1. Datos Generales de la asignatura

Nombre de la asignatura:	Aspectos legales, éticos y sociales en ciberseguridad
Clave de la asignatura:	CBD-2407
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 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.
- 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.

Aborda la intersección entre la ciberseguridad, la ética, la legislación y los impactos sociales. Esta asignatura se relaciona estrechamente con el perfil de egreso del estudiante de ingeniería en ciberseguridad, al proporcionar una comprensión integral de los desafíos éticos, legales y sociales que enfrentan los profesionales en este campo emergente.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

A su vez tiene la capacidad para desarrollar en los estudiantes habilidades críticas de análisis ético y legal, así como una comprensión profunda de las implicaciones sociales de la ciberseguridad. Al finalizar la asignatura, los estudiantes serán capaces de identificar y resolver dilemas éticos específicos en el ámbito de la ciberseguridad, interpretar y aplicar la legislación nacional e internacional pertinente, y evaluar el impacto social de los ataques cibernéticos.

La importancia de la asignatura radica en su capacidad para preparar a los futuros profesionales de la ciberseguridad para enfrentar los desafíos complejos y dinámicos del entorno digital actual. La comprensión de los aspectos legales, éticos y sociales de la ciberseguridad es fundamental para garantizar prácticas responsables y sostenibles en la protección de datos, la privacidad digital y la seguridad de la infraestructura crítica.

Esta asignatura se relaciona estrechamente con otras asignaturas del plan de estudios, como Seguridad Informática, Criptografía y Seguridad en Redes y Gestión de Riesgos en Ciberseguridad.

Intención didáctica

Los contenidos serán abordados de manera estructurada y progresiva, comenzando con una introducción a los fundamentos éticos y legales de la ciberseguridad y avanzando hacia temas más complejos como la responsabilidad profesional, la privacidad en la era digital y la diplomacia cibernética. Se dedicará especial atención al análisis de casos prácticos y situaciones reales para ilustrar los conceptos teóricos y promover la reflexión crítica.

Los contenidos serán tratados con un enfoque práctico, orientado a la aplicación de los conocimientos adquiridos en situaciones reales. Se fomentará el análisis crítico y la resolución de problemas, así como la capacidad para trabajar en equipo y comunicar eficazmente las ideas.

El papel que debe desempeñar el docente en el desarrollo de la asignatura es el de facilitador del aprendizaje, proporcionando orientación, apoyo y retroalimentación a los estudiantes en su proceso de aprendizaje. El docente actuará como guía en la exploración de los temas tratados, estimulando el debate y la reflexión crítica, y promoviendo un ambiente de aprendizaje colaborativo y respetuoso.

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
• Desarrollar habilidades para identificar y resolver dilemas éticos, evaluar el impacto social de los ataques cibernéticos y aplicar la legislación nacional e internacional en ciberseguridad para garantizar el cumplimiento normativo y la protección de datos.

5. Competencias previas

• Explora las tendencias cibernéticas, las amenazas para permanecer seguro en el ciberespacio a fin de proteger los datos personales y empresariales.

6. Temario

No.	Temas	Subtemas
1	Ética en la ciberseguridad	1.1. Fundamentos de ética y su aplicación en el contexto de la ciberseguridad. 1.2. Principios éticos en la práctica de la ciberseguridad. 1.3. Responsabilidad profesional y dilemas éticos en la toma de decisiones. 1.4. Casos de estudio y análisis de situaciones éticas en la ciberseguridad
2	Aspectos sociales de la ciberseguridad	2.1. Impacto social de los ataques cibernéticos y la vulnerabilidad de la infraestructura crítica. 2.2. Privacidad en la era digital: riesgos y desafíos. 2.3. Educación y concienciación pública sobre ciberseguridad. 2.4. Retos sociales emergentes
3	Marco legal y regulatorio	3.1. Cibercrimen (delitos informáticos) 3.2. Legislación nacional relacionada con la ciberseguridad. 3.3. Responsabilidad legal de los profesionales en ciberseguridad. 3.4. Cumplimiento normativo y estándares de seguridad.
4	Aspectos internacionales y diplomáticos	4.1. Ciberseguridad como un tema de seguridad nacional e internacional. 4.2. Diplomacia en el ciberespacio: acuerdos y tratados internacionales. 4.3. Ciberataques como herramienta de política exterior. 4.4. Cooperación internacional en la lucha contra el cibercrimen y la ciberseguridad defensiva.

7. Actividades de aprendizaje de los temas

1. Ética en la ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Comprender los fundamentos éticos y su aplicación específica en el ámbito de la ciberseguridad. *Genérica(s):* ● Habilidades para buscar, procesar y analizar información procedente de diversas fuentes. ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Capacidad de trabajo en equipo ● Compromiso Ético *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.	● 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.

2. Aspectos sociales de la ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Identificar y abordar los retos sociales emergentes relacionados con la ciberseguridad. *Genérica(s):* ● Capacidad de abstracción, análisis y síntesis ● Capacidad para identificar, plantear y resolver problemas ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas ● Compromiso ético ● Toma de decisiones ● Capacidad de trabajo en equipo *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.	● Realizar un debate acerca de temas de privacidad digital y sus implicaciones éticas y legales. ● Realizar una investigación sobre el impacto social de ataques cibernéticos específicos en la infraestructura crítica. ● Desarrollo y presentación de campañas de concienciación pública sobre ciberseguridad dirigidas a diferentes grupos demográficos. ● Construir un listado priorizado por importancia de los retos emergentes en ciberseguridad

3. Marco legal y regulatorio	
Competencias	Actividades de aprendizaje
Específica(s): Interpretar la legislación nacional e internacional, así como los aspectos regulatorios relevantes en el ámbito de la ciberseguridad. *Genérica(s):* ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de aplicar los conocimientos en la práctica. ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad de trabajo en equipo. ● Toma de decisiones. 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.	● Realizar un análisis de casos judiciales relevantes relacionados con delitos informáticos y discusión sobre sus implicaciones legales en el ámbito nacional. ● Elaborar un plan de cumplimiento normativo para una organización, considerando estándares de seguridad y regulaciones vigentes. ● Participación en debates sobre la responsabilidad legal de los profesionales en ciberseguridad en diferentes contextos y jurisdicciones.

4. Aspectos internacionales y diplomáticos	
Competencias	Actividades de aprendizaje
Específica(s): Analizar los acuerdos y tratados internacionales relacionados con la diplomacia en el ciberespacio. *Genérica(s):* ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de aplicar los conocimientos en la práctica. ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad de trabajo en equipo. ● Toma de decisiones. 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.	● Análisis de casos históricos de ciberataques como herramientas de política exterior y discusión sobre sus repercusiones. ● Investigación sobre acuerdos y tratados internacionales relevantes para la ciberseguridad y su impacto en las relaciones internacionales. ● Colaboración en un proyecto de investigación sobre estrategias de cooperación internacional para combatir el cibercrimen y fortalecer la ciberseguridad defensiva.

8. Práctica(s)

● Los estudiantes trabajarán en equipos para desarrollar un proyecto integral que aborde los aspectos legales, éticos y sociales de la ciberseguridad. El proyecto simulará una situación real en la que se enfrentarán a diversos desafíos y dilemas relacionados con la seguridad cibernética, la privacidad digital y la legislación pertinente

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 permanente por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Realizar una evaluación diagnóstica para identificar las áreas de oportunidad de los alumnos.
- Revisión de los indicadores de desempeño del alumno a través de un instrumento de evaluación (rúbricas, lista de cotejo, tablas de observación, mapas mentales, mapas conceptuales, entre otras).
- Revisión del desempeño individual y en equipo (reporte de dinámicas, reportes de actividades).

Evaluación del proyecto considerando los factores de contenido, desarrollo, actitudinal, habilidad del uso de las TIC´s en el diseño de su presentación y en el manejo de las mismas, expresión oral, además de la conducción de su presentación.

11. Fuentes de Información

1. Spinello, R. A. (2019). Cyberethics: Morality and law in cyberspace (6th ed.). Jones & Bartlett Learning.
2. Himma, K. E., & Tavani, H. T. (Eds.). (2015). The handbook of information and computer ethics. John Wiley & Sons.
3. Johnson, D. G. (2017). Computer ethics (5th ed.). Prentice Hall.
4. Vacca, J. R. (Ed.). (2019). Computer and information security handbook (3rd ed.). Morgan Kaufmann Publishers.
5. Baase, S. (2017). A gift of fire: Social, legal, and ethical issues for computing technology (5th ed.). Pearson.
6. Goodman, S. E., & Brenner, J. (Eds.). (2019). The Cambridge handbook of consumer privacy. Cambridge University Press.
7. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI