1. Datos Generales de la asignatura

Nombre de la asignatura:	Auditoría de Seguridad
Clave de la asignatura:	CBD-2408
SATCA[1]:	3-2-5
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.
- 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.
- 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.

Se enfoca en proporcionar a los estudiantes de Ingeniería en Ciberseguridad todas las habilidades necesarias para poder evaluar, analizar y auditar la seguridad de sistemas de información y redes. Esta asignatura aborda los principios fundamentales de auditoría, las metodologías de evaluación de riesgos y la aplicación de estándares de seguridad reconocidos internacionalmente.

La asignatura es fundamental para la formación de profesionales en Ingeniería en Ciberseguridad, ya que se basa en analizar vulnerabilidades y debilidades para establecer un adecuado plan de auditoría que funcione de manera efectiva.

Intención didáctica

El contenido de esta materia se encuentra distribuido en 5 temas, busca dotar a los estudiantes de habilidades necesarias para llevar a cabo auditorías de seguridad efectivas en sistemas de información y redes. Se enfoca en desarrollar la capacidad de los estudiantes para aplicar

[1] Sistema de Asignación y Transferencia de Créditos Académicos

metodologías de auditoría, evaluar riesgos, interpretar estándares de seguridad y comunicar de manera clara los hallazgos y recomendaciones. Los estudiantes serán capaces de identificar vulnerabilidades, diseñar planes de acción y contribuir significativamente a la protección de la información en entornos empresariales.

En el tema 1, el estudiante adquirirá una visión general de los conceptos básicos de la auditoría, incluyendo su aplicación específica en el ámbito de la seguridad informática. A través de este tema, el estudiante comenzará a desarrollar las habilidades y conocimientos necesarios para abordar de manera efectiva los desafíos relacionados con la evaluación y mejora de la seguridad de los sistemas de información y redes.

En el tema 2, el estudiante obtendrá herramientas y técnicas necesarias para planificar y ejecutar auditorías de seguridad de manera efectiva. A través de este tema, el estudiante desarrollará una comprensión práctica de cómo llevar a cabo auditorías de seguridad de manera sistemática y rigurosa, contribuyendo así a la identificación y mitigación de riesgos en los sistemas de información y redes.

En el tema 3, el estudiante se familiarizará con las normativas y estándares internacionales relevantes en el campo de la ciberseguridad, así como proporcionarles las herramientas necesarias para evaluar los riesgos asociados a los sistemas de información y redes. A través de este tema, el estudiante desarrollará una comprensión sólida de los marcos normativos y de evaluación de riesgos, lo que le permitirá realizar auditorías de seguridad más efectivas y contribuir a la protección de la información en las organizaciones.

En el tema 4, el estudiante adquirirá las habilidades necesarias para llevar a cabo auditorías de seguridad en sistemas de información y redes. A través de este tema, el estudiante desarrollará la capacidad de identificar y analizar los riesgos de seguridad en sistemas y redes, así como proponer medidas correctivas y preventivas para mitigar dichos riesgos y fortalecer la seguridad de la información en las organizaciones.

Finalmente en el tema 5, el estudiante aprenderá a elaborar informes de auditoría detallados y en la gestión efectiva de los hallazgos de seguridad. Se busca que el estudiante comprenda la importancia de comunicar de manera clara y precisa los resultados de una auditoría, así como las recomendaciones para mejorar la seguridad de la información.

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
• Identificar los diferentes tipos de auditorías de seguridad. • Realizar auditorías de seguridad en sistemas de información y redes. • Aplicar metodologías de evaluación de riesgos para identificar amenazas y vulnerabilidades. • Interpretar y aplicar estándares y normativas de seguridad. • Elaborar informes de auditoría detallados con hallazgos y recomendaciones. • Diseñar planes de acción para mitigar riesgos y mejorar la seguridad de la información.

5. Competencias previas

- Analiza y Evalúa redes de datos conmutadas para inferir problemas de diseño, implementación y/o desempeño.
- Diseña sistemas y técnicas específicas para asegurar los sistemas informáticos de la empresa y diversos dispositivos.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Auditoría de Ciberseguridad	1.1. Conceptos básicos de auditoría y su aplicación en seguridad informática. 1.2. Diferentes tipos de auditorías de seguridad 1.3. Marco legal y regulaciones relevantes. 1.4. Importancia de la auditoría de seguridad en la protección de la información
2	Procesos de Auditoría en Ciberseguridad	2.1. Metodologías y enfoques de auditoría en ciberseguridad. 2.2. Planificación y programación de auditorías. 2.3. Análisis de vulnerabilidades y brechas de seguridad. 2.4. Recolección y análisis de evidencia digital. 2.5. Técnicas de muestreo aplicadas a la auditoría en ciberseguridad. 2.6. Documentación y comunicación de hallazgos. 2.7. Herramientas de software y hardware aplicadas a la auditoria en ciberseguridad
3	Normativas, Estándares y Evaluación de Riesgos	3.1. ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información. 3.2. NIST SP 800-53: Seguridad y Privacidad en Sistemas de Información. 3.3. PAS 555 Gestión de la seguridad cibernética 3.4. Evaluación de activos, amenazas y vulnerabilidades
4	Auditoría de Sistemas y Redes	4.1. Revisión de políticas de seguridad. 4.2. Evaluación de la arquitectura de red y sistemas. 4.3. Pruebas de penetración y evaluación de seguridad.
5	Informes de Auditoría y Gestión de Hallazgos	5.1. Planificación y preparación de una auditoria. 5.2. Recolección de evidencia y análisis de datos. 5.3. Pruebas de penetración y análisis de vulnerabilidades.

		5.4. Redacción de informes de auditoría. 5.5. Presentación de resultados a la gerencia.

7. Actividades de aprendizaje de los temas

1. Introducción a la Auditoria en Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer los diferentes tipos de auditorías de ciberseguridad: Auditorías de redes, auditorías de aplicaciones, auditorías de sistemas operativos, auditorías de datos, etc. • Identificar y clasificar las amenazas, vulnerabilidades y riesgos de ciberseguridad: Comprender las diferentes categorías de amenazas, vulnerabilidades y riesgos, y cómo pueden afectar a una organización. • Realizar un análisis de riesgos de ciberseguridad: Identificar los activos de una organización que son más vulnerables a los ataques cibernéticos, y evaluar el impacto potencial de esos ataques *Genérica(s):* ● Pensamiento crítico y resolución de problemas ● Comunicación y trabajo en equipo ● Aprendizaje continuo ● Ética y responsabilidad profesional ● Habilidades informáticas y tecnológicas ● Capacidad de análisis ● Atención al detalle ● Orientación a resultados ● Capacidad de adaptación ● Adaptabilidad y Flexibilidad ● Creatividad e innovación ● Iniciativa y proactividad ● Liderazgo	● Estudios de casos: La presentación de estudios de casos reales o simulados permite a los estudiantes analizar situaciones concretas de vulnerabilidades y ataques cibernéticos, así como las medidas de auditoría implementadas para identificarlos y mitigarlos ● Simulaciones de auditoría: La realización de simulaciones de auditoría permite a los estudiantes poner en práctica los conocimientos y habilidades adquiridos, simulando el proceso completo de una auditoría en ciberseguridad. Esto incluye la planificación, la recopilación de evidencia, el análisis de riesgos, la elaboración de informes y la presentación de hallazgos. Las simulaciones pueden realizarse de forma individual o grupal, utilizando herramientas y metodologías específicas de auditoría. ● Juegos de roles: Los juegos de roles permiten a los estudiantes asumir diferentes roles en el contexto de una auditoría en ciberseguridad, como auditores, responsables de seguridad de la información o directivos.

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.	
2. Procesos de Auditoría en Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): ● Conocimiento profundo de los principios y prácticas de seguridad de la información: Esto incluye comprender conceptos como la confidencialidad, integridad y disponibilidad de la información, así como las diferentes amenazas y vulnerabilidades que pueden afectar a los sistemas de información. ● Experiencia en la realización de auditorías de seguridad de la información: Esto implica tener conocimiento de las diferentes metodologías de auditoría, así como la capacidad de planificar, ejecutar y documentar auditorías de manera efectiva. ● Conocimiento de las normas y regulaciones de seguridad de la información: Esto incluye comprender las normas ISO 27001, NIST Cybersecurity Framework y PCI DSS, entre otras.	● Desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. Las actividades que engloban esta función son fundamentales para el uso efectivo del marco. ● Describir las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. ● Definir las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo su descubrimiento oportuno. ● Incluir actividades necesarias para tomar medidas frente a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial ataque. ● Identificar las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado como consecuencia de un incidente de ciberseguridad.

Genérica(s): ● Pensamiento crítico y resolución de problemas ● Comunicación y trabajo en equipo ● Aprendizaje continuo ● Ética y responsabilidad profesional ● Habilidades informáticas y tecnológicas ● Capacidad de análisis ● Atención al detalle ● Orientación a resultados ● Capacidad de adaptación ● Adaptabilidad y Flexibilidad ● Creatividad e innovación ● Iniciativa y proactividad ● Liderazgo *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	
3. Normativas, Estándares y Evaluación de Riesgos	
Competencias	Actividades de aprendizaje
Específica(s): ● Comprensión profunda de las principales normativas y estándares de ciberseguridad a nivel nacional e internacional, como ISO/IEC 27001, NIST Cybersecurity Framework, PCI	● Gestionar información sobre la normatividad vigente aplicable en auditorías informáticas y preparar una exposición de 20 minutos. ● Discutir en grupo la justificación sobre alguna de las normas considerada para las normas,

DSS, GDPR, Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), entre otras. ● Capacidad para interpretar y aplicar estas normativas y estándares en el contexto de una organización específica. ● Conocimiento de las últimas tendencias y desarrollos en el ámbito de las normativas y estándares de ciberseguridad. *Genérica(s):* ● Pensamiento crítico y resolución de problemas ● Comunicación y trabajo en equipo ● Aprendizaje continuo ● Ética y responsabilidad profesional ● Habilidades informáticas y tecnológicas ● Capacidad de análisis ● Atención al detalle ● Orientación a resultados ● Capacidad de adaptación ● Adaptabilidad y Flexibilidad ● Creatividad e innovación ● Iniciativa y proactividad ● Liderazgo *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	estándares y evaluación de riesgos, según el contexto. ● Identificar un área de ciberseguridad dentro de cualquier organización en la cual se pueda iniciar el proceso de normas, estándares y evaluación de riesgos.

aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	
4. Auditoría de Sistemas y Redes	
Competencias	Actividades de aprendizaje
Específica(s): ● Sólido conocimiento de sistemas operativos, redes y protocolos de comunicación: El auditor debe comprender cómo funcionan los sistemas informáticos y las redes para poder identificar vulnerabilidades y evaluar la efectividad de las medidas de seguridad. ● Conocimiento profundo de las amenazas y vulnerabilidades de ciberseguridad: El auditor debe estar actualizado sobre las últimas amenazas y vulnerabilidades, y saber cómo identificarlas y evaluar su impacto potencial. ● Experiencia en herramientas y técnicas de auditoría de seguridad: El auditor debe saber cómo utilizar una variedad de herramientas y técnicas para realizar auditorías de seguridad, como escáneres de vulnerabilidades, herramientas de análisis de red y software de prueba de penetración. ● Conocimiento de las normas y regulaciones de ciberseguridad: El auditor debe estar familiarizado con las normas y regulaciones relevantes para la ciberseguridad, como ISO 27001, NIST Cybersecurity Framework y PCI DSS. *Genéricas:* • Pensamiento crítico y resolución de problemas	● Realizar un checklist para la obtención de la información necesaria sobre la auditoria de sistemas y redes. ● Evaluar el nivel de aplicación de las normas y/o estándares implementados en sistemas y redes sobre su administración, instalación, operación, seguridad y personal responsable, emitiendo hallazgos y recomendaciones. ● Discutir en grupo la finalidad e impacto de la evaluación de sistemas y redes. ● Gestionar información sobre los puntos del tema y escribir los resultados en un resumen.

• Comunicación y trabajo en equipo • Aprendizaje continuo • Ética y responsabilidad profesional • Habilidades informáticas y tecnológicas • Capacidad de análisis • Atención al detalle • Orientación a resultados • Capacidad de adaptación • Adaptabilidad y Flexibilidad • Creatividad e innovación • Iniciativa y proactividad • Liderazgo *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.	
5. Informes de Auditoría y Gestión de Hallazgos	
Competencias	Actividades de aprendizaje
Específica(s): ● Comprensión profunda de los principios y conceptos fundamentales de la ciberseguridad, incluyendo redes, sistemas operativos, aplicaciones, malware, vulnerabilidades y amenazas. ● Conocimiento actualizado de las últimas tendencias, técnicas y procedimientos en ciberseguridad.	● Investigar los principales elementos de la auditoría y gestión de hallazgos. ● Desarrollar una Auditoría en ciberseguridad de una empresa del entorno. ● Gestionar información que le permita ● identificar la terminología y el contexto de las auditorías y gestión de hallazgos en ciberseguridad, así como las herramientas computacionales para planear y ejecutar una auditoría, plasmar sus resultados en un resumen y compartir en grupo.

• Capacidad para planificar, realizar y documentar auditorías de ciberseguridad de manera sistemática y rigurosa. • Habilidad para identificar, evaluar y clasificar vulnerabilidades y riesgos de seguridad. • Capacidad para recopilar y analizar evidencia de manera efectiva. • Habilidad para redactar informes de auditoría claros, concisos y completos *Genérica(s):* • Pensamiento crítico y resolución de problemas • Comunicación y trabajo en equipo • Aprendizaje continuo • Ética y responsabilidad profesional • Habilidades informáticas y tecnológicas • Capacidad de análisis • Atención al detalle • Orientación a resultados • Capacidad de adaptación • Adaptabilidad y Flexibilidad • Creatividad e innovación • Iniciativa y proactividad • Liderazgo 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)

- Realizar un análisis de vulnerabilidades en un sistema operativo Windows 10.
- Auditar la seguridad de una red doméstica.
- Evaluación de Políticas de Seguridad
- Redactar un informe de auditoría de seguridad sobre una pequeña empresa.
- Simulación de presentación de informe de auditoría

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

- Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales, ensayos, reporte de investigación y/o revisiones bibliográficas, reportes de prácticas, estudio de casos, exposiciones en clase, portafolio de evidencias.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, rúbricas, entre otros.

11. Fuentes de Información

1. "Auditing and Assurance Services" Alvin A. Arens, Randal J. Elder, Mark S. Beasley.

2. “Auditoria de Seguridad Informática - Una Guía Práctica” Michael E. Whitman y Herbert J. Mattord
3. “IT Auditing: Using Controls to Protect Information Assets” Chris Davis y Mike Schiller
4. "ISO/IEC 27001:2013 - A Pocket Guide" Alan Calder
5. “Information Security: The Complete Reference” Mark Rhodes-Ousley.
6. “The Basics of IT Audit: Purposes, Processes, and Practical Information” Stephen D. Gantz.
7. "Computer Security Handbook" Seymour Bosworth, M.E. Kabay, Eric Whyne.
8. “NIST Cybersecurity Framework” National Institute of Standards and Technology
9. “Control de Seguridad de la Información para la Protección de Datos Personales” Ana Marzo Portera
10. “Auditoría de la seguridad informática. Curso práctico” Silvia Clara Menéndez Arantes
11. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI