Programa de estudios del módulo

Aplicación de herramientas de seguridad en hardware y software

Currículum Laboral

Área:
Tecnología y transporte

Carrera:
Profesional Técnico-Bachiller en
Soporte y mantenimiento de equipo de cómputo

6º semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de herramientas de seguridad en hardware y software.

Área: Tecnología y transporte.

Carrera: PT-B en Soporte y mantenimiento de equipo de cómputo.

Semestre: Sexto

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 actualice.

Directorio

Rodrigo Alejandro Rojas Navarrete
Dirección General

Ana María Rosas Muciño
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Aplicación de herramientas de seguridad en hardware y software

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 Objetivo de la carrera

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.

CAPÍTULO II: Aspectos específicos del módulo

2.1 Presentación

El módulo de **Aplicación de herramientas de seguridad en hardware y software,** pertenece al trayecto técnico Seguridad de redes y sistemas informáticos y se imparte en el sexto semestre de la carrera de Profesional Técnico-Bachiller en **Soporte y mantenimiento de equipo de cómputo**. Tiene como finalidad que la o el alumno adquiera las habilidades y destrezas necesarias para instalar tecnología de seguridad de hardware y software del equipo de cómputo, con base en las recomendaciones técnicas vigentes enfocadas a reducir riesgos y amenazas que atenten contra la integridad, confidencialidad y disponibilidad de la información.

Está conformado por dos unidades de aprendizaje, la primera se enfoca al diagnóstico de riesgos, amenazas y vulnerabilidades a la integridad de la información y operación del equipo y la segunda, hacia la evaluación de recomendaciones tecnológicas en materia de seguridad y hacia la instalación de herramientas de seguridad al hardware y software.

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: identificar las características técnicas de componentes, equipos, dispositivos periféricos y sistemas mediante la interpretación de documentación técnica; validar la operación de software de aplicación general.

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

Instalar tecnología de seguridad de hardware y software del equipo de cómputo, con base en las recomendaciones técnicas vigentes enfocadas a reducir riesgos y amenazas que atenten contra la integridad, confidencialidad y disponibilidad de la información.

2.3 Mapa del módulo

Nombre del módulo	Unidad de aprendizaje	Resultado de aprendizaje
Aplicación de herramientas de seguridad en hardware y software **90 horas**	**1.** Diagnóstico de riesgos y amenazas en la seguridad del equipo **35 horas**	**1.1** Identifica riesgos y amenazas en la seguridad del hardware y software con base en las advertencias que emite el equipo. **15 horas**
		1.2 Evalúa la integridad de la información y operación del equipo de cómputo conforme a las recomendaciones técnicas de seguridad contra riesgos y amenazas. **20 horas**
	2. Implementación de tecnología de seguridad en hardware y software del equipo de cómputo. **55 horas**	**2.1** Establece recomendaciones de tecnología de seguridad en hardware y software orientada a la protección y preservación de la integridad de la información. **25 horas**
		2.2 Implementa tecnología de seguridad protegiendo la integridad de la información y el equipo de cómputo contra amenazas. **30 horas**

2.4 Unidades de aprendizaje

Unidad de aprendizaje:	**1. Diagnóstico de riesgos y amenazas en la seguridad del equipo.**	**35 horas**
Propósito de la unidad	Evaluar la integridad de la información, los riesgos y amenazas en la operación del equipo de cómputo emitiendo un diagnóstico sobre la seguridad en el mismo.	
Resultado de aprendizaje:	**1.1** Identifica riesgos y amenazas en la seguridad del hardware y software con base en las advertencias que emite el equipo.	**15 horas**

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
1.1.1 Elabora un reporte de resultados identificando riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo.	• **Reporte de resultados de la simulación de riesgos y amenazas.**	**20 %**	**A.** Identificación de riesgos y amenazas en el hardware y software • Descripción de las vulnerabilidades. • Detección de amenazas en el hardware - Equipo de cómputo - Routers - Módem de cable - Servidores de video - Impresoras • Detección de amenazas en el software - Sistemas operativos - Servidores - Bases de datos - Navegadores - Aplicaciones de oficina - Aplicación de normas y estándares de calidad para el desarrollo de software. **B.** Detección de vulnerabilidades de seguridad en dispositivos ADSL y su entorno. • Comandos de monitoreo de tráfico en la red • .Herramienta de evaluación de seguridad de Microsoft (MSAT) • Herramienta de bloqueo IIS

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			• Reportero de puertos (Port reporter). • Muestreo de seguridad de la red (network security scan). • Monitoreo de las actualizaciones de seguridad **C**. Evaluación de riesgos en los sistemas de información • Reconocimiento de sistemas. • Detección de vulnerabilidades. • Robo de información mediante intercepción de mensajes. • Modificación de la secuencia de mensajes. • Análisis de tráfico en la red • Ataques de suplantación de identidad. • Conexión a redes abiertas • Servicios innecesarios habilitados.
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

Resultado de aprendizaje:	**1.2** Evalúa la integridad de la información y operación del equipo de cómputo conforme a las recomendaciones técnicas de seguridad contra riesgos y amenazas.	**20 horas**

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
1.2.1 Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación.	• **Diagnóstico de la integridad de la información.**	**25 %**	**A**. Identificación de amenazas (agentes externos) de intrusión • Conductos de intrusión • Virus • Malware • Navegación en servidores web • Intercepción pasiva (eavesdropping). • Espionaje de información (snooping) • Modificación de la información (tampering) • Envío de correos electrónicos con nuestra identidad • Saturación de servidores web • Suplantación de identidad (spoofing). **B.** Evaluación de riesgos originados por la configuración e instalación de la red. • Protocolos de red abiertos e innecesarios • Actualización versión del IOS • Archivos e impresoras compartidos usando TCP/IP • NetBIOS habilitado sobre TCP • Red o sistema informático no aislado de otras redes o sistemas • Vulnerabilidad de contraseñas • Omisión en la instalación y/o actualización de antivirus. • Desactivación de la actualización de aplicaciones

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			• Ejecución y descarga de archivos y/o programas de dudosa procedencia. • Servicios de red habilitados e innecesarios. • Rutas estáticas configuradas en donde sea necesario • Ejecución de applets de Java y activex. • Respaldos de información no actualizados. • Uso de WEP / WPA (Wireless Equivalent privacy/WiFi Protected Acces).
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

Unidad de aprendizaje:	**2. Implementación de tecnología de seguridad en hardware y software del equipo de cómputo**	**55 horas**
Propósito de la unidad	Aplicar la tecnología de seguridad en hardware y software considerando el diagnóstico y recomendaciones en riesgos y amenazas a la información	
Resultado de aprendizaje:	**2.1** Establece recomendaciones de tecnología de seguridad en hardware y software orientada a la protección y preservación de la integridad de la información	**25 horas**

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
2.1.1 Establece recomendaciones de seguridad identificando sus efectos a través de un reporte de resultados.	• **Listado de recomendaciones de seguridad.** • **Reporte de resultados.**	**25 %**	**A.** Estructuración de recomendaciones contra vulnerabilidades • Autorización y registro de usuarios - Control de acceso a usuarios locales y remotos - Servidores de autenticación - Administración de contraseñas • Sistemas biométricos. - Reconocimiento de firmas manuscritas - Huellas dactilares - Análisis del iris • Recomendaciones de criptografía. - Certificados digitales - Implantación de algoritmos en hardware y software. - Métodos de encriptación - Algoritmos en protocolos **B**. Implementación de acciones a favor de la seguridad. • Identificación de actividades - Denegación de servicio. - Modificación al contenido de mensajes. - Suplantación de actividad. - Conexión no autorizada a equipos y servidores. • Prevención de ataques que:

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			- Realicen llamadas al sistema operativo - Traten de acceder a carpetas alojadas en un servidor web. - Detecten de URL sospechosas **C**. Elaboración de políticas para el desarrollo de aplicaciones en internet • Autenticación del usuario • Administración de sesiones del usuario. • Encriptación de datos corruptibles. • Protección con comandos y métodos de HTTP. • Prevención de ataques tipo Cross Site Scripting.
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

Resultado de aprendizaje:	**2.2** Implementa tecnología de seguridad protegiendo la integridad de la información y el equipo de cómputo contra amenazas.	**30 horas**

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
2.2.1 Instala y configura tecnología de seguridad reportando su efecto en la integridad de la información.	• **Reporte de resultados de la instalación de tecnología de seguridad.**	**30 %**	**A.** Instalación y configuración de herramientas de seguridad en redes de computadoras • Restricciones a los dispositivos ADSL (hardening). - Eliminar servicios de entrada salida innecesarios. - Restricción en listas de control de acceso. - Privilegios de acceso a módems y routers, así como al personal. - Acceso físico a los dispositivos. - No ejecución de archivos de programa de dudoso origen - Ejecución de applets de Java y activex. • Configuración de seguridad en modems y dispositivos ADSL. • Configuración de seguridad en enlaces ADSL. **B**. Instalación de herramientas de seguridad en redes VPN y Windows • Uso de protocolos - PPTP - L2F - L2TP • Redes basadas en SSL (Secure Socket Layers). • Recomendaciones de seguridad de Microsoft.

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			C. Aplicación de seguridad a componentes físicos en oficinas de la organización. • Protocolo WEP • Protocolo WPA • Estándar RSN • Estándar 802.1x • Detección de intentos de intrusión • Separación de la red inalámbrica de la red local interna **D.** Instalación, configuración e implementación de tecnología de seguridad en servicios de internet • Actualización parches de seguridad • Seguridad en función de la zona de trabajo • Administración de cookies • Discriminación en la descarga desde internet Identificación de sitios web seguros • Evaluación de enlaces y correos de dudosa procedencia • Control de contenido activo en páginas WEB • Opciones avanzadas de seguridad del explorador • Control de certificados • Medidas de seguridad contra SPAM y PHISING

Actividades de evaluación	Evidencias por recopilar	Ponderación	Contenidos
			E. Comunicación de políticas operativas de seguridad informática. • Acceso a los sistemas • Operación del equipo • Desarrollo de programas • Configuración de redes • Norma ISO 14000.
Sesión para recapitulación y entrega de evidencias, al término de cada resultado de aprendizaje.			

2.5 Referencias

Básicas:

- Gómez Vieites, A. (2007). *Enciclopedia de la seguridad informática*. Alfaomega RA-MA.
- Ariganello, E. (2008). *Técnicas de Configuración de Routers Cisco.* Alfaomega Grupo Editor.
- Roebuck, K. (2011). *Wireless Security*. Editorial Tebbo.

Complementarias:

- Comer, Douglas E. (2000). *Redes Globales de Información con Internet y TCP/ IP.* Prentice Hall.
- Cisco NetworkingAcademy; Cisco Systems, Fundamentos de seguridad de redes, Pearson Alhambra, 2005
- Ataques informáticos (DNS seguro). http://www.dnssec.net
- Ataques informáticos (KeyGhost). http://www.keyghost.com
- Escáner de vulnerabilidad, video demostrativo.7 http://www.youtube.com/watch?v=3RgOtjv4v8E
- Herramientas para el reconocimiento de sistemas y escaneo de puertos (Netscantools). http://www.nwpsw.com/
- Identificación de riesgos y tipos de hackers. http://es.kioskea.net/contents/attaques/typologie-pirates.php3
- Información técnica seguridad.: http://www.textoscientificos.com/
- Listas de seguridad, herramientas de seguridad y escaneo. http://www.insecure.org/
- Medidas de seguridad. http://www.windowsecurity.com/whitepapers/security_secure_internet_data_transmission.html
- Metodología de intrusión de red. http://es.kioskea.net/contents/attaques/methodologie.php3
- Parámetros de configuración de un dispositivo inalámbrico. http://www.usr.com/support/9108/9108-es-ug/wui_internet.htm
- Recomendaciones de seguridad por Microsunsystems. http://www.sun.com/bigadmin/content/developer/howtos/generic_host.jsp
- Security focus. http://www.securityfocus.com/
- Squid, software usado como proxy en seguridad. http://www.deckle.co.za/squid-users-guide/Terminology_and_Technologies