1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos de ciberseguridad.
Clave de la asignatura:	CID2601
SATCA[1]:	2 -3 – 5
Carrera:	• Ingeniería en Sistemas Computacionales • Ingeniería en Tecnologías de la Información y Comunicaciones • Ingeniería en Inteligencia Artificial • Ingeniería en Ciencia de Datos • Ingeniería en Desarrollo de Aplicaciones. • Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

La asignatura de **fundamentos de ciberseguridad** se encuentra en el semestre del módulo de especialidad formando parte de un grupo de asignaturas de la misma llamada **ciberseguridad**. Y se relaciona con las competencias del perfil de egreso: Identificar y comprender las tecnologías de hardware para proponer, desarrollar y mantener aplicaciones eficientes y administrar bases de datos conforme a requerimientos definidos, normas organizacionales de manejo y seguridad de la información, utilizando tecnologías emergentes.

La importancia de la asignatura se relaciona con la formación profesional de los alumnos en los conceptos y técnicas básicas para proponer estrategias preventivas en materia de Ciberseguridad, para salvaguardar la seguridad integral en la red de datos personales y confidenciales, sistemas y equipos de información.

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad de identificar las amenazas y vulnerabilidades que existe en la infraestructura de red de una organización, de tal forma que puede hacer un análisis de riesgos.

Además, permite identificar e integrar los mecanismos de seguridad y la infraestructura tecnológica necesaria para asegurar la disponibilidad, confidencialidad e integridad de la información en las redes de computadoras.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

©TecNM 2025

Permite también al alumno, aplicar mecanismos de mejora continua en los servicios de tecnologías de información y comunicaciones, encaminados a satisfacer las necesidades de los usuarios.

Proporciona al estudiante la capacidad necesaria para diseñar aplicaciones Web con los mecanismos de seguridad necesarios para su funcionalidad.

Intención didáctica

Las amenazas cibernéticas nos afectan a todos, y los trabajos de ciberseguridad continúan creciendo. De hecho, las fallas de ciberseguridad se encuentran entre los 5 principales riesgos globales según el Informe de Riesgos Globales del Foro Económico Mundial (2021). El mundo necesita profesionales diversos y con habilidades tecnológicas en ciberseguridad para defenderse de adversarios digitales astutos.

Aprenderá habilidades vitales como inteligencia de amenazas, seguridad de la red y gestión de riesgos para protegerse y proteger a las organizaciones de los ataques cibernéticos.

El temario del curso se ha organizado en seis unidades cada una conformada por contenidos que contribuirán al buen aprendizaje de esta materia. El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el manejo de estándares, protocolos, métodos, reglas, herramientas y leyes que permitan minimizar los posibles riesgos a la infraestructura o a la información. Para esta asignatura se requiere de conocimientos sobre software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas.

Además, se contempla el desarrollo de habilidades para el planteamiento de problemas, trabajo en equipo, asimismo, elementos que propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; las actividades teóricas se han descrito como actividades previas al tratamiento práctico de los temas. En las actividades prácticas sugeridas, es conveniente que el profesor solo guie al estudiante en la construcción de su conocimiento.

En la unidad I y II el alumno evaluará la vulnerabilidad y aplicará protecciones básicas para la red, los sistemas operativos y las terminales. Su red consta de software, hardware y medios. Los sistemas operativos hacen posible el uso del hardware en su red. Enpoints o terminales, son los dispositivos como computadoras, servidores, teléfonos móviles y tabletas que se utilizan en su red. El conocimiento y las habilidades que aprenderá lo ayudarán a mantener la integridad, confidencialidad y disponibilidad de su red y sus datos.

©TecNM 2025

En la unidad II, IV y V se proporciona conocimientos y habilidades básicas e intermedias que utilizará todos los días en su rol de técnico en ciberseguridad. Aprenderá sobre diferentes maneras de monitorear su red y cómo evaluar las alertas que recibe. Profundizará en las herramientas y técnicas utilizadas para proteger su red, incluidos el control de acceso, los firewalls, la seguridad en la nube y la criptografía. Estas herramientas de supervisión y defensa, junto con otras, trabajan juntas para crear una estrategia de ciberseguridad de defensa en profundidad por capas. El conocimiento y las habilidades que aprenderán lo ayudarán a defender las redes contra muchos tipos de ataques y a reaccionar rápidamente ante cualquier ataque que pueda ocurrir.

En la última unidad, el estudiante creará documentos de políticas que cubran la gobernanza y el cumplimiento. Aprenderá sobre el cumplimiento de estándares de ética y marcos legales y regulatorios. Además, evaluará la vulnerabilidad de la red y los sistemas y creará un plan de gestión de riesgos. Finalmente, aprenderá sobre la respuesta posterior a un incidente, incluidas las investigaciones forenses, los métodos de recuperación y la planificación de la respuesta a incidentes. Todas estas acciones son aspectos críticos de la seguridad de la red.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México, campus Tuxtla Gutiérrez del 18 septiembre al 26 de octubre de 2024	Representantes de los Institutos Tecnológicos de: Tuxtla Gutiérrez • Francisco de Jesús Suárez Ruiz. • María Guadalupe Monjaras Velasco	Foro Estatal Actualización Curricular para la Consolidación de Proyectos Estratégicos del TecNM en el Estado de Chiapas

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Diseña mecanismos de Ciberseguridad para redes de computadoras, desarrolla algoritmos de cifrado de datos, e implementa esquemas lógicos de seguridad para apoyar la productividad de las organizaciones. Diseñar e implementar políticas y procedimientos de seguridad, considerando las mejores prácticas y estándares internacionales, de forma ética y profesional en el campo de la ciberseguridad, para garantizar la integridad, confidencialidad y disponibilidad de la información en sistemas y redes informáticas.

©TecNM 2025

Identificar y evaluar riesgos informáticos, aplicando técnicas y herramientas de análisis de riesgos, para proponer soluciones efectivas de seguridad informática y minimizar los riesgos en sistemas y redes informáticas.

Gestionar y administrar la seguridad de redes y sistemas informáticos, aplicando las mejores prácticas y estándares internacionales, de forma ética y profesional en el campo de la ciberseguridad, para garantizar la protección de la información y la prevención de riesgos informáticos.

Investigar y analizar incidentes de seguridad informática, en el campo del de cómputo forense, para identificar la causa raíz y proponer soluciones efectivas para prevenir futuros incidentes.

Comunicar de manera efectiva los resultados de las investigaciones y análisis forenses informáticos, a través de informes, cumpliendo con las mejores prácticas y estándares internacionales, de forma ética y profesional en el campo de la ciberseguridad.

- Explicar principios de seguridad de la red, cómo las vulnerabilidades de TCP/IP permiten los ataques a las redes, cómo los agentes de amenazas ejecutan algunos de los tipos más comunes de ataques cibernéticos, cómo se emplean los dispositivos y servicios para reforzar la seguridad de las redes, los enfoques para la defensa de la seguridad de la red, proceso de evaluación de alertas, cómo se evalúan y administran las vulnerabilidades de las terminales, cómo las tecnologías de seguridad afectan el monitoreo de la seguridad, cómo se implementan los firewalls para proporcionar seguridad de red.

- Utilizar los comandos para verificar la vulnerabilidad de las aplicaciones y los servicios de red, las mejores prácticas de ciberseguridad para proteger los archivos, diferentes tipos de registros y registros para almacenar información sobre hosts y la red, herramientas para las pruebas de seguridad de la red.
- Implementar la seguridad básica de Linux, listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red, firewall de políticas basado en zonas mediante la CLI.
- Evaluar la protección de terminales y los impactos del malware, los controles de seguridad de acuerdo con los requisitos de cumplimiento ético, regulatorio y legal, las fuentes de inteligencia de amenazas.
- Configurar el control de acceso local y basado en el servidor.
- Recomendar requisitos de seguridad en la nube basados en un escenario de nube determinado.
- Determinar las técnicas criptográficas necesarias para garantizar la confidencialidad, la integridad y la autenticidad.

©TecNM 2025

- Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos. Utilizar modelos de respuesta a incidentes y técnicas forenses para investigar incidentes de seguridad.

5. Competencias previas

Competencias específicas:

- Explica los conceptos básicos de la seguridad en línea, lo que incluye qué es la ciberseguridad y su impacto potencial, cómo las organizaciones pueden proteger sus operaciones contra estos ataques, las amenazas, los ataques y las vulnerabilidades más comunes.

- Explica conceptos importantes en la comunicación de red, los tipos de red, los componentes y las conexiones, la importancia de los estándares y protocolos en las comunicaciones de red, cómo se produce la comunicación en las redes Ethernet, las funciones de una dirección IP, cómo se usan las direcciones IPv4 en la comunicación y la segmentación de la red, las características del direccionamiento IPv6, cómo los routers conectan las redes entre sí, cómo ARP y ND permiten la comunicación en una red, cómo acceden los clientes a los servicios de Internet, la función de los servicios comunes de la capa de aplicación, como utiliza varias herramientas para probar y solucionar problemas de conectividad de red.
- Configura dispositivos móviles para conectividad inalámbrica, un enrutador inalámbrico integrado y clientes inalámbricos para que se conecten de manera segura a Internet, Configura un servidor DHCP.

Aplicar conocimientos y habilidades en redes de computadoras, para diseñar y gestionar redes seguras y protegidas contra riesgos informáticos.

Utilizar técnicas y herramientas de programación, para desarrollar aplicaciones seguras y protegidas contra vulnerabilidades informáticas.

Aplicar conocimientos y habilidades en bases de datos, para diseñar y gestionar bases de datos seguras y protegidas contra riesgos informáticos.

Utilizar técnicas y herramientas de sistemas operativos, para implementar y gestionar sistemas operativos seguros y protegidos contra riesgos informáticos.

Aplicar conocimientos y habilidades en auditoria de sistemas y seguridad en redes y sistemas, para evaluar y auditar la seguridad informática en sistemas y

©TecNM 2025

redes informáticas, y proponer soluciones efectivas para minimizar riesgos y prevenir incidentes de seguridad.

Competencias genéricas:

- Capacidad de análisis y síntesis.
- Capacidad de organizar y planificar.
- Comunicación oral y escrita.
- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Solución de problemas.
- Toma de decisiones.
- Capacidad crítica y autocrítica.
- Capacidad de trabajar en equipo.
- Capacidad de comunicar sus ideas.
- Capacidad de liderazgo.
- Capacidad de aplicar los conocimientos en la práctica.
- Habilidades de investigación.
- Capacidad de adaptarse a nuevas situaciones.
- Capacidad de generar nuevas ideas (creatividad).

6. Temario

No	Temas	Subtemas
1	Introducción a la Ciberseguridad	1.1 Introducción a la ciberseguridad. 1.2 Ataques, conceptos y técnicas. 1.3 Protegiendo sus datos y su 1.4 privacidad. 1.5 Protegiendo a la organización. 1.6 El futuro y la ciberseguridad.
2.	Seguridad de la red.	2.1 Amenazas, vulnerabilidades y ataques a la ciberseguridad. 2.2 Protección de redes. 2.3 Ataque a los fundamentos. 2.4 Atacando lo que hacemos. 2.5 Comunicación de red Inalámbrica. 2.6 Infraestructura de seguridad de redes.
3.	Sistemas operativos y seguridad de puntos finales.	3.1 Sistema operativo Windows. 3.2 Descripción general de Linux. 3.3 Protección de terminales. 3.4 Principios prácticas y procesos de ciberseguridad.

©TecNM 2025

4.	Principios, prácticas y procesos de defensa de la red.	4.1 Comprendiendo que es defensa. 4.2 Defensa del sistema y de la red. 4.3 Control de acceso. 4.4 Lista de control de acceso. 4.5 Tecnologías firewall. 4.6 Firewalls de políticas basadas en zondas. 4.7 Seguridad en la nube. 4.8 Criptografía.
5.	Evaluación de alertas de seguridad, vulnerabilidad y gestión de riesgos. (Administración de Amenazas Cibernéticas)	5.1 Tecnologías y protocolos. 5.2 Datos de seguridad de red. 5.3 Evaluar alertas. 5.4 Gestión y cumplimiento. 5.5 Pruebas de seguridad de la red. 5.6 Inteligencia contra las amenazas. 5.7 Evaluación de vulnerabilidades de las terminales. 5.8 Administración de riesgos y controles de seguridad.

7. Actividades de aprendizaje de los temas

Introducción a la Ciberseguridad	
Competencias	Actividades de aprendizaje
Explicar los conceptos básicos de la seguridad en línea, lo que incluye qué es la ciberseguridad y su impacto potencial. Explicar las amenazas, los ataques y las vulnerabilidades más comunes. Explicar cómo las organizaciones pueden proteger sus operaciones contra estos ataques. **Genéricas:** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo	Leer las diapositivas de la Unidad “Introducción a la ciberseguridad”. Realizar la práctica de laboratorio: ¿Quién posee sus datos? Realizar el ejercicio “ejemplos de brechas de seguridad”. Analizar el diagrama “árbol de decisiones ético”. Responder la encuesta “Introducción a la ciberseguridad”

©TecNM 2025

virtualizado Solución de problemas Toma de decisiones	

Seguridad de la red.	
Competencias	Actividades de aprendizaje
Específica(s): asignatura Explicar las amenazas, vulnerabilidades y ataques que ocurren en los distintos dominios. Explicar los principios de seguridad de la red. Explicar como las vulnerabilidades TCP/IP permiten que se ejecuten ataques a las redes. Recomendar medidas para mitigar las amenazas. Resolver problemas de redes empresariales. Explicar como se emplean los dispositivos y servicios para forzar la seguridad de las redes. **Genéricas:** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado Solución de problemas Toma de decisiones	Leer las diapositivas de la Unidad (Endpoint Security V1.0) y realizar una lluvia de conceptos, para identificar los elementos esenciales. Realizar prácticas guiadas con la herramienta Packet Tracer. a) Exploración de modos lógicos y físicos. b) Configuración de la seguridad inalámbrica básica. c) Solución de problemas de conexión inalámbrica. Responder los cuestionarios: a) Seguridad de la red.
Sistemas operativos y seguridad de puntos finales.	
Competencias	Actividades de aprendizaje
Específica(s): Utilizar herramientas administrativas de windows.	Realizar prácticas guiadas con la herramienta Packet Tracer. a) Demostración de ACL

©TecNM 2025

Implementar la seguridad basica de linux. Evaluar la protección de terminales y los impactos del malware. Utilizar las mejores practicas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad. Genéricas: Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado Solución de problemas Toma de decisiones	b) Exploración del cifrado de archivos y datos. c) Investigar un panorama de amenazas. d) Verificación de la integridad de Datos y Archivos. Realizar los laboratorios: a) Recuperar contraseñas. b) El cubo de hechicería de ciberseguridad. Responder los cuestionarios: a) Sistemas operativos y seguridad de puntos final. b) Seguridad de terminales.
Principios, prácticas y procesos de defensa de la red.	
Competencias	Actividades de aprendizaje
Específica(s): Explicar enfoques para la defensa de seguridad de la red. Poner en práctica algunos de los diversos aspectos de la defensa de sistemas y redes. Configurar el control de acceso local y basado en el servidor. Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red. Explicar como se implementan los firewalls para proporcionar seguridad de red. Implementar frewall asaso en políticas de zona mediante la CLI.	Realizar prácticas guiadas con la herramienta Packet Tracer. a) Exploración de modos lógicos y físicos. b) Configuración de listas de control de acceso (ACL) de IP para mitigar ataques. c) Configuración ZPF. Realizar los laboratorios a) configuración de la protección y la seguridad del enrutador inalámbrico. b) Configurar autenticación y autorización en Linux. c) Packet Tracer: configuración de la autenticación basada en servidor con TACACS+ y RADIUS.

©TecNM 2025

Recomendar requisitos de seguridad en la nube basados en un escenario de nube determinado. Explicar como utilizar las herramientas de hash. Genéricas: Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado Solución de problemas Toma de decisiones	d) configuración de listas de control de acceso extendidas Escenario 1. e) configuración de listas de control de acceso (ACL) IPv4 estándar numeradas. f) configuración de listas de control de acceso (ACL) IPv4 estándar con nombre. g) Configurar listas de control de acceso (ACL) de IPv6 Responder los cuestionarios. a) Principios, prácticas y procesos de defensa de la red. b) Firewalls, criptografía y seguridad en la nube.
Evaluación de alertas de seguridad.	
Competencias	Actividades de aprendizaje
Específica(s): Explicar cómo las tecnologías de seguridad afectan el monitoreo de la seguridad. Utilizar diferentes tipos de logs y registros para almacenar información sobre los hosts y la red. Explicar el proceso de evaluación de alertas. Genéricas: Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo virtualizado Solución de problemas	Realizar prácticas guiadas con la herramienta Packet Tracer. a) Explorar una implementación de NetFlow. b) Registro desde varias fuentes. Realizar los laboratorios: a) Snort and Firewall Rules. b) Classify Alerts Realizar los cuestionarios a) “Evaluación de alertas de seguridad”. b) Defensa de la red (NetDef)

©TecNM 2025

Toma de decisiones	
Evaluación de vulnerabilidad y gestión de riesgos	
Competencias	Actividades de aprendizaje
Específica(s): Evaluar los controles de seguridad de acuerdo con los requisitos de cumplimiento ético, regulatorio y legal. Utilizar herramientas para las pruebas de seguridad de la red. Evaluar las fuentes de inteligencia de amenazas. Explicar cómo se evalúan y administran las vulnerabilidades de los terminales. Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos. Utilizar modelos de respuesta a incidentes y técnicas forenses para investigar incidentes de seguridad. Genéricas: Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidades intelectuales para el desarrollo de un entorno informativo	Realizar prácticas guiadas con la herramienta Packet Tracer. a) Exploración de modos lógicos y físicos. b) Investigar la recuperación ante un desastre. c) Uso de comandos de diagnóstico. Realizar los laboratorios: a) Uso de Wireshark para comparar el tráfico Telnet y SSH. b) Evaluación de informes de ciberseguridad. c) Identificar información relevante sobre amenazas. d) Evaluación de vulnerabilidades. e) Gestión de riesgos. f) Análisis de riesgos. g) Análisis de ataques. h) Manejo de incidentes. i) Recomendar medidas de recuperación ante desastres. Realizar los cuestionarios a) Evaluación de vulnerabilidad y gestión de riesgos. b) Respuesta a incidentes.

©TecNM 2025

virtualizado Solución de problemas Toma de decisiones	

8. Práctica(s)

Unidad I. Realizar la práctica guiadas con la herramienta Packet Tracer.

a) ¿Quién posee sus datos?

Unidad II. Realizar prácticas guiadas con la herramienta Packet Tracer.

a) Exploración de modos lógicos y físicos.
b) Configuración de la seguridad inalámbrica básica.
c) Solución de problemas de conexión inalámbrica.

Unidad III. Realizar prácticas guiadas con la herramienta Packet Tracer.

a) Demostración de ACL
b) Exploración del cifrado de archivos y datos.
c) Investigar un panorama de amenazas.
d) Verificación de la integridad de Datos y Archivos.

Unidad IV. Realizar prácticas guiadas con la herramienta Packet Tracer.

a) Exploración de modos lógicos y físicos.
b) Configuración de listas de control de acceso (ACL) de IP para mitigar ataques.
c) Configuración ZPF.

Unidad V. Realizar prácticas guiadas con la herramienta Packet Tracer.

a) Exploración de modos lógicos y físicos.
b) Investigar la recuperación ante un desastre.
c) Uso de comandos de diagnóstico.

9. Proyecto de asignatura

©TecNM 2025

Obtener un proyecto de Fundamentos de Ciberseguridad para identificar y evaluar riesgos informáticos, aplicando técnicas y herramientas de análisis de riesgos, para proponer soluciones efectivas de seguridad informática y minimizar los riesgos en sistemas y redes informáticas, en una organización.

Fundamentación:

En la actualidad, las organizaciones manejan grandes cantidades de información y datos importantes que deben ser protegidos de posibles amenazas y ataques cibernéticos. Estos ataques pueden causar danos irreparables en la organización, como la perdida de datos, el robo de información confidencial, la interrupción de los servicios y la afectación a la reputación de la organización.

Por lo tanto, es importante contar con un proyecto de fundamentos de ciberseguridad que permita identificar y evaluar los riesgos informáticos a los que está expuesta la organización, aplicando técnicas y herramientas de análisis de riesgos. De esta manera, se podrán proponer soluciones efectivas de seguridad informática y minimizar los riesgos en sistemas y redes informáticas, para proteger la información y los datos importantes de la organización. Además, contar con un proyecto de fundamentos de ciberseguridad permite cumplir con las normativas y regulaciones en materia de seguridad informática, lo que puede ser un factor importante para la reputación y el éxito de la organización.

El alumno deberá integrar el conocimiento con respecto a las siguientes temáticas:

- Deberá integrar conocimientos sobre los conceptos básicos de ciberseguridad, técnicas y herramientas de análisis de riesgos.

- identificación de amenazas y vulnerabilidades, soluciones de seguridad informática y cumplimiento normativo, para poder identificar y evaluar riesgos informáticos.

- Proponer soluciones efectivas de seguridad informática y minimizar los riesgos en sistemas y redes informáticas, en una organización.

Planeación:

Una planificación para 16 semanas acotadas de 4 en 4, para el proyecto de Fundamentos de Ciberseguridad para identificar y evaluar riesgos informáticos, aplicando técnicas y herramientas de análisis de riesgos, para proponer soluciones efectivas de seguridad informática y minimizar los riesgos en sistemas y redes informáticas, en una organización:

©TecNM 2025

Primer Bloque (semana 1 a la 4)

1.- Introducción al proyecto y conceptos básicos de ciberseguridad.
2.- Identificación de los principales riesgos informáticos y las amenazas a los sistemas y redes informáticas.

3.- Técnicas de análisis de riesgos.

Segundo Bloque (semana 5 a la 8)

1.- Metodologías de análisis de riesgos, como la norma ISO/IEC 27005.

2.- Identificación de vulnerabilidades y soluciones de seguridad informática.

Tercer Bloque (semana 9 a la 12)

1.- Análisis cualitativo y cuantitativo de riesgos informáticos.

2.- Implementación de soluciones de seguridad informática.

Cuarto Bloque (semana 13 a la16)

1.- Evaluación de la efectividad de las soluciones de seguridad informática implementadas.

2.- Cumplimiento normativo en materia de seguridad informática. 3.- Presentación del proyecto.

Ejecución:

La ejecución del proyecto deberá ser realizada en colaboración con la organización ya que se requerirá acceso a los sistemas y redes informáticas de la misma. Además, se deberá contar con el apoyo de los responsables de seguridad informática de la organización para la implementación de las soluciones de seguridad informática seleccionadas y la evaluación de su efectividad.

©TecNM 2025

Evaluación:

El proceso de evaluación del proyecto se realizará por cada bloque realizado para su integración, para lo cual se validará con lo que indica el docente en su matriz de evaluacion

1.- Evaluación de la efectividad de las soluciones de seguridad informática implementadas.

2.- Cumplimiento normativo en materia de seguridad informática. 3.- Presentación del proyecto.

1. **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.

2. **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.

3. **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 las competencias genéricas y especificas a desarrollar.

4. **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”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

©TecNM 2025

10. Evaluación por competencias

Evaluación formativa	
Producto o Evidencia de aprendizaje	Instrumento de evaluación
Lista de cotejo de mapa conceptual	Lista de cotejo de mapa conceptual: palabras clave, organización, jerarquía, enlaces.
Presentación grupal: Cómputo en la nube	Rúbrica de presentación de temas relacionados a ciberseguridad, categorías:
	-Se identifican claramente las ideas primarias de las ideas secundarias. -El organizador gráfico está ordenado. -Las relaciones entre conceptos presentan jerarquías. -No hay errores ortográficos en la presentación -Se observa la preparación del tema, el uso de referencias empleadas y un orden de ideas. -Se observa seguridad al tratar el tema, buen uso del recurso de apoyo, fluidez de ideas, tono de voz adecuado.
Infografía	Evaluar la infografía respetando los siguientes indicadores de logro: – El título es llamativo, está centrado en la lámina y está acompañado de una imagen principal. – Formato de texto según las instrucciones dadas por la docente (tamaño de fuente, interlineado, sangría, alineación, entre otros). – Utiliza imágenes relacionadas con el contenido. – Hace uso de elementos llamativos que ayudad a reforzar la información (flechas, formas, figuras geométricas, entre otras) – Organización coherente del contenido. (desde lo más complejo a lo más específico) – Se evidencia originalidad en la elaboración de la infografía. – Ordena la información de manera que sea comprensible representativa del tema sugerido.

©TecNM 2025

Elaboración de un objeto de aprendizaje: vídeo.	▪ Lista de cotejo, indicadores de logro para el desarrollo del proyecto: ✓ El sonido es adecuado, la voz es fluida, no hay sonidos que interrumpan y se entiende cuando pasa de una idea a otra. ✓ El vídeo está bien grabado, presenta imágenes sin pixelear y hay apoyos gráficos. ✓ El recurso presenta la información de forma objetiva, no presenta errores u omisiones que pudieran confundir o equivocar la interpretación de los contenidos. ✓ Enfatiza los puntos clave y las ideas más significativas con un nivel adecuado de detalle. ✓ El recurso es útil para generar aprendizajes con respecto al tema que aborda. ✓ Presenta información de forma clara y precisa, incluyendo ejemplos o demostraciones de uso del recurso para el uso en la enseñanza. ✓ El recurso presenta al final las fuentes de información que permiten respaldar los contenidos que se presentan. ✓ El recurso se encuentra en la nube y la liga de acceso puede abrirse desde cualquier dispositivo.

Evaluación del proyecto: Configuración, instalación y desarrollo de un Sistema operativo seguro.	Indicadores de logro que se tienen que cumplir: _Analizamos los requerimientos de desarrollo de software _Identificamos los algoritmos de cifrado mediante el lenguaje de programación orientada a objetos _Configuramos el servicio dns y aseguirarlo mediante políticas de seguridad. _Definimos la estrategia de pruebas. _Definimos los criterios de funcionalidad, codificación y documentación. _Identificamos los entornos (ambientes) requeridos. _Determinamos necesidades de personal y entrenamiento. _Establecimos procedimientos de prueba.
Autoevaluación del equipo:	Preguntas de reflexión: ¿qué problemáticas se identificaron? ¿Qué necesitamos aprender?, ¿qué temas debo estudiar de manera individual para mejorar mi desempeño en el equipo? ¿qué decisiones tuvo que tomar el equipo para resolver el problema?, ¿en qué áreas de aprendizaje relacionadas con los resultados me considero experto?.

©TecNM 2025

Evaluación sumativa:

1. Participación en clases
2. Evidencias de productos y desempeños en la plataforma
3. Portafolio de aprendizaje personal
4. Autoevaluación

11. Fuentes de información

Anderson, R. J. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley. ISBN: 978-1-119-64281-7. Recuperado de: https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642817

Bancal, D., Beirnaert, J., Clarhaut, J., Crocfer, R. Fortunato, G., Lasson S., Rault, R., Schalkwijk, L., & Vicogne, F. (2023). *Seguridad Informatica: Ethical*

Hacking. Conocer el ataque para una mejor defensa, 5a. edicion. Epsilon. ISBN: 978-2-409-03914-0. Recuperado de: https://www.ediciones-eni.com/libro/seguridad-informatica-ethical-hacking-conocer-el-ataque- para-una-mejor-defensa-5a-edicion-9782409039140

Cano M., J. J., & Rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital/Cybersecurity and cyberdefense. Challenges and perspectives in a digital world. *RISTI* [Revista Iberica de Sistemas e Tecnologias de Informacao], (32), vii+. https://link.gale.com/apps/doc/A596318112/AONE?u=anon~5e6b180a&sid=googleScholar&xid=96472cce

Villa, E., & Morales, I. (2022). Ciberseguridad IoT y su aplicación en Ciudades Inteligentes. (2022). España: RA-MA S.A. Editorial y Publicaciones.

Recuperado https://www.google.com/books/edition/Ciberseguridad_IoT_y_su_aplicaci%C3%B3n_en_Ci/41W6EAAAQBAJ?kptab=editions&gbpv=1

©TecNM 2025

Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., Álava Cruzatty, J. E., Figueroa Morán, G. L., Vera Navarrete, D. S., Romero Castro, M. I., Castillo Merino, M. A. (2018). INTRODUCCIÓN A LA

SEGURIDAD INFORMÁTICA Y EL ANÁLISIS VULNERABILIDADES. España: 3Ciencias. Recuperado https://www.google.com.mx/books/edition/INTRODUCCI%C3%93N_A_LA_SEGURIDAD_INFORM%C3%81TIC/5Z9yDwAAQBAJ?hl=es&gbpv=1&dq=de,+I.+M.+(2022).+CIENCIA+DE+DATOS+PARA+LA+CIBERSEGURIDAD.+Ra-Ma.&printsec=frontcover

Lewis, E. (2020). Ciberseguridad: Guía completa para principiantes aprende todo de la ciberseguridad de la Aa la Z(Libro En Español/Spanish version). (n.p.): Independently Published. Recuperado de: https://www.google.com.mx/books/edition/Ciberseguridad/7ruHzQEACAAJ?hl=es

Tejerina, O. (2022). Aspectos jurídicos de la ciberseguridad. Ed. Ra-Ma. ISBN: 9788499649719 . Recuperado de: https://www.gandhi.com.mx/aspectos-juridicos-de-la-ciberseguridad

Romero, F. M. (2021). *Manual básico de ciberseguridad y protección de datos.* Exit. ISBN: 9788497443203.

Lopez Torres, Jonathan. (2023). *Ciberespacio & Ciberseguridad. Elementos Esenciales.* Tirant Lo Blanch. ISBN: 9788413550688. Recuperado de: https://www.gonvill.com.mx/libro/ciberespacio-ciberseguridad-elementos-esenciales-lect-nube_15661286

©TecNM 2025