



## 1. Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	Ciberinteligencia
<b>Clave de la asignatura:</b>	CBD-2409
<b>SATCA<sup>1</sup>:</b>	2-3-5
<b>Carrera:</b>	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.
- 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.
- 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.
- 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.

La asignatura se caracteriza por ser una disciplina que se centra en el estudio y aplicación de técnicas, herramientas y metodologías para la recopilación, análisis e interpretación de información digital con el fin de identificar amenazas, vulnerabilidades y patrones de comportamiento en entornos cibernéticos. Su aportación al perfil de egreso se centra en formar profesionales capaces de diseñar estrategias de ciberseguridad avanzadas, tomar decisiones informadas basadas en inteligencia digital y contribuir a la protección de activos y datos en organizaciones y sistemas informáticos. La importancia de esta asignatura radica en la creciente dependencia de la tecnología y la información digital en la sociedad actual, lo que requiere de expertos preparados para enfrentar y prevenir ciberataques. Se relaciona estrechamente con asignaturas como "seguridad informática", "análisis forense digital" y "gestión de riesgos en tecnologías de la información",

<sup>1</sup> Sistema de Asignación y Transferencia de Créditos Académicos



abordando temas como criptografía, hacking ético, análisis de malware y gestión de incidentes de seguridad, fomentando competencias específicas en investigación, análisis crítico, toma de decisiones y trabajo colaborativo. Estas conexiones permiten identificar y generar proyectos integradores que aborden desafíos complejos en el ámbito de la ciberseguridad, promoviendo una formación integral y multidisciplinaria.

#### **Intención didáctica**

Es fundamental abordar los contenidos de manera estructurada y secuencial, comenzando por los fundamentos teóricos y avanzando hacia aplicaciones prácticas y casos de estudio actuales. Se debe adoptar un enfoque práctico y multidisciplinario, combinando aspectos técnicos, éticos y estratégicos de la ciberinteligencia. La extensión de los contenidos debe ser suficiente para proporcionar una comprensión completa de los temas, mientras que la profundidad debe permitir a los estudiantes desarrollar habilidades analíticas y críticas en la identificación y resolución de problemas de ciberseguridad. Se deben resaltar actividades como análisis de incidentes, ejercicios de simulación, trabajos en equipo y proyectos de investigación para fomentar competencias genéricas como el pensamiento crítico, la resolución de problemas, la comunicación efectiva y la colaboración. Las competencias genéricas que se desarrollan incluyen la capacidad de análisis, la toma de decisiones éticas, la adaptabilidad tecnológica y la gestión de la información. En cuanto al papel del docente, debe actuar como guía y facilitador del aprendizaje, proporcionando orientación, retroalimentación constructiva y recursos actualizados, promoviendo un ambiente de aprendizaje activo, participativo y reflexivo que motive a los estudiantes a explorar, cuestionar y aplicar los conceptos y técnicas de la ciberinteligencia de manera creativa y responsable.

### **3. Participantes en el diseño y seguimiento curricular del programa**

<b>Lugar y fecha de elaboración o revisión</b>	<b>Participantes</b>	<b>Observaciones</b>
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.	<p>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.</p> <p>Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.</p>	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	<p>Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas</p>	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"> <li>Identifica, analiza y mitiga amenazas cibernéticas mediante el uso de técnicas y herramientas avanzadas de inteligencia digital, demostrando habilidades para recopilar información relevante, interpretar patrones de comportamiento y diseñar estrategias efectivas de protección y defensa en entornos tecnológicos, contribuyendo así a la seguridad y resiliencia de sistemas informáticos y redes empresariales.</li> </ul>

#### 5. Competencias previas

<ul style="list-style-type: none"> <li>Evalúa y comprende los aspectos legales, éticos y sociales relacionados con la ciberseguridad, garantizando el cumplimiento normativo y promoviendo prácticas responsables.</li> <li>Analiza y Evalúa redes de datos conmutadas para inferir problemas de diseño, implementación y/o desempeño.</li> <li>Analiza y aplica técnicas y herramientas forenses para recolectar, preservar, analizar y presentar evidencia digital de manera ética y conforme a los estándares legales y metodológicos establecidos, para contribuir a la detección, investigación y resolución de incidentes de seguridad y delitos cibernéticos.</li> <li>Comprender, aplicar y evaluar técnicas de hacking ético.</li> </ul>
---



## 6. Temario

No.	Temas	Subtemas
1	Introducción a la ciberinteligencia.	1.1. Definición y conceptos fundamentales de ciberinteligencia. 1.2. Importancia y aplicaciones en la seguridad cibernética. 1.3. Ciclo inteligencia. 1.4. Seguridad operativa (OPSEC). 1.5. Ciberprotección y anonimización. 1.6. Identidades digitales (sock puppets).
2	Ciberinteligencia en materia de ciberseguridad.	2.1. Principales vectores de ataque en el ciberespacio. 2.2. Ciberseguridad en empresas e instituciones. 2.3. Inteligencia aplicada al ciberdelito. 2.4. Inteligencia en el ciberterrorismo. 2.5. Inteligencia en el hacktivismo.
3	Inteligencia de fuentes abiertas (OSINT).	3.1. Tipos de OSINT. 3.2. Metodologías y técnicas de OSINT. 3.3. Securitización del entorno de trabajo. 3.4. Entorno de trabajo y contramedidas. 3.5. Técnicas, herramientas y procedimientos de recopilación de información. 3.6. Cyberthreat Intelligence. 3.7. Técnicas de análisis.
4	SOCMINT (social media intelligence).	4.1. Análisis de perfiles y usuarios. 4.2. Monitoreo de conversaciones y tendencias. 4.3. Detección y análisis de amenazas y riesgos. 4.4. Geolocalización y análisis espacial. 4.5. Análisis de imágenes y multimedia. 4.6. Inteligencia de influencia y campañas de información. 4.7. Análisis de redes sociales y estructuras de conexión.



## 7. Actividades de aprendizaje de los temas

1. Introducción a la ciberinteligencia.	
Competencias	Actividades de aprendizaje
<p><b>Específica(s):</b> El estudiante debe comprender y aplicar los conceptos y fundamentos de la ciberinteligencia, identificar su importancia y aplicaciones en la seguridad cibernética, gestionar el ciclo de inteligencia, implementar medidas de seguridad operativa (OPSEC), aplicar técnicas de ciberprotección y anonimización, y manejar identidades digitales (Sock Puppets), con el fin de fortalecer la capacidad de detección, análisis, protección y respuesta a amenazas y riesgos cibernéticos, y contribuir al desarrollo de estrategias y acciones efectivas en el ámbito de la ciberseguridad.</p> <p><b>Genérica(s):</b></p> <ul style="list-style-type: none"> <li>• Capacidad de análisis y síntesis.</li> <li>• Capacidad de organizar y planificar.</li> <li>• Habilidad para buscar y analizar información proveniente de fuentes diversas.</li> <li>• Solución de problemas.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar los conocimientos.</li> <li>• Habilidades de investigación.</li> <li>• Capacidad de generar nuevas ideas</li> <li>• Liderazgo.</li> <li>• Habilidad para trabajar en forma autónoma.</li> <li>• Búsqueda del logro.</li> </ul> <p><b>Transversal(es):</b></p> <ul style="list-style-type: none"> <li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li> </ul>	<ul style="list-style-type: none"> <li>• Realización de seminarios y conferencias introductorias para comprender la definición y conceptos fundamentales de ciberinteligencia, así como su importancia y aplicaciones en la seguridad cibernética.</li> <li>• Análisis de casos prácticos y estudios de caso relacionados con la aplicación de la ciberinteligencia en la detección, prevención, mitigación y respuesta a amenazas y ataques cibernéticos.</li> <li>• Desarrollo de talleres prácticos para aplicar el ciclo de inteligencia, incluyendo la planificación, recopilación, procesamiento, análisis, difusión y retroalimentación de la información de inteligencia.</li> <li>• Simulaciones y ejercicios prácticos de seguridad operativa (OPSEC), donde los estudiantes aprenderán a identificar y proteger información sensible y operaciones críticas de inteligencia.</li> <li>• Talleres prácticos para aprender y aplicar técnicas de ciberprotección y anonimización, incluyendo el uso de herramientas y servicios para proteger la privacidad y la identidad en línea.</li> <li>• Desarrollo de ejercicios prácticos para crear, gestionar y utilizar identidades digitales (sock puppets) de forma segura y efectiva en operaciones de inteligencia y ciberseguridad.</li> </ul>



<ul style="list-style-type: none"><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• 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.</li></ul>	
<b>2. Ciberinteligencia en materia de ciberseguridad.</b>	
<b>Competencias</b>	<b>Actividades de aprendizaje</b>
<p><i>Específica(s):</i> Aplica técnicas de ciberinteligencia para identificar y analizar los principales vectores de ataque en el ciberespacio, evaluar la ciberseguridad en empresas e instituciones, y gestionar la inteligencia aplicada al cibercrimen, ciberterrorismo y heactivismo, con el fin de fortalecer la detección, prevención, mitigación y respuesta a amenazas y ataques cibernéticos, protegiendo sistemas, redes, datos y activos, y contribuyendo al desarrollo de estrategias y acciones efectivas en el ámbito de la ciberseguridad.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de organizar y planificar.</li><li>• Habilidad para buscar y analizar información proveniente de fuentes diversas.</li><li>• Solución de problemas.</li><li>• Toma de decisiones.</li><li>• Trabajo en equipo.</li><li>• Capacidad de aplicar los conocimientos.</li><li>• Habilidades de investigación.</li><li>• Capacidad de generar nuevas ideas</li><li>• Liderazgo.</li></ul>	<ul style="list-style-type: none"><li>• Estudio y análisis de casos reales y simulados de principales vectores de ataque en el ciberespacio, identificando técnicas, herramientas y motivaciones de los atacantes.</li><li>• Simulación de incidentes de seguridad en entornos empresariales e institucionales, donde los estudiantes deberán identificar, contener, mitigar y responder a los ataques cibernéticos.</li><li>• Investigación y análisis de amenazas cibernéticas, incluyendo ciberdelitos y ataques dirigidos a empresas, instituciones, infraestructuras críticas y sistemas gubernamentales.</li><li>• Análisis de casos de terrorismo cibernético, incluyendo incidentes de ciberterrorismo pasados y potenciales, así como las estrategias de inteligencia utilizadas para prevenir y responder a tales amenazas.</li><li>• Ejercicios prácticos de Hacktivism, donde los estudiantes simulan ataques y acciones de hacktivistas, y desarrollan contramedidas y estrategias de inteligencia para hacer frente a estos desafíos.</li></ul>



<ul style="list-style-type: none"><li>• Habilidad para trabajar en forma autónoma.</li><li>• Búsqueda del logro.</li></ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"><li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li><li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li><li>• 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.</li></ul>	
<b>3. Inteligencia de fuentes abiertas (OSINT).</b>	
<b>Competencias</b>	<b>Actividades de aprendizaje</b>
<p><i>Específica(s):</i> Identifica y aplica metodologías y técnicas de recopilación de información de fuentes abiertas, dominar herramientas y procedimientos de OSINT, y analizar información para la detección, evaluación y gestión de amenazas cibernéticas, contribuyendo así al fortalecimiento de la capacidad de inteligencia en el ámbito de la ciberseguridad y la toma de decisiones informadas.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis.</li><li>• Capacidad de organizar y planificar.</li><li>• Habilidad para buscar y analizar información proveniente de fuentes diversas.</li><li>• Solución de problemas.</li><li>• Toma de decisiones.</li><li>• Trabajo en equipo.</li></ul>	<ul style="list-style-type: none"><li>• Realización de seminarios y conferencias introductorias para comprender los tipos de OSINT y su importancia en la inteligencia cibernética y la ciberseguridad.</li><li>• Desarrollo de talleres prácticos para aprender y aplicar metodologías y técnicas de OSINT, incluyendo la búsqueda en motores de búsqueda, redes sociales, foros, sitios web y bases de datos públicas.</li><li>• Ejercicios prácticos para implementar medidas de securización del entorno de trabajo, incluyendo la configuración de redes seguras, el uso de VPN, la autenticación de dos factores y el cifrado de datos.</li><li>• Desarrollo de talleres prácticos para identificar y aplicar contramedidas contra amenazas de seguridad en el entorno de trabajo de OSINT, incluyendo la detección de amenazas y la respuesta a incidentes de seguridad.</li><li>• Desarrollo de ejercicios prácticos para aprender y aplicar técnicas, herramientas y procedimientos de recopilación de información en OSINT, incluyendo el uso de herramientas de</li></ul>





<ul style="list-style-type: none"> <li>• Capacidad de aplicar los conocimientos.</li> <li>• Habilidades de investigación.</li> <li>• Capacidad de generar nuevas ideas</li> <li>• Liderazgo.</li> <li>• Habilidad para trabajar en forma autónoma.</li> <li>• Búsqueda del logro.</li> </ul> <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"> <li>• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.</li> <li>• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.</li> <li>• 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.</li> </ul>	<p>análisis de inteligencia y la verificación de fuentes de información.</p> <ul style="list-style-type: none"> <li>• Simulaciones y ejercicios prácticos de cyberthreat intelligence, donde los estudiantes aprenderán a analizar y evaluar amenazas cibernéticas utilizando OSINT.</li> <li>• Desarrollo de talleres prácticos para aprender y aplicar técnicas de análisis en OSINT, incluyendo el análisis de datos, la evaluación de la credibilidad de la información y la elaboración de informes de inteligencia.</li> </ul>
<b>4. SOCMINT (social media intelligence).</b>	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <p>Analiza perfiles y usuarios, monitorear conversaciones y tendencias, detectar y analizar amenazas y riesgos, aplicar geolocalización y análisis espacial, analizar imágenes y multimedia, gestionar inteligencia de influencia y campañas de información, y analizar redes sociales y estructuras de conexión, con el fin de fortalecer la capacidad de recopilación, análisis e interpretación de información en redes sociales y plataformas en línea para la detección, prevención, mitigación y respuesta a amenazas y riesgos cibernéticos, y contribuir al desarrollo de</p>	<ul style="list-style-type: none"> <li>• Desarrollo de talleres prácticos para aprender y aplicar técnicas de análisis de perfiles y usuarios en plataformas y redes sociales, identificando comportamientos, intereses y relaciones.</li> <li>• Ejercicios prácticos de monitoreo y análisis de conversaciones y tendencias en redes sociales y plataformas en línea para identificar temas relevantes y actores clave.</li> <li>• Simulaciones y ejercicios prácticos para detectar, analizar y evaluar amenazas y riesgos en el entorno digital, incluyendo ciberataques, fraudes y desinformación.</li> <li>• Desarrollo de talleres prácticos para aplicar técnicas de geolocalización y análisis espacial en la inteligencia cibernética, identificando ubicaciones, movimientos y patrones geográficos de interés.</li> </ul>





estrategias y acciones efectivas en el ámbito de la ciberseguridad y la ciberinteligencia.

*Genérica(s):*

- Capacidad de análisis y síntesis.
- Capacidad de organizar y planificar.
- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Solución de problemas.
- Toma de decisiones.
- Trabajo en equipo.
- Capacidad de aplicar los conocimientos.
- Habilidades de investigación.
- Capacidad de generar nuevas ideas
- Liderazgo.
- Habilidad para trabajar en forma autónoma.
- Búsqueda del 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.

- Desarrollo de ejercicios prácticos para analizar y evaluar imágenes y multimedia en el ámbito de la inteligencia cibernética, identificando objetos, personas y contextos relevantes.
- Simulaciones y ejercicios prácticos para identificar, analizar y evaluar campañas de desinformación, propaganda y manipulación en plataformas y redes sociales.
- Desarrollo de talleres prácticos para analizar redes sociales y estructuras de conexión, identificando comunidades, grupos y relaciones entre actores en el entorno digital.



## 8. Práctica(s)

- Análisis de OSINT en una campaña de desinformación
  - Investigación preliminar.
  - Recopilación de Información con OSINT.
  - Análisis de datos.
  - Elaboración de Informe de inteligencia
- Simulación de análisis de threat intelligence
  - Definición de escenario de simulación.
  - Recolección de datos de threat intelligence.
  - Análisis de amenazas y riesgos.
  - Elaboración de informe de threat intelligence.

## 9. Proyecto de asignatura

El objetivo del proyecto que plantee 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

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

- Análisis de casos.
- Análisis y solución de problemas.
- Análisis de videos y material audiovisual de diverso tipo.
- Recorridos de campo.
- Solución de problemas realizados en forma individual o en equipo.
- Discusiones y debates en equipos.
- Exhibiciones presenciales o virtuales.
- Entrevistas a expertos
- Desarrollo de proyectos.
- Paneles de presentaciones de temas.

## 11. Fuentes de Información

1. Casey, E. (2014). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
2. Gordon, S. (2015). The internet police: How crime went online, and the cops followed. Reaktion Books.
3. Inteltechniques. (n.d.). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information (6th ed.).
4. NATO Open Source Intelligence Handbook. (2011). NATO.
5. Rogers, M. (2016). Open Source Intelligence Investigation: From Strategy to Implementation. CRC Press.
6. Russell, C. (2018). Practical OSINT Techniques. Packt Publishing.
7. SANS Institute. (2016). Securing the human: CISO briefing. SANS Institute.
8. Steele, R. D. (2017). OSINT for cybersecurity. Springer.
9. Trulove, J. (2019). Cyber Intelligence: The role of OSINT in the cyber domain. Palgrave Macmillan.
10. Twitter. (n.d.). Twitter Transparency Report.  
<https://transparency.twitter.com/en/reports/index.html>
11. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.