



GOBIERNO DE
MÉXICO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



Programa de estudios del módulo

Manejo de tecnologías de ciberseguridad

Currículum Laboral

Área(s):

Tecnología y transporte

Carrera(s):

Profesional Técnico-Bachiller en
Informática, Soporte y mantenimiento de equipo de cómputo
y Telecomunicaciones

5º semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Manejo de tecnologías de ciberseguridad

Área(s): Tecnología y transporte

Carrera(s): PT-B en Informática, Soporte y mantenimiento de equipo de cómputo y Telecomunicaciones

Semestre(s): Quinto

Horas por semana: 5

Fecha de diseño o actualización: 28 de abril de 2025

Vigencia: a partir de la aprobación de la Junta Directiva y en tanto no se genere un documento que lo actualice.

© Colegio Nacional de Educación Profesional Técnica

Prohibida la reproducción total o parcial de esta obra por cualquier medio, sin autorización por escrito del CONALEP.

Directorio

Rodrigo Alejandro Rojas Navarrete
Dirección General

Ana María Rosas Muciño
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Manejo de tecnologías de ciberseguridad

Contenido		Pág.
Capítulo I:	Generalidades del Profesional Técnico-Bachiller	
1.1	Marco Curricular Común de la Educación Media Superior	5
1.2	Objetivo(s) de la(s) carrera(s)	6
Capítulo II:	Aspectos específicos del módulo	
2.1	Presentación	7
2.2	Propósito del módulo	8
2.3	Mapa del módulo	9
2.4	Unidades de aprendizaje	10
2.5	Referencias	18

CAPÍTULO I: Generalidades del Profesional Técnico-Bachiller

1.1 Marco Curricular Común de la Educación Media Superior

El Marco Curricular Común de la Educación Media Superior propone una apuesta curricular centrada en el desarrollo integral de las y los adolescentes y jóvenes, con la finalidad de formar estudiantes capaces de conducir su vida hacia su futuro con bienestar y satisfacción; con sentido de pertenencia social, conscientes de los problemas sociales, económicos y políticos que aquejan al país, dispuestos a participar de manera responsable y con toma de decisión hacia los procesos de la democracia participativa y compromiso por generar soluciones de las problemáticas que los aquejan y que tengan la capacidad de aprender a aprender en el trayecto de su vida. Que sean adolescentes y jóvenes capaces de erigirse como agentes de transformación social y que fomenten una cultura de paz y de respeto hacia la diversidad social, sexual, política y étnica; solidarios y empáticos.

A través del currículum laboral, el Profesional Técnico-Bachiller desarrollará competencias laborales extendidas pertinentes, buscando la transversalidad con los módulos del currículum fundamental y ampliado; permitiendo con ello desarrollar conocimientos, destrezas, habilidades, actitudes y valores que le permitan comprender los procesos productivos en los que está involucrado para enriquecerlos, transformarlos, resolver problemas, ejercer la toma de decisiones y desempeñarse en diferentes ambientes laborales, con una actitud creadora, crítica, responsable y propositiva; de la misma manera, fomenta el trabajo en equipo, colaborativo, el desarrollo pleno de su potencial en los ámbitos profesional, personal, así como la convivencia de manera armónica con el medio ambiente y la sociedad.

1.2 Objetivo(s) de la(s) carrera(s)

PT-B en Informática

Desempeñar funciones técnico-operativas inherentes al desarrollo e implantación de soluciones de tecnologías de información basados en la automatización, organización, codificación, recuperación de la información y optimización de recursos informáticos a fin de impulsar la competitividad, las buenas prácticas y toma de decisiones en organizaciones o empresas de cualquier ámbito.

PT-B en Telecomunicaciones

Realizar servicios de instalación, operación, diagnóstico, mantenimiento y mejora de equipo, sistemas y redes de telecomunicación implementados con diversas tecnologías.

PT-B en Soporte y mantenimiento de equipos de cómputo

Realizar los servicios de instalación, configuración, operación, mantenimiento y actualización de equipo, dispositivos periféricos, sistemas y redes de computadoras, incorporando tecnologías de vanguardia.

CAPÍTULO II: Aspectos específicos del módulo

2.1 Presentación

El módulo de **Manejo de tecnologías de ciberseguridad** pertenece al Trayecto Técnico denominado Ciberseguridad y se imparte en el quinto semestre de la carrera de Profesional Técnico-Bachiller en Informática, Soporte y mantenimiento de equipo de cómputo y Telecomunicaciones. Tiene como finalidad que la o el alumno adquiera las habilidades y destrezas necesarias para utilizar tecnologías de ciberseguridad empleando conceptos, fundamentos y procedimientos de configuración presentes en distintos procesos de comunicación, protección y control informático con la finalidad de establecer las bases programáticas de la protección de red.

Está conformado por tres unidades de aprendizaje. La primera, pretende que los estudiantes realicen la identificación de conceptos básicos de redes para la comunicación en red empleando procedimientos de direccionamiento y enrutamiento.; la segunda, busca que los estudiantes apliquen fundamentos de ciberseguridad a través configuraciones y tecnologías para la protección y confidencialidad de información ; por último, la tercera unidad pretende que los estudiantes realicen la programación y utilizará lenguajes informáticos a través del uso de operadores para establecer estructuras de flujo de control.

La contribución del módulo es desarrollar competencias profesionales esenciales para su perfil de egreso y para su inserción laboral, incluyendo conocimientos, destrezas, habilidades, actitudes y valores que se integran y relacionan con otros módulos del plan de estudios, como el manejo de tecnología para la ciberseguridad, así como configuraciones, lenguajes de programación, conceptos de red, dispositivos móviles, seguridad de TI y solución de problemas. Las habilidades específicas desarrolladas en cada capítulo se describen al comienzo de cada uno de ellos. Cabe mencionar, que el módulo está organizado por tres unidades, articuladas y diseñadas con base en procesos vigentes de certificación en ciberseguridad y tecnologías de red.

La tarea educativa tendrá que diversificarse, a fin de que el personal docente realice funciones preceptoras, que consistirán en la guía y acompañamiento del alumnado durante su proceso de formación académica y personal y en la definición de estrategias de participación que le permitan incorporar a su familia en un esquema de corresponsabilidad que coadyuve a su desarrollo integral; por tal motivo, deberá destinar tiempo dentro de cada unidad para brindar este apoyo a la labor educativa de acuerdo con el Programa de Preceptorías.

Por otro lado, el alumnado deberá gestionar su aprendizaje, a fin de distribuir su tiempo para dedicar un porcentaje de la duración del módulo al estudio independiente, para reforzar el conocimiento previo o adquirido en clase, de tal forma que obtengan hábitos de estudio que le permitan ser autodidacta.

Finalmente, es necesario que al concluir cada resultado de aprendizaje se considere una sesión de clase en la cual se realice la recapitulación de los aprendizajes logrados, con el propósito de verificar que éstos se han alcanzado o, en caso contrario, determinar las acciones de mejora pertinentes. Cabe señalar que en esta sesión el alumno o la alumna que haya obtenido insuficiencia en sus actividades de evaluación o desee mejorar su resultado, tendrá la oportunidad de entregar nuevas evidencias.

2.2 Propósito del módulo

Utilizar tecnologías de ciberseguridad empleando conceptos, fundamentos y procedimientos de configuración presentes en distintos procesos de comunicación, protección, confidencialidad de la información y control informático con la finalidad de establecer las bases programáticas de la protección de red.

2.3 Mapa del módulo

Nombre del módulo	Unidad de aprendizaje	Resultado de aprendizaje
<p>Manejo de tecnologías de ciberseguridad</p> <p>90 horas</p>	<p>1. Descripción de conceptos básicos de redes para la comunicación en red empleando procedimientos de direccionamiento y enrutamiento.</p> <p>30 horas</p>	<p>1.1 Describe la configuración de comunicación en red empleando los conceptos, componentes y conexiones requeridas para su óptimo funcionamiento.</p> <p>15 horas</p>
		<p>1.2 Describe el direccionamiento y enrutamiento de redes de acuerdo con los protocolos y configuración para compartir los paquetes de información en red.</p> <p>15 horas</p>
	<p>2. Aplicación de fundamentos de ciberseguridad empleando configuraciones y tecnologías para la confidencialidad.</p> <p>30 horas</p>	<p>2.1 Identifica fundamentos de la ciberseguridad de acuerdo con los principios y tecnologías de confidencialidad con la finalidad de contextualizar su aplicación en la red.</p> <p>15 horas</p>
		<p>2.2 Utiliza principios y tecnologías de confidencialidad empleando los protocolos tecnológicos aplicados en la seguridad cibernética.</p> <p>15 horas</p>
	<p>3. Programación y uso de lenguajes informáticos a través del uso de operadores para estructuras de flujo de control.</p> <p>30 horas</p>	<p>3.1 Utiliza fundamentos y lenguajes de programación informática de acuerdo con las operaciones requeridas a fin de optimizar funciones y acciones predefinidas.</p> <p>15 horas</p>
		<p>3.2 Utiliza estructuras de flujo de control empleando el lenguaje e instrucciones de programación requeridas a fin de agrupar instrucciones de manera controlada.</p> <p>15 horas</p>

2.4 Unidades de aprendizaje

Unidad de aprendizaje:	1. Descripción de conceptos básicos de redes para la comunicación en red empleando procedimientos de direccionamiento y enrutamiento.	30 horas
Propósito de la unidad	Realizar la identificación de conceptos básicos de redes para la comunicación en red empleando procedimientos de direccionamiento y enrutamiento.	
Resultado de aprendizaje:	1.1 Describe la configuración de comunicación en red empleando los conceptos, componentes y conexiones requeridas para su óptimo funcionamiento.	15 horas

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
<p>1.1.1 Realiza un diagrama describiendo la configuración de la comunicación en red, considerando:</p> <ul style="list-style-type: none"> • Componentes y conexiones • Redes • Protocolos de comunicación 	<ul style="list-style-type: none"> • Diagrama 	15 %	<p>A. Comunicación en red</p> <ul style="list-style-type: none"> • Tipos de red • Transmisión de datos • Ancho de banda y rendimiento <p>B. Componentes y conexiones de red</p> <ul style="list-style-type: none"> • Clientes • Servidores • Conectividad <p>C. Redes inalámbricas y móviles</p> <ul style="list-style-type: none"> • Redes • Conectividad <p>D. Redes domésticas</p> <ul style="list-style-type: none"> • Conceptos • Tecnologías • Estándares • Configuración <p>E. Protocolos de comunicación</p> <ul style="list-style-type: none"> • Estándares • Modelos • Principios

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			F. Medios de red <ul style="list-style-type: none"> • Concepto • Tipos
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

Resultado de aprendizaje:	1.2 Describe el direccionamiento y enrutamiento de redes de acuerdo con los protocolos y configuración para compartir los paquetes de información en red.		15 horas
Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
1.2.1 Realiza un reporte sobre el direccionamiento y enrutamiento de redes, considerando sus protocolos y configuración.	<ul style="list-style-type: none"> • Reporte 	15 %	<ul style="list-style-type: none"> A. Capa de acceso <ul style="list-style-type: none"> • Concepto • Comunicación B. Protocolo de internet <ul style="list-style-type: none"> • Propósito • Estructura de la Dirección IPv4 C. Direccionamiento IPv4 <ul style="list-style-type: none"> • Unidifusión, difusión y multidifusión • Tipos de direcciones • Segmentación D. Direccionamiento IPv6 <ul style="list-style-type: none"> • Problemas con IPv4 • Direccionamiento IPv6 • Direccionamiento dinámico con DHCP E. Puerta de enlace a otras redes <ul style="list-style-type: none"> • Resolución de dirección • Enrutamiento entre redes • Capa de transporte • Capa de aplicación
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

Unidad de aprendizaje:	2. Aplicación de fundamentos de ciberseguridad empleando configuraciones y tecnologías para la confidencialidad.	30 horas	
Propósito de la unidad	Aplicar fundamentos de ciberseguridad a través configuraciones y tecnologías para la confidencialidad de información.		
Resultado de aprendizaje:	2.1 Identifica fundamentos de la ciberseguridad de acuerdo con los principios y tecnologías de confidencialidad con la finalidad de contextualizar su aplicación en la red.	15 horas	
Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
<p>2.1.1 Describe a través de una presentación electrónica los fundamentos de la ciberseguridad considerando:</p> <ul style="list-style-type: none"> • Principios de seguridad • Amenazas y ataques • Protección y seguridad 	<ul style="list-style-type: none"> • Presentación electrónica 	20 %	<p>A. Ciberseguridad</p> <ul style="list-style-type: none"> • Concepto • Delincuencia cibernética • Amenazas internas y externas • Vulnerabilidades • Especialistas en ciberseguridad • Certificaciones <p>B. Principios de seguridad</p> <ul style="list-style-type: none"> • Confidencialidad • Control de acceso • Integridad • Disponibilidad • Estado de los datos • Contramedidas • Modelos • Marco de trabajo <p>C. Amenazas, vulnerabilidades y ataques</p> <ul style="list-style-type: none"> • Malware • Código malicioso • Trucos • Ciberataques

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			<p>D. Protección y seguridad</p> <ul style="list-style-type: none"> • Criptografía • Encriptación • Controles de acceso • Autenticación • Autorización • Control de seguridad • Ocultamiento de datos
<p>Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.</p>			

Resultado de aprendizaje:	2.2 Utiliza principios y tecnologías de confidencialidad empleando los protocolos tecnológicos aplicados en la seguridad cibernética.	15 horas	
Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
<p>2.2.1 Elabora un reporte demostrando el uso de principios y tecnologías de confidencialidad aplicados en la ciberseguridad, evidenciando:</p> <ul style="list-style-type: none"> • Estándar • Defensa de sistemas • Dominio de ciberseguridad 	<ul style="list-style-type: none"> • Reporte 	<p>15 %</p>	<p>A. Controles de integridad de datos</p> <ul style="list-style-type: none"> • Algoritmos • Técnica salting • HMAC • Firmas digitales • Certificados • Integridad en base de datos <p>B. Estándar de ciberseguridad</p> <ul style="list-style-type: none"> • Alta disponibilidad • Disponibilidad • Defensa en profundidad • Respuesta a incidentes • Recuperación tras un desastre <p>C. Defensa de sistemas y dispositivos</p> <ul style="list-style-type: none"> • Protección del host • Protección del servidor • Protección de la red • Seguridad física <p>D. Dominio Ciberseguridad</p> <ul style="list-style-type: none"> • Dominio de vulnerabilidades • Ética y principios rectores • Herramientas
<p>Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.</p>			

Unidad de aprendizaje:	3. Programación y uso de lenguajes informáticos a través del uso de operadores para estructuras de flujo de control.	30 horas
Propósito de la unidad	Realizar la programación y utilizar lenguajes informáticos a través del uso de operadores para establecer estructuras de flujo de control.	
Resultado de aprendizaje:	3.1 Utiliza fundamentos y lenguajes de programación informática de acuerdo con las operaciones requeridas a fin de optimizar funciones y acciones predefinidas.	15 horas

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
3.1.1 Elabora un reporte demostrando el uso de fundamentos y lenguajes de programación empleando las operaciones predefinidas.	<ul style="list-style-type: none"> Reporte 	20 %	<p>A. Programación informática</p> <ul style="list-style-type: none"> • Conceptos universales • Instrucciones • Archivo fuente • Elementos del lenguaje • Programación moderna <p>B. Codificación</p> <ul style="list-style-type: none"> • Sintaxis • Semántica • Variables • Literales • Operadores • Herramientas

Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.

Resultado de aprendizaje:	3.2 Utiliza estructuras de flujo de control empleando el lenguaje e instrucciones de programación requeridas a fin de agrupar instrucciones de manera controlada.	15 horas	
Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
<p>3.2.1 Demuestra el uso de estructuras de flujo de control evidenciando el procesamiento y las funciones de programación requeridas.</p>	<ul style="list-style-type: none"> • Reporte 	<p>15 %</p>	<p>A. Procesamiento</p> <ul style="list-style-type: none"> • Sentencias condicionales • Toma de decisiones • Bucles • Iteraciones • Operadores lógicos • Operaciones bit a bit • Listas • Ordenamiento de listas • Algoritmo • Operaciones con listas • Aplicaciones avanzadas <p>B. Funciones de programación</p> <ul style="list-style-type: none"> • Comunicación de funciones • Resultados • Expresión de retorno • Valores • Mecanismos • Múltiples parámetros • Excepciones • Errores en el código
<p>Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.</p>			

2.5 Referencias

Básicas:

- Ariganello, E. (2018). *Técnicas de configuración de routers Cisco*. Editorial Alfa Omega Ra-Ma.
- Cardador, A. (2018). *Ciberseguridad para usuarios*. Ic Editorial
- López, Y. (2022). *Ciberseguridad en el teletrabajo*. Ic Editorial
- Fusario, R. y Castro, A. (2015). *Comunicaciones y redes para profesionales en sistemas de información*. Alfaomega Grupo Editor.

Complementarias:

- Ariganello, E. (2016). *Redes Cisco. Guía de estudio para la certificación CCNA routing y switching*. Editorial Ra-Ma.
- Fusario, R. y Castro, A. (2013). *Comunicaciones. una introducción a las redes digitales de transmisión de datos y señales isócronas*. Alfaomega Grupo Editor.
- Pedrosa, A. (2013). *Cisco Ccnav7. Curso Práctico*. Altaria Publicaciones.
- Pérez, D. (2018). *Redes Cisco. Fundamentos de networking para el examen de certificación CCNA*. Alfaomega Grupo Editor.
- ¿Qué es la ciberseguridad?. Consultado el 08 de abril de 2025 de: <https://club-ciso.aec.es/conceptos-clave-de-ciberseguridad/>
- Ciberseguridad ciudadana. Consultado el 08 de abril de 2025 de: <https://www.gob.mx/gncertmx/articulos/ciberseguridad-ciudadana-263949>
- Ciberseguridad, ¿cómo protegerte en internet? Consultado el 08 de abril de 2025 de: <https://www.unicef.org/mexico/ciberseguridad>