Programa de estudios del módulo

Aplicación de la seguridad informática

Núcleo de Formación Profesional

Área(s):
Tecnología y Transporte

Carrera(s):
Profesional Técnico-Bachiller en Informática

3° semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad informática

Área(s): Tecnología y Transporte

Carrera(s): PT-B en Informática

Semestre(s): 3°

Horas por semestre: 72

Créditos por semestre: 7

Fecha de diseño o actualización: 21 de abril 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 Barrientos
Dirección General

Lauro Cordero Frayre
Secretaría General

Hugo Nicolás Pérez González
Secretaría Académica

Edith Chávez Ramos
Dirección de Diseño Curricular

Aplicación de la seguridad informática

Contenido **Pág.**

CAPÍTULO I: Generalidades del Profesional Técnico-Bachiller

1.1 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.

1.2 Competencias Transversales al Currículum (*)

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 informática** se imparte en el tercer semestre y corresponde al núcleo de formación profesional, de la carrera de Profesional Técnico-Bachiller en Informática. Tiene como finalidad, que el alumno conozca y aplique los procedimientos y estándares de seguridad en equipos de cómputo y en las redes de comunicación, que acorde a los requerimientos de uso, conserven la integridad de la información generada, procesada y almacenada.

Para ello, el módulo está conformado por dos unidades de aprendizaje. La primera unidad aborda la aplicación de estándares de protección de información; la segunda unidad desarrolla la administración de herramientas y métodos de seguridad informática y en la tercera unidad se establecen las acciones de monitoreo y control de parámetros de protección.

La formación profesional del PT-B, está diseñada con un enfoque de procesos, lo cual implica un desarrollo en la adquisición de competencias profesionales 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.

Además, estas competencias se complementan con la incorporación de competencias básicas, profesionales y genéricas que refuerzan la formación tecnológica y científica, y fortalecen la formación integral de los educandos; que los prepara 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, el desarrollo pleno de su potencial en los ámbitos profesional y personal y la convivencia de manera armónica con el medio ambiente y la sociedad.

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

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.** Aplicación de 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. Administración de 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**. Aplicación de 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 desastresnaturales. • Administración del software de la organización.

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 deseguridad 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 principaleselementos de protección. • Definición de las metas de seguridad a alcanzar en un periodo de tiempo establecido. • Definición de políticas. - De acceso físico a equipos. - De acceso lógico a equipos. - Para la creación de cuentas deusuario.

Actividades de evaluación	Evidencias a recopilar	Ponderación	Contenidos
			- 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 controlesimplementados. • Define el modo en que los indicadores serán medidos.
Sesión para recapitulación y entrega de evidencias.			

Unidad de aprendizaje:	**2.** Administración de 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	• Instala y configura herramientas informáticas de manera segura y en apego al manual determinado	**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.

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**.**	• Reporte del estado de las aplicaciones. • Reporte de modificación de configuraciones • Respaldo digital de configuraciones.	**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.	• 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.	**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:

Enrique H., (2011), *Auditoria y seguridad de la función informática informática.* México, Alfaomega.

Terán David**,** *Administración estratégica de la función informática***,** Alfaomega.

Wlalker, Andy, (2006), *Seguridad, Spam, Spyware y Virus*, 1a. Edición, España, Anaya Multimedia.

Fine, Leonard H. (2009), *Seguridad en Centros de Cómputo*, Trillas.

Complementaria:

Lam, Kevin; LeBlanc, David; Smith, Ben. *Assessing Network Security.* Microsoft Corp.,

Fine, Leonard H.(2004), *Administración de Centros de Cómputo***,** 1a. Edición, MéxicoTrillas.

Piattini, Mario; Del Peso, Emilio; del Peso, Mar,(2008), *Auditoría De Tecnologías Y Sistemas De Información*, México, Alfaomega.

Piattini, Mario; Del Peso, Emilio,(2001), *Auditoría Informática - Un Enfoque Práctico* - 2ª ed. Ampliada Y Revisada, México, Alfaomega.

Ramos Varón, Antonio Angel,(2004), *Protege tu PC,* 1a. Edición, España, Anaya Multimedia.

Smith, Ben; Komar, Brian.(2005), *Windows Security Resource Kit*. 2a. Edición. Microsoft Corp.

Páginas Web:

Biblioteca digital CONALEP.- Cursos Calidad, *Seguridad Informática*. Consultado el 10 de marzo de 2023: http://sied.conalep.edu.mx/bv3/ y http://www.cursos-en-mexico.com.mx/cursos/calidad-seguridad-informatica?gclid=CKnwlpTPjKoCFU976wodnE6rzA

Métodos y tipos de control. Consultado el 10 de marzo de 2023. http://www.mailxmail.com/curso/informatica/centrodecomputo/capitulo4.htm

Definición de Seguridad informática - ¿Qué es Seguridad informática? Concepto del término seguridad informática. Consultado el 10 de marzo de 2023: http://www.alegsa.com.ar/Dic/seguridad%20informatica.php