diversas.
- Capacidad para identificar, planear y resolver problemas.
- Capacidad para tomar decisiones.

Competencias interpersonales:
- Capacidad crítica y autocrítica.
- Capacidad de trabajo en equipo
- Habilidades interpersonales.

Competencias sistémicas:
- Capacidad de aplicar los conocimientos en la práctica.
- Habilidades de investigación.
- Capacidad de aprender y actualizarse permanentemente
- Capacidad creativa.

5. Competencias previas

- Tener conocimientos de redes de computadoras.
- Conocer aspectos básicos de sistemas operativos.
- Conocer de arquitectura de computadoras.
- Tener conocimientos de bases de datos.
- Conocer metodologías básicas para realizar una investigación.

6. Temario

No.	Temas	Subtemas
1	Introducción a ciberseguridad	1.1 Introducción 1.2 Datos personales 1.3 Datos de la organización 1.4 Atacantes y profesionales de la ciberseguridad 1.5 Guerra cibernética

		1.6 Ingresar el tema de Ética 1.7 Cuestiones legales en ciberseguridad
2	Ataques, conceptos y técnicas	2.1 Análisis de un ciberataque 2.1.1 Aprovechamiento de las vulnerabilidades 2.1.2 Tipos de vulnerabilidades 2.1.3 Tipos de malware y síntomas 2.1.4 Métodos de infiltración 2.1.5 Denegación de servicio 2.2 El panorama de la ciberseguridad 2.2.1 Ataque combinado 2.2.2 Reducción del impacto 2.3 Laboratorio
3	Protección de los datos y de la privacidad	3.1 Protección de sus datos 3.1.1 Protección de dispositivos y red 3.1.2 Mantenimiento de datos 3.2 Protección de la privacidad en línea 3.2.1 Autenticación sólida 3.2.2 Compartir información de forma segura 3.3 Laboratorio
4	Protección de la organización	4.1 Firewalls 4.1.1 Tipos 4.1.2 Dispositivos 4.1.3 Detección 4.2 Comportamiento en la ciberseguridad 4.2.1 Botnet 4.2.2 Proceso de ataque 4.2.3 Seguridad 4.2.4 Ciberataques 4.3 Cisco para la ciberseguridad 4.3.1 CSIRT (Equipo de respuesta a incidentes de seguridad informática) 4.3.2 Libro de estrategias 4.3.3 Herramientas 4.3.4 IDS e IPS 4.4 Caso práctico

7. Actividades de aprendizaje de los temas

1. Introducción a ciberseguridad	
Competencias	Actividades de aprendizaje

Específicas: • Identifica el estado laboral actual para los profesionales en el área de la seguridad informática • Identifica el impacto de un ataque a una empresa • Analiza el perfil de los atacantes cibernéticos Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas.	• Investigar las ofertas de trabajo en ciberseguridad • Investigar las características de seguridad que utilizan las organizaciones para mantener los datos seguros • Investigar el impacto de un ataque de ciberseguridad en una organización • Práctica de laboratorio: comparar datos con un hash • Investigar casos recientes de violaciones de seguridad • Describir el perfil de los atacantes cibernéticos
2. Ataques, conceptos y técnicas	
Competencias	Actividades de aprendizaje
Específicas: • Identifica tipos de vulnerabilidades • Analiza métodos de infiltración • Identifica los conceptos: DoS, DDoS y Envenenamiento SEO • identifica las características de un ataque combinado Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas.	• Investigar los tipos de malware • Investigar ejemplos reales de: ingeniería social y suplantación de identidad • Realizar una lluvia de ideas sobre acciones a tomar en una empresa para reducir el impacto de un ataque
3. Protección de los datos y de la privacidad	
Competencias	Actividades de aprendizaje
Específicas: • Identifica y aplica métodos para proteger los dispositivos y la red • Realiza encriptación de contenido para proteger datos • Realiza respaldo de datos	• Investigar: ¿Quién posee sus datos?, analizar la propiedad de los datos cuando estos no se almacenan en un sistema local. • Dinámica: Descubre su propio comportamiento riesgoso en línea • Práctica de laboratorio: crear y almacenar

• Realiza eliminación permanente de datos • Identifica buenas prácticas para el comportamiento en redes sociales Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas.	contraseñas seguras • Práctica de laboratorio: respaldar los datos en un almacenamiento externo
4. Protección de la organización	
Competencias	Actividades de aprendizaje
Específicas: • Identifica malware y ataques en tiempo real • Analiza las características de la seguridad basada en el comportamiento • Identifica las características, ventajas y desventajas de los IDS e IPS Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas.	• Investigar los tipos de Firewall • Investigar herramientas para realizar escaneo de puertos describiendo características, ventajas y desventajas • Investigar los conceptos: Botnet, Kill Chain y NetFlow • Investigar ejemplos de herramientas IDS e IPS

8. Práctica(s)

- Detección de vulnerabilidades
- Ejemplos de ingeniería social
- Práctica DoS

- Crear y almacenar contraseñas seguras
- Crear respaldos de datos
- Eliminar datos de forma permanente

9. Proyecto de asignatura

Realizar un caso práctico que involucre las buenas prácticas y herramientas de prevención y detección de ataques abordadas en la asignatura para con ello reforzar los conocimientos y habilidades adquiridos.

10. Evaluación por competencias

La evaluación de la asignatura se hará con base en siguiente desempeño:

- Reportes escritos de las observaciones hechas durante las actividades, así como de las conclusiones obtenidas de dichas observaciones.
- Información obtenida durante las investigaciones solicitadas plasmada en documentos escritos.
- Exámenes para comprobar el manejo de aspectos teóricos - declarativos y de habilidades y destrezas.
- Resolución de tareas, trabajos prácticas relacionadas con el tema en cuestión, haciendo uso del cómputo en la nube.
- Participaciones y actitudes del estudiante (responsabilidad, cumplimiento en tiempo y forma, trabajo en equipo, exposición de temas, etc.)
- Integración del portafolio de evidencias del curso (tareas, trabajos, prácticas, exámenes, entre otros).
- Desarrollo de proyectos de aplicación real debidamente documentado que describa la experiencia concreta y conclusiones obtenidas, para ser expuesto ante el grupo.

11. Fuentes de información

1. Arboledas, D. (2014). Backtrach 5: Hacking de redes inalámbricas. (A. Grupo, Ed.) (Primera ed). 2. Carballar, J. (2006). Firewall- la seguridad de la banda ancha. (A. Grupo,

Ed.) (Primera ed).

3. Gómez, Á. (2011). Enciclopedia de la seguridad informática. (A. Grupo, Ed.) (Segunda ed).

4. Picouto, F., Lorente, I., García-Morán, J., & Ramos, A. (2008). Hacking y seguridad en internet. (A. Grupo, Ed.) (Primera ed).

5. Zemánek, J. (2005). Cracking sin secretos- ataque y defensa de software. (A. Grupo, Ed.) (Primera ed).

6. L. Joyanes Aguilar, Industria 4.0-la cuarta revolución industrial. Alfaomega, 2017