Programa de estudios del módulo

Aplicación de la seguridad cibernética

Núcleo de Formación Profesional

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 semestre: 90

Créditos por semestre: 9

Fecha de diseño o actualización: 20 de octubre de 2023.

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

Directorio

Manuel de Jesús Espino
Dirección General

Lauro Cordero Frayre
Secretaría General

Hugo Nicolás Pérez González
Secretaría Académica

Edith Chávez Ramos
Dirección de Diseño Curricular

Aplicación de la seguridad cibernética

Contenido **Pág.**

CAPÍTULO I: Generalidades del Profesional Técnico-Bachiller

1.1 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.

1.2 Marco Curricular Común de la Educación Media Superior

Competencias Genéricas	Atributos
Se autodetermina y cuida de sí **1.** Se conoce y valora a sí mismo y aborda problemas y retos teniendo en cuenta los objetivos que persigue.	**1.1** Enfrenta las dificultades que se le presentan y es consciente de sus valores, fortalezas y debilidades. **1.2** Identifica sus emociones, las maneja de manera constructiva y reconoce la necesidad de solicitar apoyo ante una situación que lo rebase. **1.3** Elige alternativas y cursos de acción con base en criterios sustentados y en el marco de un proyecto de vida. **1.4** Analiza críticamente los factores que influyen en su toma de decisiones. **1.5** 1Asume las consecuencias de sus comportamientos y decisiones. **1.6** Administra los recursos disponibles teniendo en cuenta las restricciones para el logro de sus metas.
2. Es sensible al arte y participa en la apreciación e interpretación de sus expresiones en distintos géneros.	**2.1** Valora el arte como manifestación de la belleza y expresión de ideas, sensaciones y emociones. **2.2**. Experimenta el arte como un hecho histórico compartido que permite la comunicación entre individuos y culturas en el tiempo y el espacio, a la vez que desarrolla un sentido de identidad. **2.3** Participa en prácticas relacionadas con el arte
3. Elige y practica estilos de vida saludables.	**3.1** Reconoce la actividad física como un medio para su desarrollo físico, mental y social. **3.2** Toma decisiones a partir de la valoración de las consecuencias de distintos hábitos de consumo y conductas de riesgo. **3.3** Cultiva relaciones interpersonales que contribuyen a su desarrollo humano y el de quienes lo rodean.
Se expresa y comunica **4.** Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados.	**4.1** Expresa ideas y conceptos mediante representaciones lingüísticas, matemáticas o gráficas. **4.2** Aplica distintas estrategias comunicativas según quienes sean sus interlocutores, el contexto en el que se encuentra y los objetivos que persigue. **4.3** Identifica las ideas clave en un texto o discurso oral e infiere conclusiones a partir de ellas. **4.4** Se comunica en una segunda lengua en situaciones cotidianas. **4.5** Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas.
Piensa crítica y reflexivamente **5.** Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos.	**5.1** Sigue instrucciones y procedimientos de manera reflexiva, comprendiendo como cada uno de sus pasos contribuye al alcance de un objetivo. **5.2** Ordena información de acuerdo con categorías, jerarquías y relaciones. **5.3** Identifica los sistemas y reglas o principios medulares que subyacen a una serie de fenómenos. **5.4** Construye hipótesis y diseña y aplica modelos para probar su validez. **5.5** Sintetiza evidencias obtenidas mediante la experimentación para producir conclusiones y formular nuevas preguntas. **5.6** Utiliza las tecnologías de la información y comunicación para procesar e interpretar información.
6. Sustenta una postura personal sobre temas de interés y relevancia general, considerando	**6.1** Elige las fuentes de información más relevantes para un propósito específico y discrimina entre ellas de acuerdo a su relevancia y confiabilidad. **6.2** Evalúa argumentos y opiniones e identifica prejuicios y falacias.

Competencias Genéricas	Atributos
otros puntos de vista de manera crítica y reflexiva.	**6.3** Reconoce los propios prejuicios, modifica sus puntos de vista al conocer nuevas evidencias, e integra nuevos conocimientos y perspectivas al acervo con el que cuenta. **6.4** Estructura ideas y argumentos de manera clara, coherente y sintética.
Aprende de forma autónoma **7.** Aprende por iniciativa e interés propio a lo largo de la vida.	**7.1** Define metas y da seguimiento a sus procesos de construcción de conocimiento. **7.2** Identifica las actividades que le resultan de menor y mayor interés y dificultad, reconociendo y controlando sus reacciones frente a retos y obstáculos. **7.3** Articula saberes de diversos campos y establece relaciones entre ellos y su vida cotidiana.
Trabaja en forma colaborativa **8.** Participa y colabora de manera efectiva en equipos diversos.	**8.1** Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos. **8.2** Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva. **8.3** Asume una actitud constructiva, congruente con los conocimientos y habilidades con los que cuenta dentro de distintos equipos de trabajo.
Participa con responsabilidad en la sociedad **9.** Participa con una conciencia cívica y ética en la vida de su comunidad, región, México y el mundo.	**9.1** Privilegia el diálogo como mecanismo para la solución de conflictos. **9.2** Toma decisiones a fin de contribuir a la equidad, bienestar y desarrollo democrático de la sociedad. **9.3** Conoce sus derechos y obligaciones como mexicano y miembro de distintas comunidades e instituciones, y reconoce el valor de la participación como herramienta para ejercerlos. **9.4** Contribuye a alcanzar un equilibrio entre el interés y bienestar individual y el interés general de la sociedad. **9.5** Actúa de manera propositiva frente a fenómenos de la sociedad y se mantiene informado. **9.6** Advierte que los fenómenos que se desarrollan en los ámbitos local, nacional e internacional ocurren dentro de un contexto global interdependiente.
10. Mantiene una actitud respetuosa hacia la interculturalidad y la diversidad de creencias, valores, ideas y prácticas sociales.	**10.1** Reconoce que la diversidad tiene lugar en un espacio democrático de igualdad de dignidad y derechos de todas las personas, y rechaza toda forma de discriminación. **10.2** Dialoga y aprende de personas con distintos puntos de vista y tradiciones culturales mediante la ubicación de sus propias circunstancias en un contexto más amplio. **10.3** Asume que el respeto de las diferencias es el principio de integración y convivencia en los contextos local, nacional e internacional.
11. Contribuye al desarrollo sustentable de manera crítica, con acciones responsables.	**11.1** Asume una actitud que favorece la solución de problemas ambientales en los ámbitos local, nacional e internacional. **11.2** Reconoce y comprende las implicaciones biológicas, económicas, políticas y sociales del daño ambiental en un contexto global interdependiente. **11.3** Contribuye al alcance de un equilibrio entre los intereses de corto y largo plazo con relación al ambiente.

*Fuente: Acuerdo 444 por el que se establecen las competencias que constituyen el Marco Curricular Común del Sistema Nacional de Bachillerato.

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 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 al 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 en este módulo tendrá que diversificarse, a fin de que los docentes realicen 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 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. Así mismo, se deberán evaluar de manera continua los tres tipos de aprendizaje: conceptual, procedimental y actitudinal a lo largo del desarrollo de competencias.

Por último, es necesario que al final de cada unidad 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. **30 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. **15 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. **15 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. **30 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. **15 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. **15 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.	**30 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 de amenazas de red comunes y emergentes.	**15 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 de 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.	**15 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.	**30 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.	**15 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.	**15 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.* México, Alfaomega Grupo Editor.
- Pérez, D. (2018) Redes Cisco. *Fundamentos de networking para el examen De certificación CCNA*. México. Alfaomega Grupo Editor
- Fusario, R. y Castro, A. (2015). *Comunicaciones y redes para profesionales en sistemas de información*. México, Alfaomega Grupo Editor.

Páginas Web:

- CISCO, (2023) *Introduction to Cybersecurity.* Recuperado el (22/08/2023) de: https://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity
- CISCO, (2023) *Cursos de TI: Ciberseguridad.* Recuperado el (22/08/2023) de: https://www.netacad.com/courses/