Programa de estudios del módulo

Aplicación de la seguridad cibernética

Currículum Laboral

Área:
Tecnología y transporte

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

6° semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad cibernética

Área: Tecnología y transporte

Carrera: PT-B Informática/ Soporte y mantenimiento de equipo de cómputo/ Telecomunicaciones

Semestre: 6°

Horas por semana: 5

Fecha de diseño o actualización: 14 de noviembre de 2025.

Vigencia: a partir de la aprobación de la junta directiva y en tanto no se genere un documento que lo anule o actualice.

Directorio

Rodrigo Alejandro Rojas Navarrete
Dirección General

Ana María Rosas Muciño
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Aplicación de la seguridad cibernética

Contenido **Pág.**

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 Objetivos de las Carreras

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 Soporte y mantenimiento de equipo 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.

PT-B en Telecomunicaciones

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

CAPÍTULO II: Aspectos Específicos del Módulo

2.1 Presentación

El módulo de **Aplicación de la seguridad cibernética** pertenece al Trayecto Técnico denominado Ciberseguridad que se imparte en el sexto semestre de las carreras de Profesional Técnico-Bachiller en Informática, Soporte y mantenimiento de equipo de cómputo y Telecomunicaciones. Tiene como finalidad que la o el alumno aplique la seguridad informática en software, hardware, redes, información e infraestructura de usuarios y organizaciones empleando principios, prácticas y procesos de ciberseguridad con la finalidad de mantener la integridad, confidencialidad y disponibilidad en su red y sus datos.

Se encuentra conformado por tres unidades de aprendizaje; la primera unidad, pretende que los estudiantes realicen la evaluación de red, sistemas y puntos finales para la detección de amenazas y vulnerabilidades en red empleando procedimientos de protección; la segunda unidad busca que los estudiantes apliquen prácticas de monitoreo y protección de red empleando configuraciones y alertas por la seguridad y defensa y la tercera unidad pretende que los estudiantes realicen la administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad.

Las competencias desarrolladas en este módulo, contribuyen al perfil de egreso de las carreras se centra en el desarrollo de habilidades técnicas relacionadas con el la evaluación de red, la administración de amenazas y el monitoreo y protección de red empleando configuraciones y alertas para la seguridad y serán empleadas o relacionadas con los módulos de manejo de redes, programación con sistemas gestores de datos, aplicación de la seguridad informática, mantenimiento de redes de telecomunicaciones, administración de sistemas de interconexión de redes departamentales, construcción de redes de telecomunicación, instalación de redes de datos y actualización de equipos de cómputo.

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

Aplicar la seguridad informática en software, hardware, redes, información e infraestructura de usuarios y organizaciones empleando principios, prácticas y procesos de ciberseguridad con la finalidad de mantener la integridad, confidencialidad y disponibilidad en su red y sus datos.

2.3 Mapa del Módulo

Nombre del Módulo	Unidad de Aprendizaje	Resultado de aprendizaje
Aplicación de la seguridad cibernética **90 horas**	**1.** Evaluación de red, sistemas y puntos finales para la detección de vulnerabilidades en red empleando procedimientos de protección. **20 horas**	**1.1** Configura una red simulada de una organización empleando conceptos de ciberseguridad, medidas de mitigación y seguridad ante amenazas de red comunes y emergentes. **10 horas**
		1.2 Evalúa la seguridad del punto final y documenta una estrategia de seguridad en la red configurando medidas de seguridad en dispositivos de red y terminales para su protección. **10 horas**
	2. Monitoreo y protección de red empleando configuraciones y alertas para la seguridad. **30 horas**	**2.1** Configura prácticas y procesos de defensa de la red de acuerdo con los principios y tecnologías de confidencialidad aplicados en la seguridad cibernética **15 horas**
		2.2 Configura medidas y alertas de seguridad en la nube empleando los mecanismos tecnológicos, de monitoreo y criptografía aplicados en la seguridad cibernética. **15 horas**

	3. Administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad. **40 horas**	**3.1** Evalúa vulnerabilidades y realiza la gestión de riesgos de red a través de herramientas y pruebas de seguridad a fin de establecer controles de seguridad. **20 horas**
		3.2 Utiliza modelos de respuesta ante incidentes de acuerdo con su tipo y características a fin de aplicar la ciberseguridad en la red. **20 horas**

2.4 Unidades de Aprendizaje

Unidad de aprendizaje:	**1.** Evaluación de red, sistemas y puntos finales para la detección de vulnerabilidades en red empleando procedimientos de protección.	**20 horas**
Propósito de la unidad	Realizar la evaluación de red, sistemas y puntos finales para la detección de amenazas y vulnerabilidades en red empleando procedimientos de protección.	
Resultado de aprendizaje:	**1.1** Configura una red simulada de una organización empleando conceptos de ciberseguridad, medidas de mitigación y seguridad ante amenazas de red comunes y emergentes.	**10 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
1.1.1. Realiza un diagrama describiendo la configuración de una red considerando la ciberseguridad, medidas de mitigación y seguridad ante amenazas de red comunes y emergentes	• **Diagrama**	**15%**	**A.** Ataques a la ciberseguridad • Amenazas comunes • Ataques cibernéticos • Ataques a dispositivos • Ataques a las aplicaciones **B.** Protección de redes • Estado actual • Ataque de red • Seguridad en red **C.** Ataque a los fundamentos • Detalles de la PDU de IP • Vulnerabilidades IP, TCP y UDP • Mitigación de ataques **D.** Comunicación de red inalámbrica • Amenazas • Wlan seguras • Dispositivos de comunicación

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			E. Infraestructura de seguridad de redes • Dispositivos de seguridad • Servicios de seguridad • Infraestructura de seguridad

Resultado de aprendizaje:	**1.2** Evalúa la seguridad del punto final y documenta una estrategia de seguridad en la red configurando medidas de seguridad en dispositivos de red y terminales para su protección.	**10 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
1.2.1. Realiza un reporte escrito evaluando la seguridad del punto final considerando la estrategia de seguridad de red.	• **Reporte escrito.**	**15%**	**A.** Sistema operativo • Arquitectura y operaciones • Configuración y monitoreo • Seguridad **B.** Sistema operativo de código abierto • Características • Estructura • Servidores • Administración • Sistema de archivos • Instalación • Configuración y manejo **C.** Protección de terminales • Defensa de sistemas y dispositivos • Protección antimalware • Prevención de intrusiones • Seguridad en aplicaciones **D.** Prácticas y procesos de ciberseguridad • Tres dimensiones • Estados de los datos • Contramedidas • Principios • Seguridad en terminales
Sesión para recapitulación y entrega de evidencias.			

Unidad de aprendizaje:	**2.** Monitoreo y protección de red empleando configuraciones y alertas para la seguridad.	**30 horas**
Propósito de la unidad	Realizar prácticas de monitoreo y protección de red empleando configuraciones y alertas para la seguridad y defensa.	
Resultado de aprendizaje:	**2.1.** Configura prácticas y procesos de defensa de la red de acuerdo con los principios y tecnologías de confidencialidad aplicados en la seguridad cibernética.	**15 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
2.1.1. Describe a través de una presentación electrónica la configuración de prácticas y procesos de defensa de la red considerando los principios y tecnologías requeridos.	• **Presentación electrónica**	**20%**	**A.** Defensa de la red • Defensa en profundidad • Gestión de operaciones • Regulación y políticas • Estándares **B.** Defensa del sistema • Seguridad física • Seguridad en aplicaciones • Servicios y protocolos • Segmentación • Protección de dispositivos • Resiliencia de la ciberseguridad • Sistemas embebidos **C.** Control de acceso • Concepto • Administración de cuentas • Uso • Funcionamiento

Resultado de aprendizaje:	**2.2.** Configura medidas y alertas de seguridad en la nube empleando los mecanismos tecnológicos, de monitoreo y criptografía aplicados en la seguridad cibernética.	**15 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
2.2.1. Demuestra la configuración de medidas y alertas de seguridad en la nube considerando los mecanismos establecidos.	• **Reporte escrito**	**15%**	**A.** Manejo de listas de control • Enmascaramiento • Configuración • Sintaxis • Implementación • Mitigación **B.** Tecnologías de firewall • Redes seguras • Diseño de redes • Firewalls en diseño de redes • Firewalls de política basados en zona **C.** Seguridad en la nube • Virtualización • Dominios • Infraestructura • Aplicaciones • Datos • Máquinas virtuales **D. Criptografía** • Confidencialidad • Ocultamiento de datos • Integridad y autenticidad • Hashes • Clavé pública

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			• Autoridades y sistema de confianza • Aplicaciones **E.** Tecnologías y protocolos • Monitoreo • Tecnologías de seguridad • Datos de seguridad en la red – Tipos de datos – Registros • Evaluar alertas – Fuentes de alertas • Descripción general
Sesión para recapitulación y entrega de evidencias.			

Unidad de aprendizaje:	**3.** Administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad.	**40 horas**
Propósito de la unidad	Realizar la administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad.	
Resultado de aprendizaje:	**3.1.** Evalúa vulnerabilidades y realiza la gestión de riesgos de red a través de herramientas y pruebas de seguridad a fin de establecer controles de seguridad.	**20 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
3.1.1. Realiza un reporte escrito sobre la evaluación de vulnerabilidades y la gestión de riesgos conforme a las pruebas establecidas.	• **Reporte escrito**	**20%**	**A.** Gestión y cumplimiento • Políticas • Procedimientos • Principios rectores • Manejo de amenazas • Ética de la ciberseguridad • Marco de trabajo **B.** Pruebas de seguridad en la red • Evaluaciones • Técnicas de prueba • Herramientas de prueba • Pruebas de seguridad **C.** Inteligencia contra amenazas • Fuentes de información • Servicios de inteligencia **D.** Evaluación de vulnerabilidades de terminales • Perfiles de redes • Sistema común

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			• Administración dispositivos • Administración de riesgos • Controles de seguridad

Resultado de aprendizaje:	**3.2.** Utiliza modelos de respuesta ante incidentes de acuerdo con su tipo y características a fin de aplicar la ciberseguridad en la red.	**20 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
3.2.1. Demuestra la aplicación del análisis digital y la respuesta a incidentes considerando los procedimientos establecidos.	• **Reporte escrito de la actividad.**	**15%**	**A.** Análisis digital • Manejo de evidencia • Atribución del ataque • Cadenas de seguimiento • Modelo de análisis **B.** Respuesta a incidentes • Tipos de incidentes • Procedimiento • Partes interesadas • Ciclo de vida • Detección y análisis • Respuesta a incidentes • Recuperación ante desastres
Sesión para recapitulación y entrega de evidencias.			

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

Complementarias:

- Ariganello, E. (2016). Redes Cisco. *Guía de estudio para la certificación CCNA routing y switching* / 4 Ed., 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.
- Pérez, D. (2018) Redes Cisco. *Fundamentos de networking para el examen De certificación CCNA*. Alfaomega Grupo Editor
- Fusario, R. y Castro, A. (2015). *Comunicaciones y redes para profesionales en sistemas de información*. Alfaomega Grupo Editor.
- CISCO, (2023) *Introduction to Cybersecurity.* https://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity
- CISCO, (2023) *Cursos de TI: Ciberseguridad.* https://www.netacad.com/courses/