1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos de Ciberseguridad
Clave de la asignatura:	CBD-2417
SATCA[1]:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Aporta el perfil del Ingeniero en Ciberseguridad las siguientes habilidades:

- Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
- Evalúa riesgos de seguridad y vulnerabilidad en aplicaciones o instalaciones de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo con metodologías, normas y estándares de excelencia.
- Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.
- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.
- Propone soluciones para proteger la transmisión y almacenamiento de información sensible dentro de un área funcional o técnica, a partir de marcos de referencia con excelencia, vanguardia e innovación social aplicando mejores prácticas del mercado.
- Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza eficientemente los recursos, si se atienden los principios de no discriminación, Inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.
- Implementa soluciones metodológicas y controles de seguridad en el ciclo de vida del desarrollo de software que permitan la reducción de vulnerabilidades y la inclusión de mejores prácticas de seguridad, con una perspectiva de responsabilidad social.

Los ingenieros de ciberseguridad construyen tecnologías que mantienen segura la arquitectura informática. Su responsabilidad es anticiparse a las vulnerabilidades de la red, lo que requiere crear firewalls, ejecutar programas de encriptación y actualizar el software.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Intención didáctica
Se organiza el temario en cuatro temas agrupando los contenidos conceptuales de la asignatura en la primera unidad donde se abordan los temas referentes la necesidad de la ciberseguridad. En el segundo tema se estudia y analiza los ataques, conceptos y técnicas. Se incluye un tercer tema que se destina a la protección de los datos y su privacidad. En el cuarto tema se establece la protección en la organización y finalmente en el quinto tema define el futuro relacionado con la ciberseguridad. El enfoque sugerido para la materia es ofrecer escenarios de trabajo y problemática distinta, ya sean construidos o virtuales. En el curso de las actividades programadas es importante que el estudiante valore las actividades que realiza y entienda que está construyendo su futuro y actúe de manera profesional.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.
Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad

Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Explora las tendencias cibernéticas, las amenazas para permanecer seguro en el ciberespacio a fin de proteger los datos personales y empresariales.

5. Competencias previas

- Utiliza el razonamiento lógico utilizando sistemas de cómputo.

6. Temario

No.	Temas	Subtemas
1	Introducción a la ciberseguridad.	1.1. Antecedentes históricos y aplicaciones. 1.2. Datos personales. 1.3. Datos de la organización. 1.4. Ataques y profesionales de la ciberseguridad. 1.4.1. Perfil del atacante cibernético 1.4.2. Tipos de atacantes 1.5. Guerra cibernética. 1.5.1. Qué es la guerra cibernética 1.5.2. Propósito de la guerra cibernética 1.6. Penetration Testing 1.6.1. Pasos en las pruebas de Intrusión 1.6.2. Acuerdos iniciales, Alcance, Fechas de Entrega 1.6.3. Análisis, Explotación y Post Explotación de vulnerabilidades 1.6.4. Reporte Técnico
2	Ataques, conceptos y técnicas.	2.1. Análisis de un ciberataque. 2.1.1. Aprovechamiento de las vulnerabilidades de seguridad. 2.1.2. Tipos de vulnerabilidades de seguridad. 2.1.3. Tipos de Malware y síntomas. 2.1.4. Métodos de infiltración.

		2.1.5. Denegación de servicios. 2.2. El panorama de la ciberseguridad. 2.2.1. Ataque combinado. 2.2.2. Reducción del impacto
3	Protección de los datos y su privacidad.	3.1. Protección de sus datos. 3.1.1. Protección de dispositivos y la red. 3.1.2. Mantenimiento de datos. 3.2. Protección de la privacidad en línea. 3.2.1. Autenticación sólida, 3.2.2. ¿Se comparte demasiada información?
4	Sistemas de detección y prevención de intrusos.	4.1. Firewalls. 4.1.1. Tipos de firewalls. 4.1.2. Dispositivos de seguridad. 4.1.3. Detección de ataques en tiempo real. 4.1.4. Detección de malware 4.2. Comportamiento que seguir en la ciberseguridad. 4.2.1. BotNet. 4.2.2. Cadena de eliminación o proceso de ataque. 4.2.3. Seguridad basada en el comportamiento. 4.2.4. NetFlow y los ciberataques. 4.3. Otros enfoques de la ciberseguridad. 4.3.1. CSIRT 4.3.2. Libro de estrategias de ciberseguridad. 4.3.3. Herramientas para prevención y detección de incidencias. 4.3.4. IDS e IPS

7. Actividades de aprendizaje de los temas

1. Introducción a la ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Conocer los conceptos sobre la ciberseguridad informática. Habilidad en el uso de tecnologías de información y comunicación. *Genérica(s):* ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad para trabajar en equipo interdisciplinario. ● Capacidad crítica y autocrítica. ● Habilidades interpersonales. ● Capacidad de aplicar los conocimientos en la práctica. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Investigar las diferencias fundamentales y específicas de la seguridad informática para una comunicación confiable. ● Asociar el funcionamiento de los componentes básicos del contemplados en la ciberseguridad. ● Buscar y seleccionar información sobre los diferentes modelos de transición en la comunicación de redes.

2. Ataques conceptos y técnicas.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer y aplicar las diversas formas de conexión en el entorno de red para implementar prototipos. *Genérica(s):* ● Habilidad en el uso de tecnologías de información y comunicación. ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad para trabajar en equipo interdisciplinario. ● Capacidad crítica y autocrítica. ● Habilidades interpersonales. ● Capacidad de aplicar los conocimientos en la practica ● Liderazgo ● Búsqueda de logro. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Investigar las diferentes formas de conectividad en el entorno de red y formalizar lo investigado. ● Describir los distintos tipos de conexión y efectuar ejercicios básicos.

3. Protección de los datos y su privacidad.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer y comprender los procesos empresariales existentes. *Genérica(s):* ● Habilidad en el uso de tecnologías de información y comunicación. ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad para trabajar en equipo interdisciplinario. ● Capacidad crítica y autocrítica. ● Habilidades interpersonales. ● Capacidad de aplicar los conocimientos en la practica ● Liderazgo ● Búsqueda de logro. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Identificar proveedores y clientes, así sus necesidades. ● Establecer el programa y los pasos del proceso para crear y entregar una oferta. ● Realizar casos de usos aplicados en los diferentes sectores.

4. Sistemas de detección y prevención de intrusos.	
Competencias	Actividades de aprendizaje
Específica(s): Investigar, establecer y definir las diversas estrategias de seguridad en tiempo real. *Genérica(s):* ● Habilidad en el uso de tecnologías de información y comunicación. ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad para trabajar en equipo interdisciplinario. ● Capacidad crítica y autocritica. ● Habilidades interpersonales. ● Capacidad de aplicar los conocimientos en la práctica. ● Liderazgo. ● Búsqueda de logro. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Enlistar para identificar las principales arquitecturas de seguridad para el mejor funcionamiento del entorno. ● Analizar el funcionamiento de las diversas estrategias de seguridad, utilizando un Software que permita obtener datos respecto al funcionamiento de los programas de seguridad.

8. Práctica(s)

- Generar el glosario de conceptos clave de cada tema.
- Desarrollar actividades interactivas y de laboratorio correspondientes a cada unidad.
- Desarrollar ejercicios básicos mediante software de aplicación y optimización de recursos.
- Instalar un laboratorio de pruebas virtual para las pruebas
- Elaboración de diferentes escenarios de entorno de red, mediante el simulador Packet Tracer en su versión vigente.
- Verificar mediante el simulador Packet Tracer las prácticas de laboratorio asignadas.

9. Proyecto de asignatura

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

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de los saberes, habilidades y destrezas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación de saberes, habilidades y destrezas

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

- Reportes escritos de prácticas realizadas en clase, así como de las conclusiones obtenidas.
- Análisis de la información obtenida durante las investigaciones solicitadas en documentos escritos.
- Descripción de experiencias concretas que podrían realizarse adicionalmente.
- Exámenes escritos para comprobar el manejo de aspectos teóricos y declarativos.

11. Fuentes de Información

1. https://www.netacad.com/es/
2. curso: Introduccion to Cybersecurity.
3. Peltier, T. R. (2010). Information security risk analysis (3rd ed.). CRC Press/Auerbach Publications.
4. Stallings, W. (2000). Network security essentials: Applications and standards (2nd ed.). Prentice Hall.
5. McClure, S., Scambray, J., & Kurtz, G. (2007). Hacking exposed: Network security secrets & solutions (6th ed.). McGraw-Hill.
6. Navarro Isla, Jorge. (2005). Tecnologías de la información y de las comunicaciones: Aspectos legales (Primera edición). Editorial Porrúa.
7. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.