GOBIERNO DE MÉXICO | EDUCACIÓN | conalep

Programa de estudios del módulo

Aplicación de la seguridad informática

Currículum Laboral

Área:
Tecnología y Transporte

Carrera:
Profesional Técnico-Bachiller en Informática

3°. Semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad informática.

Área: Tecnología y Transporte.

Carrera: PT-B en Informática.

Semestre: Tercero

Horas por semana: 4

Fecha de diseño o actualización: 31 de mayo del 2024.

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

Directorio

Arturo Pontifes Martínez
Dirección General

Camilo García Ramírez
Secretaría General

Hugo Nicolás Pérez González
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Aplicación de la seguridad informática

Contenido **Pág.**

Capítulo I:	**Generalidades del Profesional Técnico-Bachiller**	
1.1	Marco Curricular Común de la Educación Media Superior	5
1.2	Objetivo de la Carrera	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	19

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 básicas y extendidas pertinentes, buscando la transversalidad con los módulos del currículum fundamental y ampliado; permitiendo con ello desarrollar habilidades, conocimientos y actitudes para 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 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.

CAPÍTULO II: Aspectos Específicos del Módulo

2.1 Presentación

El módulo de **Aplicación de la seguridad informática** corresponde al currículum laboral, es de tipo específico y se imparte en el tercer semestre de la carrera de Profesional Técnico-Bachiller en Informática. Tiene como finalidad, que el alumno ofrezca servicios de seguridad informática apegados a procedimientos, estándares en equipos de cómputo y necesidades del cliente, a través de la aplicación, administración y control de herramientas de protección, garantizando integridad, disponibilidad y confidencialidad en la información almacenada en sistemas informáticos.

El módulo se divide en dos unidades de aprendizaje. La primera unidad aborda la aplicación de estándares de protección de información y la segunda unidad desarrolla la administración de herramientas y métodos de seguridad informática.

La contribución del módulo al perfil de egreso de la carrera en la que está considerado incluye el desarrollo de habilidades que incluye que el alumno domine los conocimientos relacionados con la administración de seguridad de la información de equipos de cómputo y adquiera paralelamente habilidades y destrezas en la configuración de sistemas de seguridad de equipos de comunicación y redes.

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.

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

Ofrecer servicios de seguridad informática apegados a procedimientos, estándares en equipos de cómputo y necesidades del cliente, a través de la aplicación, administración y control de herramientas de protección, garantizando integridad, disponibilidad y confidencialidad en la información almacenada en sistemas informáticos.

2.3 Mapa del Módulo

Nombre del Módulo	Unidad de Aprendizaje	Resultado de aprendizaje
Aplicación de la Seguridad Informática **72 horas**	**1.** Utiliza estándares de protección de la información **27 horas**	**1.1** Determina riesgos de seguridad informática con base en las características del equipo y las necesidades del usuario. **15 horas**
		1.2 Elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección. **12 horas**
	2. Administra herramientas de seguridad informática **45 horas**	**2.1** Instala y configura herramientas informáticas acorde con los estándares y buenas prácticas de seguridad en cómputo. **23 horas**
		2.2 Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado. **10 horas**
		2.3 Controla parámetros de seguridad mediante verificación y actualización acorde con nuevos requerimientos obtenidos. **12 horas**

2.4 Unidades de Aprendizaje

Unidad de aprendizaje:	**1**. Utiliza estándares de protección de la información	**27 horas**
Propósito de la unidad	Aplicar estándares de seguridad informática de acuerdo con riesgos que se identifiquen para quedar implícitos en apego a mejores prácticas del uso de la tecnología en el mercado.	
Resultado de aprendizaje:	**1.1** Determina riesgos de seguridad informática con base en las características del equipo y las necesidades del usuario.	**15 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
1.1.1 Elabora informe de análisis de riesgos de seguridad informática de una organización considerando los criterios de confidencialidad, integridad y disponibilidad de la información	• Matriz de riesgos • Ficha técnica de las características del equipo de cómputo y de comunicaciones que incluya valoración de criterios de seguridad informática. • Cuestionarios de seguridad aplicados a usuarios y administradores.	**15 %**	**A** Conceptualización de elementos de la seguridad informática. • Seguridad • Información • Informática • Seguridad informática • Principios de la seguridad informática - Confidencialidad - Integridad. - Disponibilidad **B** Clasificación de los principales riesgos de la seguridad informática. • Concepto de riesgo. • Tipos de riesgos - Alto - Medio - Bajo • Matriz de riesgo • Concepto de vulnerabilidad. • Riesgos Lógicos - Códigos maliciosos - Spam - Piratería - Fuga de información

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			- Ingeniería social. - Intrusos informáticos. - Ransomware - Ataques DDOS • Riesgos físicos **C** Recopilación de información de la organización. • Objetivos de resguardo de información en la empresa • Organigramas. • Manuales de procesos. • Controles internos de seguridad informática **D** Identifica y analiza niveles de riesgo en la organización. • Analiza configuraciones de seguridad en grupos y cuentas de usuario en el sistema operativo. - Cuestionarios. - Entrevistas. - Ficha técnica. • Políticas aplicadas - De cuenta - De auditoría - Restricciones a usuarios - Restricciones de software - Firewall - Antivirus - Antispyware • Permisos en carpetas y documentos compartidos. • Actualizaciones de sistema operativo y aplicaciones. • Respaldos de información.

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			E. Identifica riesgos físicos en la organización aplicados a equipos de cómputo y comunicaciones. • Controles de acceso. • Protección contra falla eléctrica • Protección contra desastres naturales. • Administración del software de la organización.
Sesión para recapitulación y entrega de evidencias.			

Resultado de aprendizaje:	**1.2** Elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección.	**12 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
1.2.1 Elabora el plan de seguridad informática basado en estándares internacionales estableciendo mecanismos de protección de la información y métricas de evaluación.	• Plan de seguridad a implementar. • Políticas de seguridad a implementar.	**20 %**	**A.** Analiza modelos y buenas prácticas de seguridad informática. • ITIL • Cobit • ISM3 **B.** Analiza estándares internacionales de seguridad informática • BS 17799 • Serie ISO 27000 - ISO 27001 - ISO 27002 - ISO/IMEC 27032: Directrices para la ciberseguridad - ISO/IEC 27033: Seguridad en las redes - ISO/IEC 27034: Seguridad en las aplicaciones - ISO/IEC 27035: Gestión de incidentes de seguridad de TI - ISO/IEC 27036: Gestión de incidentes de seguridad de TI • ISO 20000 **C.** Definición del plan de seguridad informática de acuerdo con los requerimientos de la organización. • Descripción de los principales elementos de protección. • Definición de las metas de seguridad a alcanzar en un periodo de tiempo establecido. • Definición de políticas.

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			- De acceso físico a equipos. - De acceso lógico a equipos. - Para la creación de cuentas de usuario. - Para el manejo de bitácoras. - De protección de red (firewall) - Para la administración de software de seguridad. - Para la gestión de actualizaciones. - De control de cambios. - De almacenamiento. - Para archivos compartidos. - De respaldo. **D.** Establece métricas y mecanismos para la evaluación de los controles implementados. • Define indicadores para evaluar la eficiencia de los controles implementados. • Define el modo en que los indicadores serán medidos.
Sesión para recapitulación y entrega de evidencias.			

Unidad de aprendizaje:	**2.** Administra herramientas de seguridad informática	**45 horas**
Propósito de la unidad	Administrar herramientas informáticas de acuerdo con el plan de seguridad determinado y situaciones específicas a resolver a fin de lograr el control y la integridad de la información.	
Resultado de aprendizaje:	**2.1** Instala y configura herramientas informáticas acorde con los estándares y buenas prácticas de seguridad en cómputo.	**23 horas**

Actividades de evaluación	Evidencias para recopilar	Ponderación	Contenidos
2.1.1 Instala y configura herramientas informáticas de manera segura y en apego al manual determinado.	• Manual de instalación y configuración de software.	**30 %**	**A.** Elaboración de manual de instalación y configuración de software. • Requerimientos de instalación. • Procedimiento de instalación. • Procedimiento de configuración. **B.** Configuración local de seguridad. • Actualizaciones automáticas para elsistema operativo y aplicaciones. • Administración de actualizaciones. - Clasificación de actualizaciones. - Servidores centrales de actualizaciones. • Manejo de cuentas. • Manejo de bitácoras. • Manejo de software. • Firewall local. • Establece políticas para el manejo del antivirus. • Establece políticas para el manejo del antispyware. • Permisos de archivos y carpetas compartidas. • Cifrado de archivos y carpetas.

Actividades de evaluación	Evidencias para recopilar	Ponderación	Contenidos
			C. Configuración de red de seguridad informática • Para el firewall perimetral. • Sistema de detección de intrusos. • Protocolos de seguridad. - IPSEC. - http sobre ssl. • Permisos de archivos y carpetas compartidas.
Sesión para recapitulación y entrega de evidencias.			

Resultado de aprendizaje:	**2.2** Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado.	**10 horas**

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
2.2.1 Monitorea la operación de las herramientas informáticas a fin de garantizar su funcionamiento y elabora un portafolio de evidencias que incluya: • Reporte del estado delas aplicaciones. • Reporte de modificación de configuraciones. • Respaldo digital de configuraciones.	• Portafolio de evidencias.	**20 %**	**A.** Elabora e interpreta reportes del estado de las aplicaciones • Estado de las aplicaciones. • Funcionamiento. **B.** Modifica configuraciones • Conforme procedimientos definidos en el manual. • Nuevos requerimientos. • Respalda las configuraciones de las aplicaciones
Sesión para recapitulación y entrega de evidencias.			

Resultado de aprendizaje:	**2.3** Controla parámetros de seguridad mediante verificación y actualización, acorde con nuevos requerimientos obtenidos.	**12 horas**

Actividades de evaluación	Evidencias para recopilar	Ponderación	Contenidos
2.3.1 Revisa las configuraciones de equipos y redes de comunicación evaluando el cumplimiento de las políticas del plan de seguridad, así como determinar nuevos requerimientos. Elabora un portafolio de evidencias que incluya: • Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. • Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados.	• Portafolio de evidencias.	**15 %**	**A.** Revisa la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación • Herramientas de auditoria para la recopilación de información • Herramientas de auditoría para la comparación de configuraciones **B.** Analiza reportes de las aplicaciones • Genera reportes de operación de las aplicaciones. • Compara métricas establecidas con los resultados obtenidos. • Identifica nuevos requerimientos. • Define nuevos requerimientos deseguridad. en caso necesario. • Establece medidas para solucionarnuevos requerimientos • Determina alternativas para optimizar los existentes. **C.** Implementación de acciones correctivas en la configuración y ejecución de herramientas de seguridad informática. • Planes de contingencia - Definición y características - Alternativas de solución - Escalamiento de problemas • Actualización de software y de equipo de seguridad
Sesión para recapitulación y entrega de evidencias.			

2.5 Referencias

Básica:

- Hernández, E. (2011). *Auditoría y seguridad de la función informática.* Alfaomega.
- Terán, D. (2014). *Administración estratégica de la función informática*. Alfaomega.
- Walker, A. (2006). *Seguridad, Spam, Spyware y Virus* (1ª ed.) Anaya Multimedia.
- Fine, L. (2009). *Seguridad en Centros de Cómputo*. Trillas.

Complementaria:

- Lam, K., LeBlanc, D y Smith, B. (2004). *Assessing Network Security.* Microsoft Press.
- Fine, L. (2004), *Administración de Centros de Cómputo* (1ª ed.). Trillas.
- Piattini, M., Del Peso E. y Del Peso, M. (2008). *Auditoría De Tecnologías Y Sistemas De Información*. Alfaomega.
- Piattini, M. y Del Peso, E. (2001). *Auditoría Informática - Un Enfoque Práctico* (2ª ed.) Alfaomega.
- Ramos, A. (2004). *Protege tu PC* (1ª ed.). Anaya Multimedia.
- Smith, B. y Komar, B. (2005). *Windows Security Resource Kit* (2ª ed.) Microsoft Press.

Páginas Web:

- Alegsa, L. (2023, 09 de julio). *Definición de Seguridad informática*. http://www.alegsa.com.ar/Dic/seguridad%20informatica.php
- DGIRE. *Seguridad digital: definición.* Consultado el 02 de mayo del 2024. https://www.dgire.unam.mx/webdgire/contenido_wp/documentos/seguridadescolar/tecnologia-informacion-definicion.html#:~:text=Es%20decir%2C%20la%20seguridad%20digital,datos%20privados%20y%20datos%20sensibles.
- Becolve Digital. (2021, 29 de julio). *Estándares de Ciberseguridad. Qué son y para qué sirven*. https://becolve.com/blog/estandares-de-ciberseguridad-que-son-y-para-que-sirven/
- IBM. *¿Qué es la ciberseguridad?* Consultado el 02 de mayo del 2024. https://www.ibm.com/mx-es/topics/cybersecurity#:~:text=La%20ciberseguridad%20tiene%20como%20objetivo,costosos%2C%20y%20todo%20lo%20dem%C3%A1s.