



1. Datos Generales de la asignatura

Nombre de la asignatura:	Tópicos avanzados de ciberseguridad
Clave de la asignatura:	CBD-2432
SATCA¹:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:

- Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.
- 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 a 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.
- Gestiona planes y proyectos de seguridad de la información de acuerdo con las necesidades del negocio, considerando riesgos y contingencias, promoviendo el cumplimiento de los principios de no discriminación, inclusión, equidad social, políticas, normas y acuerdos de nivel de servicio.
- 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.

¹ Sistema de Asignación y Transferencia de Créditos Académicos



La asignatura "tópicos avanzados de ciberseguridad" es fundamental en el programa de ingeniería de ciberseguridad al comprender a los estudiantes los desafíos y soluciones más actuales en seguridad digital. En un contexto donde las amenazas cibernéticas evolucionan constantemente, esta asignatura se destaca por su relevancia en la formación de profesionales capacitados para enfrentar los desafíos emergentes en seguridad de la información. Al abordar temas como la seguridad en dispositivos móviles, entornos en la nube, aplicaciones basadas en blockchain y los retos emergentes en ciberseguridad, esta asignatura no solo proporciona a los estudiantes una base sólida de conocimientos técnicos, sino que también les capacita para desarrollar habilidades prácticas y estratégicas necesarias para proteger activos digitales y salvaguardar la integridad, confidencialidad y disponibilidad de la información en cualquier entorno tecnológico

Intención didáctica

La asignatura "tópicos avanzados de ciberseguridad" pretende proporcionar a los estudiantes una comprensión profunda de los desafíos y soluciones contemporáneas en la ciberseguridad, preparándolos para abordar las amenazas digitales en entornos tecnológicos complejos. En este sentido, se busca desarrollar habilidades y conocimientos especializados que les permitan diseñar, implementar y evaluar estrategias efectivas de seguridad cibernética.

El primer tema, se enfoca en la seguridad en dispositivos móviles, donde los estudiantes aprenderán a proteger la información y la privacidad en dispositivos móviles, considerando las amenazas y vulnerabilidades específicas de estos dispositivos.

El segundo tema se centra en la seguridad en entornos en la nube y virtualización, abordando la protección de datos y sistemas en entornos virtualizados y en la nube.

El tercer tema introduce el uso de blockchain para la ciberseguridad, explorando cómo esta tecnología puede fortalecer la gestión de identidad y la protección de datos.

Finalmente, el cuarto tema examina los retos emergentes en ciberseguridad, como la inteligencia artificial, el internet de las cosas, computación cuántica y la infraestructura crítica, preparando a los estudiantes para enfrentar las amenazas futuras con una perspectiva proactiva y adaptativa. En conjunto, esta asignatura busca formar profesionales capaces de liderar y gestionar la seguridad cibernética en un entorno tecnológico en constante evolución.

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
<ul style="list-style-type: none">Analizar, diseñar, implementar y evaluar soluciones integrales de ciberseguridad en diversos entornos tecnológicos, incluyendo dispositivos móviles, entornos en la nube, aplicaciones basadas en blockchain y enfrentando retos emergentes en el campo de la ciberseguridad.

5. Competencias previas

<ul style="list-style-type: none">Comprende y contextualiza los principios fundamentales, métodos y aplicaciones de la inteligencia artificial para evaluar críticamente su impacto, posibilidades y limitaciones en diversos contextos; fomenta una aproximación ética y responsable en el desarrollo e implementación de soluciones tecnológicas innovadoras en el campo de la ingeniería de inteligencia artificial.Diseña sistemas y técnicas específicas para asegurar los sistemas informáticos de la empresa y diversos dispositivos.Diseña y desarrolla soluciones criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.



6. Temario

No.	Temas	Subtemas
1	Seguridad en dispositivos móviles.	<ul style="list-style-type: none">1.1. Amenazas y vulnerabilidades en dispositivos móviles.1.2. Pruebas de penetración y evaluación de seguridad en aplicaciones móviles.1.3. Gestión de la seguridad en dispositivos móviles.1.4. Protección de datos y privacidad en dispositivos móviles.1.5. Tendencias y desafíos en seguridad móvil.
2	Seguridad en entornos en la nube.	<ul style="list-style-type: none">2.1. Arquitectura y modelos de servicio en la nube.2.2. Problemas y ataques comunes de seguridad en entornos en la nube.2.3. Gestión de identidad y acceso en entornos en la nube.2.4. Herramientas y tecnologías para gestionar la seguridad en la nube.
3	Blockchain	<ul style="list-style-type: none">3.1. Fundamentos de Blockchain.3.2. Seguridad en Blockchain: consenso, privacidad e inmutabilidad.3.3. Aplicaciones de Blockchain en la seguridad de la Identidad.3.4. Blockchain en la detección y prevención de fraude.3.5. Contratos inteligentes.3.6. Desafíos y limitaciones de seguridad en la implementación de Blockchain.
4	Retos emergentes de la ciberseguridad.	<ul style="list-style-type: none">4.1. Ataques de seguridad en aplicaciones basadas en inteligencia artificial.4.2. Problemas de seguridad en entornos autónomos e inteligentes.4.3. Seguridad en entornos de realidad virtual y aumentada.4.4. Retos de seguridad en la computación post cuántica.4.5. Tendencias futuras en ciberseguridad.



7. Actividades de aprendizaje de los temas

1. Seguridad en dispositivos móviles	
Competencias	Actividades de aprendizaje
<p>Específica(s): Diseñar, implementar y evaluar estrategias de seguridad efectivas para dispositivos móviles, que aborden amenazas y vulnerabilidades comunes en el ecosistema móvil.</p> <p>Genérica(s):</p> <ul style="list-style-type: none"> • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. <p>Transversal(es):</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Realizar un estudio de casos sobre amenazas específicas en dispositivos móviles y proponer estrategias de mitigación. • Configurar herramientas de seguridad en dispositivos móviles y realizar pruebas de vulnerabilidad. • Elaborar políticas de seguridad para dispositivos móviles, considerando aspectos como el uso de contraseñas, la autenticación multifactor y la gestión de dispositivos. • Realizar simulaciones de ataques de phishing, malware o robo de información en dispositivos móviles y evaluar la respuesta de seguridad.
2. Seguridad en entornos en la nube	
Competencias	Actividades de aprendizaje
<p>Específica(s): Diseñar e implementar soluciones de seguridad robustas en entornos en la nube, comprendiendo los modelos de servicio en la nube, las tecnologías y las mejores prácticas de gestión de riesgos para proteger los activos digitales en estos entornos.</p>	<ul style="list-style-type: none"> • Configurar y asegurar una instancia en la nube utilizando prácticas recomendadas de seguridad. • Utilizar herramientas de escaneo de vulnerabilidades para identificar y mitigar riesgos en entornos virtualizados. • Implementar soluciones de gestión de identidad y acceso en un entorno cloud, como la federación de identidad o la autenticación multifactor. • Analizar brechas de seguridad recientes en servicios en la nube y proponer medidas de seguridad preventivas.



<p>Genérica(s):</p> <ul style="list-style-type: none">• Capacidad de análisis, síntesis y abstracción.• Capacidad de comunicación oral y escrita.• Habilidad en el uso de tecnologías de información y comunicación.• Trabajo en equipo.• Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad. <p>Transversal(es):</p> <ul style="list-style-type: none">• 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.		<ul style="list-style-type: none">• Configurar y evaluar firewalls virtuales para proteger redes y sistemas en entornos de nube.
3. Blockchain		
Competencias		Actividades de aprendizaje
<p>Específica(s): Evaluar, diseñar e implementar soluciones de seguridad basadas en tecnología Blockchain, comprendiendo sus fundamentos y aplicaciones en seguridad de la información y sus implicaciones en la gestión de identidad, prevención de fraude y protección de datos.</p> <p>Genérica(s):</p> <ul style="list-style-type: none">• Capacidad de análisis, síntesis y abstracción.• Capacidad de comunicación oral y escrita.		<ul style="list-style-type: none">• Diseñar y programar contratos inteligentes para aplicaciones de seguridad basadas en blockchain.• Realizar una simulación de transacciones seguras utilizando una red blockchain y analizar la resistencia a manipulaciones.• Explorar herramientas y protocolos para la gestión de identidad descentralizada en blockchain y realizar pruebas de concepto.• Investigar y presentar casos de uso reales de blockchain en la industria de la ciberseguridad.• Desarrollar una aplicación segura utilizando tecnologías blockchain y evaluar su robustez frente a ataques.



<ul style="list-style-type: none">• Habilidad en el uso de tecnologías de información y comunicación.• Trabajo en equipo. <p>Transversal(es):</p> <ul style="list-style-type: none">• 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.	
4. Retos emergentes de la ciberseguridad	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <ul style="list-style-type: none">• A proponer soluciones innovadoras para hacer frente a los desafíos emergentes en ciberseguridad, incluyendo inteligencia artificial, internet de las cosas, ransomware, seguridad en infraestructuras críticas y protección de la privacidad, desarrollando así una visión integral y proactiva de la ciberseguridad. <p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Capacidad de análisis, síntesis y abstracción.• Capacidad de comunicación oral y escrita.• Habilidad en el uso de tecnologías de información y comunicación.• Trabajo en equipo.	<ul style="list-style-type: none">• Realizar investigaciones sobre las últimas tendencias y amenazas emergentes en ciberseguridad y presentar informes.• Organizar y participar en una mesa redonda con profesionistas expertos en ciberseguridad para discutir retos y estrategias frente a amenazas emergentes.• Llevar a cabo ejercicios de simulación de incidentes cibernéticos para practicar la detección, respuesta y recuperación.• Presentar y discutir escenarios hipotéticos de amenazas emergentes y posibles contramedidas, fomentando el pensamiento crítico y la creatividad en la resolución de problemas.



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.

8. Práctica(s)

- Identificar y analizar las vulnerabilidades y riesgos en un entorno tecnológico complejo.
- Desarrollar e implementar estrategias efectivas para mitigar los riesgos y fortalecer la seguridad del entorno.
- Evaluar la efectividad de las soluciones de seguridad implementadas y realizar ajustes según sea necesario.

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 de la asignatura debe de ser continua, sumativa y formativa, por lo que debe de considerarse el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Capacidad de análisis, síntesis, abstracción, de organizar y planificar, comprobado mediante las evidencias de aprendizaje tales como: Reportes, ensayos y prácticas, solución de ejercicios extra clase, actividades de investigación, elaboración de modelos o prototipos.
- Resolución de problemas con apoyo de software.

11. Fuentes de Información

1. Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2020). Cloud Computing with Security. Springer International Publishing.
2. Rakshit, S. K. (2022). Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition). In Google Books. BPB Publications.
3. Artificial Intelligence and Blockchain for Future Cybersecurity Applications. (2021). In Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, & I. Romdhani (Eds.), Studies in Big Data. Springer International Publishing.
4. Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (2020). Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. In Google Books. CRC Press.
5. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). *Modelo curricular por competencias*. ANIEI.