1. Datos Generales de la asignatura

Nombre de la asignatura:	Análisis y Gestión de Riesgos en Ciberseguridad
Clave de la asignatura:	CBI-2401
SATCA[1]:	4-0-4
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Esta 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.
- 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.

La asignatura se centra en dotar a los estudiantes de las habilidades y conocimientos necesarios para identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información en entornos tecnológicos. Su aportación al perfil de egreso se enfoca en formar profesionales capaces

[1] Sistema de Asignación y Transferencia de Créditos Académicos

de implementar estrategias de ciberseguridad robustas y eficaces, alineadas con las necesidades actuales del mundo digital. Esta asignatura es crucial en el contexto actual, donde la seguridad de la información es esencial para proteger activos, garantizar la privacidad y mantener la confianza en los sistemas y servicios digitales. Se relaciona estrechamente con asignaturas como "Fundamentos de Ciberseguridad", "Tecnologías de la Información y Comunicación", y "Gestión de Proyectos de Tecnología de la Información", abordando temas como evaluación de vulnerabilidades, políticas de seguridad, gestión de incidentes y cumplimiento normativo. Las competencias específicas que se desarrollan incluyen análisis de riesgos, toma de decisiones basada en riesgos, diseño de políticas de seguridad y capacidad para implementar y gestionar soluciones de ciberseguridad. Estas conexiones permiten identificar y generar proyectos integradores que aborden la ciberseguridad desde una perspectiva holística y aplicada.
Intención didáctica
Los contenidos se abordarán de manera teórica y práctica, combinando el estudio de marcos teóricos con ejercicios prácticos y casos de estudio reales para ilustrar la aplicación de los conceptos. El enfoque será orientado a la resolución de problemas, fomentando el pensamiento crítico y analítico de los estudiantes para evaluar y mitigar riesgos en entornos de ciberseguridad. Los contenidos serán tratados con una extensión suficiente para garantizar una comprensión profunda de los conceptos fundamentales, pero también flexible para permitir la adaptación a las necesidades y avances del campo de la ciberseguridad. Se resaltarán actividades como análisis de casos prácticos, simulaciones de ataques y defensas, y elaboración de políticas y procedimientos de ciberseguridad, para el desarrollo de competencias genéricas como el trabajo en equipo, la comunicación efectiva, la toma de decisiones éticas y la capacidad de adaptación a nuevos escenarios y tecnologías. Las competencias genéricas que se desarrollarán incluyen la capacidad de análisis y síntesis de información, el pensamiento crítico, la toma de decisiones informadas, la comunicación efectiva, la ética profesional y la habilidad para aprender de manera autónoma. El papel del docente será el de facilitador del aprendizaje, proporcionando orientación, retroalimentación y apoyo a los estudiantes en su proceso de aprendizaje. Deberá promover la participación de los estudiantes, fomentar el debate y la reflexión crítica, y proporcionar recursos y herramientas para que los estudiantes puedan desarrollar las competencias necesarias para analizar y gestionar riesgos en ciberseguridad de manera efectiva y ética.

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
• Identifica y evalúa los riesgos asociados a la seguridad de la información en entornos tecnológicos, aplicando métodos y técnicas de análisis de riesgos de ciberseguridad para proponer e implementar estrategias de mitigación y gestión eficaces, cumpliendo con los estándares y regulaciones vigentes.

5. Competencias previas

• Analiza y aplica los aspectos legales, éticos y sociales relacionados con la ciberseguridad, considerando las normativas, regulaciones y mejores prácticas en el ámbito legal y ético de la seguridad de la información.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de riesgos en la ciberseguridad	1.1 Conceptos básicos 1.2 Tiara y obstáculos 1.3 Tipos de riesgos 1.4 Actores y motivaciones 1.5 Impacto de los riesgos cibernéticos en las organizaciones
2	Análisis de riesgos en ciberseguridad	2.1 Proceso de análisis de riesgos 2.2Identificación de activos, amenazas, controles, vulnerabilidades y consecuencias. 2.3 Métodos cualitativos y cuantitativos para medir el riesgo 2.4 Matrices de riesgo 2.5 Evaluación de impacto y probabilidad
3	Gestión de riesgos en ciberseguridad	3.1 Estrategias de gestión de riesgos 3.2 Planificación de respuestas a riesgos 3.3 Implementación de controles de seguridad 3.4 Tratamiento del riesgo 3.5 Riesgo residual 3.6 Comunicación y reporte de riesgos
4	Herramientas y técnicas de análisis de riesgo	4.1 Metodologías de gestión de riesgos 4.2 Principales normativas y estándares de ciberseguridad ISO 27001, NIST 4.3. Software de gestión de riesgos 4.4 Nuevas tecnologías aplicadas al análisis y gestión del riesgo

7. Actividades de aprendizaje de los temas

1. Fundamentos de riesgos en la ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Identificará y comprenderá los conceptos básicos, tipos de riesgos, actores y motivaciones, así como el impacto de los riesgos cibernéticos en las organizaciones, aplicando el análisis de tiara y obstáculos para evaluar y gestionar de manera efectiva los riesgos asociados a la seguridad de la información en entornos tecnológicos. *Genérica(s):* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar.	Conceptos básicos • Lecturas dirigidas sobre los fundamentos de la ciberseguridad y los conceptos básicos de los riesgos. • Discusión en grupos pequeños para compartir y analizar las definiciones y conceptos clave. • Elaboración de un glosario de términos relacionados con la ciberseguridad y los riesgos. 2. Tiara y obstáculos • Estudio de casos prácticos para identificar y analizar la Técnica de Identificación y Análisis de Riesgos (TIARA).

• Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). • Solución de problemas. • Toma de decisiones. • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Capacidad de trabajar en equipo interdisciplinario. • Compromiso ético. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones. • Capacidad de generar nuevas ideas (creatividad). • Liderazgo. • Habilidad para trabajar en forma autónoma. • Capacidad para diseñar y gestionar proyectos. • Preocupación por la calidad. 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,	• Ejercicios prácticos de identificación de obstáculos comunes en la gestión de riesgos. • Debates en clase sobre la importancia de la TIARA y cómo superar los obstáculos en la gestión de riesgos. 3. Tipos de riesgos • Análisis de casos reales para identificar diferentes tipos de riesgos cibernéticos (tecnológicos, humanos, naturales, etc.). • Ejercicios de clasificación de riesgos según su origen y naturaleza. • Estudio de las principales amenazas y vulnerabilidades en entornos de ciberseguridad. 4. Actores y motivaciones • Investigación y presentación sobre los actores involucrados en los riesgos cibernéticos (hackers, insiders, competidores, etc.) y sus motivaciones. • Análisis de escenarios para comprender las diferentes motivaciones que pueden impulsar los ataques cibernéticos. • Discusión en clase sobre las estrategias y técnicas más comunes utilizadas por los actores en el ciberespacio. 5. Impacto de los riesgos cibernéticos en las organizaciones • Estudio de casos de impactos significativos de riesgos cibernéticos en organizaciones reales. • Análisis de las consecuencias financieras, operativas y reputacionales de los riesgos cibernéticos. • Desarrollo de un plan de respuesta a incidentes de seguridad para mitigar el impacto de los riesgos cibernéticos.

rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	
2. Análisis de riesgos en ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): • Aplicará el proceso de análisis de riesgos, identificando activos, amenazas, controles, vulnerabilidades y consecuencias, utilizando métodos cualitativos y cuantitativos para medir el riesgo, desarrollando matrices de riesgo y evaluando el impacto y la probabilidad de los riesgos cibernéticos, con el fin de proponer e implementar estrategias de mitigación y gestión eficaces en entornos de ciberseguridad. *Genérica(s):* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). • Solución de problemas. • Toma de decisiones. • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Capacidad de trabajar en equipo interdisciplinario. • Compromiso ético. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones. • Capacidad de generar nuevas ideas (creatividad).	1. Proceso de análisis de riesgos • Estudio teórico sobre el proceso de análisis de riesgos en ciberseguridad. • Análisis y discusión de un caso práctico completo de análisis de riesgos. • Desarrollo de un diagrama de flujo del proceso de análisis de riesgos. 2. Identificación de activos, amenazas, controles, vulnerabilidades y consecuencias • Taller práctico para identificar activos de información en una organización. • Análisis de amenazas y vulnerabilidades asociadas a los activos identificados. • Estudio de casos para identificar controles de seguridad adecuados y sus efectos sobre las vulnerabilidades. • Análisis de las posibles consecuencias de los riesgos identificados. 3. Métodos cualitativos y cuantitativos para medir el riesgo • Estudio y aplicación de métodos cualitativos (análisis cualitativo, escala de riesgo cualitativa). • Taller práctico para aplicar métodos cuantitativos (análisis cuantitativo, cálculo de la probabilidad e impacto). • Comparación y discusión de los resultados obtenidos mediante métodos cualitativos y cuantitativos. 4. Matrices de riesgo • Desarrollo de matrices de riesgo utilizando la información recopilada durante la identificación de activos, amenazas, controles, vulnerabilidades y consecuencias.

• Liderazgo. • Habilidad para trabajar en forma autónoma. • Capacidad para diseñar y gestionar proyectos. • Preocupación por la calidad. 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 y discusión de las matrices de riesgo desarrolladas en grupos. • Aplicación de las matrices de riesgo para priorizar y gestionar los riesgos identificados. 5. Evaluación de impacto y probabilidad • Taller práctico para evaluar el impacto y la probabilidad de los riesgos identificados. • Estudio de casos para comprender la relación entre impacto y probabilidad en la evaluación de riesgos. Análisis y discusión de las estrategias de mitigación propuestas en función de la evaluación de impacto y probabilidad.

3. Gestión de riesgos en ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): • Desarrollará estrategias de gestión de riesgos, planificará respuestas a riesgos, implementará controles de seguridad, gestionará el tratamiento del riesgo y evaluará el riesgo residual, además de comunicar y reportar los riesgos de manera efectiva, para garantizar una gestión integral y eficaz de los riesgos cibernéticos en entornos de ciberseguridad. *Genérica(s):*	1. Estrategias de gestión de riesgos • Estudio teórico sobre las diferentes estrategias de gestión de riesgos en ciberseguridad. • Análisis y discusión de casos prácticos de aplicación de estrategias de gestión de riesgos. • Desarrollo de un plan de gestión de riesgos utilizando diferentes estrategias. 2. Planificación de respuestas a riesgos

• Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). • Solución de problemas. • Toma de decisiones. • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Capacidad de trabajar en equipo interdisciplinario. • Compromiso ético. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones. • Capacidad de generar nuevas ideas (creatividad). • Liderazgo. • Habilidad para trabajar en forma autónoma. • Capacidad para diseñar y gestionar proyectos. • Preocupación por la calidad. 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,	• Taller práctico para desarrollar un plan de respuesta a riesgos basado en los riesgos identificados. • Análisis y discusión de las estrategias de respuesta a riesgos más adecuadas para diferentes escenarios. • Simulación de escenarios de incidentes de seguridad para aplicar el plan de respuesta a riesgos desarrollado. 3. Implementación de controles de seguridad • Estudio de los principales controles de seguridad y su aplicación en entornos de ciberseguridad. • Taller práctico para implementar controles de seguridad específicos en un entorno simulado. • Análisis y discusión de los efectos de la implementación de controles de seguridad en la mitigación de riesgos. 4. Tratamiento del riesgo • Análisis de las diferentes estrategias de tratamiento del riesgo (aceptar, transferir, mitigar, evitar). • Desarrollo de un plan de tratamiento del riesgo para los riesgos identificados. • Estudio de casos para aplicar las estrategias de tratamiento del riesgo en situaciones prácticas. 5. Riesgo residual • Taller práctico para evaluar el riesgo residual después de aplicar las estrategias de tratamiento del riesgo. • Análisis y discusión de las estrategias adicionales necesarias para gestionar el riesgo residual de manera efectiva. • Desarrollo de un plan de gestión del riesgo residual para garantizar la continuidad de las operaciones y la protección de la información. 6. Comunicación y reporte de riesgos • Estudio de los principales métodos y técnicas de comunicación y reporte de riesgos en ciberseguridad.

vanguardia e innovación social que fortalezcan el desarrollo humano.	• Taller práctico para desarrollar informes de riesgos detallados y comunicarlos a diferentes partes interesadas. Análisis y discusión de los informes de riesgos desarrollados para mejorar la comunicación y el reporte de riesgos en entornos de ciberseguridad.
4. Herramientas y técnicas de análisis de riesgo	
Competencias	Actividades de aprendizaje
Específica(s): • Aplicará metodologías de gestión de riesgos, identificará y aplicará las principales normativas y estándares de ciberseguridad como ISO 27001 y NIST, utilizará software de gestión de riesgos y explorará nuevas tecnologías aplicadas al análisis y gestión del riesgo, para realizar un análisis de riesgos efectivo y proponer estrategias de mitigación adecuadas en entornos de ciberseguridad. *Genérica(s):* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). • Solución de problemas. • Toma de decisiones. • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Capacidad de trabajar en equipo interdisciplinario. • Compromiso ético. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones.	1. Metodologías de gestión de riesgos • Estudio teórico sobre las diferentes metodologías de gestión de riesgos en ciberseguridad. • Análisis y discusión de casos prácticos de aplicación de metodologías de gestión de riesgos. • Desarrollo de un plan de gestión de riesgos utilizando una metodología seleccionada. 2. Principales normativas y estándares de ciberseguridad ISO 27001, NIST Investigación y estudio de las normativas y estándares de ciberseguridad ISO 27001 y NIST. • Análisis y discusión de la aplicación de las normativas y estándares en entornos de ciberseguridad. • Desarrollo de un informe comparativo de las normativas y estándares de ciberseguridad ISO 27001 y NIST. 3. Software de gestión de riesgos • Taller práctico para utilizar software de gestión de riesgos específicos en un entorno simulado. • Análisis y discusión de las características y funcionalidades de diferentes software de gestión de riesgos. • Desarrollo de un informe comparativo de software de gestión de riesgos, destacando sus ventajas y desventajas. 4. Nuevas tecnologías aplicadas al análisis y gestión del riesgo • Investigación y estudio de las nuevas tecnologías aplicadas al análisis y gestión del riesgo en ciberseguridad.

• Capacidad de generar nuevas ideas (creatividad). • Liderazgo. • Habilidad para trabajar en forma autónoma. • Capacidad para diseñar y gestionar proyectos. • Preocupación por la calidad. 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.	• Taller práctico para aplicar nuevas tecnologías en el análisis y gestión del riesgo en un entorno simulado. Análisis y discusión de los beneficios y desafíos de la aplicación de nuevas tecnologías en el análisis y gestión del riesgo.

8. Práctica(s)

- **Simulaciones de ataques:** Realizar simulaciones de ataques cibernéticos en un entorno controlado donde los estudiantes puedan observar cómo se desarrollan los ataques y cuáles son sus consecuencias.
- **Laboratorios virtuales:** Utilizar plataformas de laboratorios virtuales como Cyber Aces, TryHackMe o Hack The Box para que los estudiantes realicen ejercicios prácticos sobre vulnerabilidades y amenazas.
- **Desarrollo de escenarios:** Crear escenarios ficticios donde los estudiantes deban identificar y describir diferentes tipos de riesgos y amenazas, y proponer estrategias de mitigación.
- **Proyectos de análisis de riesgo:** Asignar proyectos en los que los estudiantes realicen análisis de riesgos completos para una empresa ficticia, incluyendo la identificación de activos críticos, evaluación de amenazas y vulnerabilidades, y recomendación de medidas de mitigación.
- **Talleres de modelado de amenazas:** Realizar talleres donde los estudiantes utilicen técnicas de modelado de amenazas, como STRIDE o DREAD, para mapear posibles ataques y evaluar su impacto.

- **Uso de herramientas de análisis:** Enseñar a los estudiantes a utilizar herramientas de análisis de riesgos como OWASP Threat Dragon o Microsoft Threat Modeling Tool, y asignarles tareas prácticas para que se familiaricen con estas herramientas.
- **Desarrollo de un plan de gestión de riesgos:** Guiar a los estudiantes en la creación de un plan de gestión de riesgos para una organización ficticia, incluyendo políticas, procedimientos y roles y responsabilidades.
- **Ejercicios de respuesta a incidentes:** Organizar simulaciones de respuesta a incidentes donde los estudiantes deban gestionar un incidente de ciberseguridad desde su identificación hasta su resolución, siguiendo un plan de respuesta a incidentes.
- **Implementación de controles:** Pedir a los estudiantes que identifiquen y propongan controles de seguridad específicos para mitigar riesgos identificados en un análisis de riesgos previo, y que los implementen en un entorno de prueba.
- **Capacitación en herramientas específicas:** Proporcionar talleres prácticos en el uso de herramientas como Nessus, OpenVAS, Burp Suite y Splunk, donde los estudiantes realicen escaneos de vulnerabilidades y análisis de seguridad en entornos de laboratorio.
- **Pruebas de penetración:** Asignar ejercicios de pruebas de penetración en un entorno controlado, donde los estudiantes deban identificar y explotar vulnerabilidades, y luego realizar un informe de sus hallazgos y recomendaciones.
- **Análisis forense:** Realizar laboratorios de análisis forense donde los estudiantes investiguen incidentes de ciberseguridad simulados, recojan y analicen evidencias, y generen informes forenses detallados.

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

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. Alberts, C. J., Dorofee, A., & Killcrece, G. (2010). Managing information security risks: The OCTAVE (SM) approach. Addison-Wesley.
2. ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.
3. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce.
4. Whitman, M. E., & Mattord, H. J. (2018). Management of information security. Cengage Learning.
5. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. National Institute of Standards and Technology.
6. Hernández, J., & Rodríguez, A. (2016). Análisis de riesgos en seguridad de la información: Metodologías y estándares. 2ª Edición. RA-MA Editorial.
7. Wright, D., & Jimenez, A. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
8. Khedr, A. E. (2019). Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd.
9. Rouse, M. (2020). Risk assessment framework (RAF). TechTarget.
10. Simsek, A., & Eren, S. (2019). The Impact of New Technologies on Cyber Security. International Journal of Intelligent Systems and Applications in Engineering, 7(2), 48-54.

11. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.