

## Aplicación de herramientas de seguridad en hardware y software

Área(s):

Tecnología y transporte.

Carrera(s):

**Profesional Técnico y  
Profesional Técnico-Bachiller en**

Soporte y mantenimiento de equipo de  
cómputo



 **Programa  
de Estudios**

**Editor:** Colegio Nacional de Educación Profesional Técnica

**Programa de Estudios del Módulo:** Aplicación de herramientas de seguridad en hardware y software.

**Área(s):** Tecnología y transporte.

**Carrera(s):** Profesional Técnico y Profesional Técnico –Bachiller en Soporte y mantenimiento de equipo de cómputo.

**Semestre(s):** Sexto.

D.R 2010, Colegio Nacional de Educación Profesional Técnica.

Este material es vigente a partir de febrero de 2013.

Prohibida la reproducción total o parcial de esta obra por cualquier medio, sin autorización por escrito del Conalep.

Calle 16 de Septiembre 147 Norte, Col. Lázaro Cárdenas, Metepec, Edo. de México, C. P. 52148.

HECHO EN MÉXICO.

Tercera Edición.

[www.conalep.edu.mx](http://www.conalep.edu.mx)

Fecha en que se terminó su edición: enero de 2013.

## Directorio

Directora General  
**Candita Victoria Gil Jiménez**

Secretario General  
**Roger Armando Frías Frías**

Secretaria Académica  
**María Elena Salazar Peña**

Secretaria de Administración  
**Corazón de María Madrigal**

Secretario de Planeación y Desarrollo Institucional  
**Francisco Cuauhtémoc Santiago Jaime**

Secretario de Servicios Institucionales  
**Pedro Eduardo Azuara Arechederra**

Director Corporativo de Asuntos Jurídicos  
**Juan Carlos Castillo Guzmán**

Titular de la Unidad de Estudios e Intercambio Académico  
**Patricia Guadalupe Guadarrama Hernández**

Director Corporativo de Tecnologías Aplicadas  
**Humberto Zentella Falcón**

Directora de Diseño Curricular  
**Silvia Alejandra Guzmán Saldaña**

Coordinadora de las Áreas Básicas y de Servicios  
**Caridad del Carmen Cruz López**

Coordinador de las Áreas de Mantenimiento e Instalación,  
Electricidad, Electrónica y TIC  
**Marco Antonio Valadez Pérez**

Coordinador de las Áreas de Procesos de Producción y  
Transformación  
**René Montero Montano**

### Grupo de trabajo:

#### Técnico:

Con la asesoría de consultores contratados por obra y tiempo  
determinados

### Grupo de trabajo

#### Técnico:

**Servicios Académicos y Educativos S. C.**

#### Metodológico:

**Servicios Académicos y Educativos S. C.**

## Aplicación de herramientas de seguridad en hardware y software

Contenido		Pág.
	Mensaje de la Directora General	5
	Presentación de la Secretaria Académica	7
<b>Capítulo I:</b>	<b>Generalidades de la(s) carrera(s)</b>	
1.1	Objetivo general de la(s) carrera(s)	8
1.2	Competencias transversales al currículum	9
<b>Capítulo II:</b>	<b>Aspectos específicos del módulo</b>	
2.1	Presentación	11
2.2	Propósito del módulo	13
2.3	Mapa del módulo	14
2.4	Unidades de aprendizaje	15
2.5	Referencias	25

**Mensaje de la  
Directora General**

Me es grato poner en sus manos una herramienta muy útil para orientar a los maestros en el proceso de enseñanza y para ayudar a los alumnos en la planeación de su aprendizaje.

Esta, es precisamente la importancia de los programas de estudio: favorecer el desarrollo de destrezas, habilidades y valores, que les permitan afrontar con éxito los retos de la actualidad.

Se trata, sin lugar a dudas, del principal recurso didáctico que tendrán a su disposición para garantizar una educación integral y de calidad.

Sin dejar de lado, desde luego, aquéllos que les brinda la Biblioteca Digital de la Red Académica del CONALEP.

En ellos encontrarán los propósitos de cada módulo, la manera y el tiempo en que deben ser alcanzados, así como los respectivos criterios de evaluación.

Utilizarlos en forma cotidiana y sistemática es deber de todos, teniendo siempre presente que están elaborados con base en las necesidades de lo que el sector productivo exige y la sociedad merece.

México tiene depositada su confianza en el CONALEP, como pilar de una enseñanza técnica de vanguardia.

No es casual que el Gobierno de la República, a través de la Secretaría de Educación Pública, haya decidido fortalecer la noble labor que se realiza en nuestras aulas, laboratorios y talleres, con un Modelo Académico de primera.

Un modelo derivado de la Reforma Integral de la Educación Media Superior:

- Que avanza hacia la consolidación del Sistema Nacional de Bachillerato y la construcción de un Marco Curricular Común;
- Que se fortalece con las valiosas aportaciones de los profesores, estudiantes y representantes de la iniciativa privada;
- Que es congruente con los desafíos de la globalización;
- Y que forja generaciones competentes, emprendedoras, creativas y capaces de atender los principales problemas del país.

Este es el perfil de los profesionales que estamos formando.

Este es el compromiso que asumimos con entrega, vocación y convicción.



Y esta es la razón que nos impulsa a seguir hacia adelante.

Estimados docentes y alumnos:

Yo los invito a aprovechar al máximo estos programas de estudio, como guías de nuestras responsabilidades académicas y formativas, que sirvan de facilitadores de conocimientos e instrumentos para un diálogo respetuoso, permanente y fecundo.

Hagamos juntos la diferencia con la excelencia, responsabilizándonos de la tarea que nos corresponde cumplir.

Demostremos que sabemos, que podemos y que somos **ORGULLOSAMENTE CONALEP**.

**M.A. Candita Victoria Gil Jiménez**  
**Directora General del Sistema CONALEP**

## **Presentación de la Secretaría Académica**

De acuerdo con el Modelo Académico CONALEP, la propuesta de aprendizajes considerados para promoverse en un módulo integrado al diseño de una carrera o trayecto se concreta en el programa de estudio, en la guía pedagógica y en la de evaluación. Estos documentos, constituyen el principal referente para planear y desarrollar el proceso de enseñanza-aprendizaje en las aulas, talleres y laboratorios de nuestra institución.

Los programas y guías de estudio han sido diseñados con un enfoque de competencias, con lo que se da cumplimiento a los preceptos de la Reforma Integral de la Educación Media Superior (RIEMS), que indica el fomento y promoción de competencias genéricas y disciplinares que debe poseer una persona egresada de la educación media superior, mismas que le servirán para toda la vida; mientras que las competencias profesionales, le permiten el desempeño de funciones laborales requeridas por los sectores productivos regional y nacional.

En cada uno de los documentos curriculares se refleja el desempeño de especialistas técnicos y de profesionales en diseño curricular, así como las aportaciones de los integrantes del sector productivo, contribuyendo con sus conocimientos, habilidades y experiencias para el profesional técnico y el profesional técnico bachiller.

Lo anterior, hace posible la amplia aceptación de nuestros egresados, ya sea en el mercado laboral en el que se desempeñan con profesionalismo, o bien, en las Universidades o Institutos Tecnológicos, si es que deciden continuar estudios en el nivel superior, acción en la que destacan por su sólida formación.

**Mtra. María Elena Salazar Peña**

## **CAPÍTULO I: Generalidades de la carrera.**

### **1.1. Objetivo general de la carrera.**

#### **P.T. y P.T-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.

## 1.2. Competencias transversales al currículum ( \* )

Competencias Genéricas	Atributos
<p><b>Se autodetermina y cuida de sí</b></p> <p>1. Se conoce y valora a sí mismo y aborda problemas y retos teniendo en cuenta los objetivos que persigue.</p>	<ul style="list-style-type: none"> <li>• Enfrenta las dificultades que se le presentan y es consciente de sus valores, fortalezas y debilidades.</li> <li>• Identifica sus emociones, las maneja de manera constructiva y reconoce la necesidad de solicitar apoyo ante una situación que lo rebase.</li> <li>• Elige alternativas y cursos de acción con base en criterios sustentados y en el marco de un proyecto de vida.</li> <li>• Analiza críticamente los factores que influyen en su toma de decisiones.</li> <li>• Asume las consecuencias de sus comportamientos y decisiones.</li> <li>• Administra los recursos disponibles teniendo en cuenta las restricciones para el logro de sus metas.</li> </ul>
<p>2. Es sensible al arte y participa en la apreciación e interpretación de sus expresiones en distintos géneros.</p>	<ul style="list-style-type: none"> <li>• Valora el arte como manifestación de la belleza y expresión de ideas, sensaciones y emociones.</li> <li>• 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.</li> <li>• Participa en prácticas relacionadas con el arte.</li> </ul>
<p>3. Elige y practica estilos de vida saludables.</p>	<ul style="list-style-type: none"> <li>• Reconoce la actividad física como un medio para su desarrollo físico, mental y social.</li> <li>• Toma decisiones a partir de la valoración de las consecuencias de distintos hábitos de consumo y conductas de riesgo.</li> <li>• Cultiva relaciones interpersonales que contribuyen a su desarrollo humano y el de quienes lo rodean.</li> </ul>
<p><b>Se expresa y comunica</b></p> <p>4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados.</p>	<ul style="list-style-type: none"> <li>• Expresa ideas y conceptos mediante representaciones lingüísticas, matemáticas o gráficas.</li> <li>• Aplica distintas estrategias comunicativas según quienes sean sus interlocutores, el contexto en el que se encuentra y los objetivos que persigue.</li> <li>• Identifica las ideas clave en un texto o discurso oral e infiere conclusiones a partir de ellas.</li> <li>• Se comunica en una segunda lengua en situaciones cotidianas.</li> <li>• Maneja las tecnologías de la información y la comunicación para obtener información y expresar ideas.</li> </ul>
<p><b>Piensa crítica y reflexivamente</b></p> <p>5. Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos.</p>	<ul style="list-style-type: none"> <li>• Sigue instrucciones y procedimientos de manera reflexiva, comprendiendo como cada uno de sus pasos contribuye al alcance de un objetivo.</li> <li>• Ordena información de acuerdo a categorías, jerarquías y relaciones.</li> <li>• Identifica los sistemas y reglas o principios medulares que subyacen a una serie de fenómenos.</li> <li>• Construye hipótesis y diseña y aplica modelos para probar su validez.</li> <li>• Sintetiza evidencias obtenidas mediante la experimentación para producir conclusiones y formular nuevas preguntas.</li> </ul>

<p><b>6.</b> Sustenta una postura personal sobre temas de interés y relevancia general, considerando otros puntos de vista de manera crítica y reflexiva.</p>	<ul style="list-style-type: none"> <li>• Utiliza las Tecnología y transporte para procesar e interpretar información.</li> <li>• Elige las fuentes de información más relevantes para un propósito específico y discrimina entre ellas de acuerdo a su relevancia y confiabilidad.</li> <li>• Evalúa argumentos y opiniones e identifica prejuicios y falacias.</li> <li>• 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.</li> <li>• Estructura ideas y argumentos de manera clara, coherente y sintética.</li> </ul>
<p><b>Aprende de forma autónoma</b></p> <p><b>7.</b> Aprende por iniciativa e interés propio a lo largo de la vida.</p>	<ul style="list-style-type: none"> <li>• Define metas y da seguimiento a sus procesos de construcción de conocimiento.</li> <li>• Identifica las actividades que le resultan de menor y mayor interés y dificultad, reconociendo y controlando sus reacciones frente a retos y obstáculos.</li> <li>• Articula saberes de diversos campos y establece relaciones entre ellos y su vida cotidiana.</li> </ul>
<p><b>Trabaja en forma colaborativa</b></p> <p><b>8.</b> Participa y colabora de manera efectiva en equipos diversos.</p>	<ul style="list-style-type: none"> <li>• Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.</li> <li>• Aporta puntos de vista con apertura y considera los de otras personas de manera reflexiva.</li> <li>• Asume una actitud constructiva, congruente con los conocimientos y habilidades con los que cuenta dentro de distintos equipos de trabajo.</li> </ul>
<p><b>Participa con responsabilidad en la sociedad</b></p> <p><b>9.</b> Participa con una conciencia cívica y ética en la vida de su comunidad, región, México y el mundo.</p>	<ul style="list-style-type: none"> <li>• Privilegia el diálogo como mecanismo para la solución de conflictos.</li> <li>• Toma decisiones a fin de contribuir a la equidad, bienestar y desarrollo democrático de la sociedad.</li> <li>• 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.</li> <li>• Contribuye a alcanzar un equilibrio entre el interés y bienestar individual y el interés general de la sociedad.</li> <li>• Actúa de manera propositiva frente a fenómenos de la sociedad y se mantiene informado.</li> <li>• Advierte que los fenómenos que se desarrollan en los ámbitos local, nacional e internacional ocurren dentro de un contexto global interdependiente.</li> </ul>
<p><b>10.</b> Mantiene una actitud respetuosa hacia la interculturalidad y la diversidad de creencias, valores, ideas y prácticas sociales.</p>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Asume que el respeto de las diferencias es el principio de integración y convivencia en los contextos local, nacional e internacional.</li> </ul>
<p><b>11.</b> Contribuye al desarrollo sustentable de manera crítica, con acciones responsables.</p>	<ul style="list-style-type: none"> <li>• Asume una actitud que favorece la solución de problemas ambientales en los ámbitos local, nacional e internacional.</li> <li>• Reconoce y comprende las implicaciones biológicas, económicas, políticas y sociales del daño ambiental en un contexto global interdependiente.</li> <li>• Contribuye al alcance de un equilibrio entre los intereses de corto y largo plazo con relación al ambiente.</li> </ul>

\*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 Aplicación de herramientas de seguridad en hardware y software, es de tipo específico, pertenece al trayecto técnico Seguridad de redes y sistemas informáticos y se imparte en el sexto semestre de la carrera de Profesional Técnico y Profesional Técnico-Bachiller en Soporte y mantenimiento de equipo de cómputo. Se desarrolla con un enfoque a la adquisición de competencias en 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.

El presente módulo 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 en hardware y software.

La contribución del módulo al perfil de egreso de la carrera en las que está considerado, incluye el desarrollo de competencias para 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.

El PT y el PT-B en Soporte y mantenimiento de equipo de cómputo con el trayecto técnico en Seguridad de redes y sistemas informáticos, debe integrar en este módulo las competencias de operación de equipos de cómputo, programación estructurada, interpretación de documentación técnica, diagnóstico de fallas en equipos de cómputo, instalación de redes de datos, mantenimiento de equipo de cómputo básico, montaje de cibercafés para mantener en operación un equipo, previniendo riesgos en la operación que podrían interrumpir el servicio o corrigiendo fallas presentadas en los mismos.

Además, estas competencias se complementan con la incorporación de otras competencias básicas, las 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 docente tendrá que diversificarse en este módulo a fin de coadyuvar a que sus alumnos desarrollen las competencias propuestas en el módulo, realizando funciones tanto de facilitador del aprendizaje como de preceptor, y que consistirán en la guía y acompañamiento de los alumnos 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.

En el proceso de evaluación de las competencias, los docentes, en coordinación con el plantel, tienen la facultad de instrumentar las modalidades de autoevaluación, coevaluación y heteroevaluación, que están vinculadas a una actividad de evaluación seleccionada para este fin, indicada en este programa de estudios y explicitada en la guía de evaluación correspondiente.

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, en lo general, por los alumnos con el propósito de verificar que estos se han alcanzado o, en caso contrario, determinar las acciones de mejora pertinentes. En este proceso, los docentes tienen la facultad de instrumentar las modalidades de autoevaluación, coevaluación y heteroevaluación, de acuerdo con las condiciones particulares de su entorno, aun cuando de manera institucional se definen los criterios e indicadores para su aplicación.

## 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
<b>Aplicación de herramientas de seguridad en hardware y software</b>  <b>90 horas</b>	<b>1.</b> Diagnóstico de riesgos y amenazas en la seguridad del equipo  <b>35 horas</b>	<b>1.1</b> Identifica riesgos y amenazas en la seguridad del hardware y software con base a los alertamientos que emite el equipo. <b>15 horas</b>  <b>1.2</b> Evalúa la integridad de la información y operación del equipo de cómputo conforme recomendaciones técnicas de seguridad contra riesgos y amenazas. <b>20 horas</b>
	<b>2.</b> Implementación de tecnología de seguridad en hardware y software del equipo de cómputo.  <b>55 horas</b>	<b>2.1</b> Establece recomendaciones de tecnología de seguridad en hardware y software orientada a la protección y preservación de la integridad de la información. <b>25 horas</b>  <b>2.2</b> Instala tecnología de seguridad protegiendo la información y equipo de cómputo contra amenazas a su integridad. <b>30 Horas</b>

**2.4. Unidades de aprendizaje**

<b>Unidad de aprendizaje:</b>	Diagnóstico de riesgos y amenazas en la seguridad del equipo.	<b>Número</b>	1
<b>Propósito de la unidad:</b>	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.		35 horas
<b>Resultado de aprendizaje:</b>	1.1 Identifica riesgos y amenazas en la seguridad del hardware y software con base a los alertamientos que emite el equipo.		15 horas

Actividades de evaluación	C	P	A	Evidencias a recopilar	Ponderación	Contenidos
1.1.1 Identifica riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo, elaborando un reporte de resultados	✓	✓	✓	<ul style="list-style-type: none"> <li>Reporte de resultados de la simulación de riesgos y amenazas.</li> <li>Rúbrica</li> </ul>	20%	<b>A.</b> Identificación de riesgos y amenazas en el hardware y software <ul style="list-style-type: none"> <li>Descripción de las vulnerabilidades.</li> <li>Afectación a equipos               <ul style="list-style-type: none"> <li>Equipo de cómputo</li> <li>Routers</li> <li>Cable módems</li> <li>Servidores de video</li> <li>Impresoras y faxes</li> </ul> </li> <li>Afectación a programas               <ul style="list-style-type: none"> <li>Sistemas operativos</li> <li>Servidores</li> <li>Bases de datos</li> <li>Navegadores</li> <li>Aplicaciones de oficina</li> </ul> </li> <li>Normas de seguridad incompletas en el desarrollo de software.</li> </ul>

						<p><b>B.</b> Detección de debilidades en seguridad en dispositivos ADSL y su entorno.</p> <ul style="list-style-type: none"> <li>• Comandos de monitoreo de tráfico hacia determinados sitios.</li> <li>• .Herramienta de evaluación de seguridad de Microsoft (MSAT)</li> <li>• Herramienta de bloqueo IIS</li> <li>• Reportador de puertos (Port reporter).</li> <li>• Muestreo de seguridad de la red (network security scan).</li> <li>• Monitoreo de las actualizaciones de seguridad</li> </ul> <p><b>C.</b> Evaluación de actividades en el sistema de información que atentan contra la seguridad</p> <ul style="list-style-type: none"> <li>• Reconocimiento de sistemas.</li> <li>• Detección de vulnerabilidades.</li> <li>• Robo de información mediante interceptación de mensajes.</li> <li>• Modificación de la secuencia de mensajes.</li> <li>• Análisis de tráfico</li> <li>• Ataques de suplantación de identidad.</li> <li>• Modificación del tráfico en tablas de enrutamiento</li> <li>• Conexión no autorizada a equipos</li> </ul>
--	--	--	--	--	--	--

						• Servicios innecesarios habilitados.
--	--	--	--	--	--	---------------------------------------

C: Conceptual

P: Procedimental

A: Actitudinal

<b>Resultado de aprendizaje:</b>	1.2 Evalúa la integridad de la información y operación del equipo de cómputo conforme recomendaciones técnicas de seguridad contra riesgos y amenazas.	20 horas
----------------------------------	--	----------

Actividades de evaluación	C	P	A	Evidencias a recopilar	Ponderación	Contenidos
1.2.1 Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación.	✓	✓	✓	<ul style="list-style-type: none"> <li>• Diagnóstico de la integridad de la información.</li> <li>• Rúbrica.</li> </ul>	25 %	<p><b>A.</b> Identificación de amenazas (agentes externos) de intrusión</p> <ul style="list-style-type: none"> <li>• Conductos de intrusión               <ul style="list-style-type: none"> <li>- Hackers</li> <li>- Crakers.</li> <li>- Sniffers</li> <li>- Phreakers</li> <li>- Spammers.</li> <li>- Piratas informáticos</li> <li>- Creadores de virus</li> <li>- Personal interno</li> <li>- Intrusos remunerados.</li> </ul> </li> <li>• Virus               <ul style="list-style-type: none"> <li>- De boot</li> <li>- De archivos ejecutables.</li> <li>- De lenguaje JAVA</li> <li>- De macros.</li> </ul> </li> <li>• Troyanos</li> <li>• Rootkits</li> <li>• Gusanos</li> </ul>

					<ul style="list-style-type: none"> <li>• Spyware</li> <li>• Malware</li> <li>• Navegación por servidores web</li> <li>• Intercepción pasiva (eavesdropping).</li> <li>• Espionaje de información (snooping)</li> <li>• Modificación de la información (tampering)</li> <li>• Envío de correos electrónicos con nuestra identidad</li> <li>• Saturación de servidores web</li> <li>• Suplantación de identidad (spoofing).</li> </ul> <p><b>B.</b> Evaluación de riesgos originados por debilidades en la instalación.</p> <ul style="list-style-type: none"> <li>• Protocolos de red no necesarios</li> <li>• Actualización versión del IOS</li> <li>• Archivos e impresoras compartidos usando TCP/IP</li> <li>• NetBIOS habilitado sobre TCP</li> <li>• Red o sistema informático no aislado de otras redes o sistemas</li> <li>• Contraseñas potencialmente débiles</li> <li>• Antivirus desactualizada o inapropiado</li> <li>• Navegador con versiones no recientes.</li> <li>• Ejecución de archivos de programa de dudoso origen.</li> <li>• Servicios de red no utilizados habilitados.</li> </ul>
--	--	--	--	--	--



						<ul style="list-style-type: none"><li>• Rutas estáticas configuradas en donde sea necesario</li><li>• Ejecución de applets de Java y activex.</li><li>• Respaldos de información no actualizados.</li><li>• Uso de WEP / WPA (Wireless Equivalent privacy/WiFi Protected Acces).</li></ul>
--	--	--	--	--	--	--

**Sesión para recapitulación y entrega de evidencias**

**C:** Conceptual

**P:** Procedimental

**A:** Actitudinal

<b>Unidad de aprendizaje:</b>	Implementación de tecnología de seguridad en hardware y software del equipo de cómputo.	<b>Número</b>	<b>2</b>
<b>Propósito de la unidad:</b>	Aplicar la tecnología de seguridad en hardware y software considerando el diagnóstico y recomendaciones en riesgos y amenazas a la información.	55 horas	
<b>Resultado de aprendizaje:</b>	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	C	P	A	Evidencias a recopilar	Ponderación	Contenidos
2.1.1 Establece recomendaciones de seguridad identificando sus efectos a través de un reporte de resultados	✓	✓	✓	<ul style="list-style-type: none"> <li>Listado de Recomendaciones de seguridad.</li> <li>Reporte de resultados.</li> <li>Rúbrica.</li> </ul>	<b>25%</b>	<p><b>A.</b> Preparación de recomendaciones contra vulnerabilidades</p> <ul style="list-style-type: none"> <li>Autorización y registro de usuarios               <ul style="list-style-type: none"> <li>Control de acceso a usuarios locales y remotos</li> <li>Certificados digitales</li> <li>Servidores de autenticación</li> <li>Administración de contraseñas</li> </ul> </li> <li>Sistemas biométricos.               <ul style="list-style-type: none"> <li>Reconocimiento de firmas manuscritas</li> <li>Huellas dactilares</li> <li>Análisis del iris</li> </ul> </li> <li>Recomendaciones de criptografía.               <ul style="list-style-type: none"> <li>Implantación de algoritmos en hw y sw.</li> <li>Sistemas criptográficos</li> <li>Algoritmos en protocolos</li> </ul> </li> </ul> <p><b>B.</b> Planeación de acciones a favor de la seguridad.</p> <ul style="list-style-type: none"> <li>Identificación de actividades:</li> </ul>

						<ul style="list-style-type: none"> <li>- Denegación de servicio.</li> <li>- Modificación al contenido de mensajes.</li> <li>- Suplantación de actividad.</li> <li>- Conexión no autorizada a equipos y servidores.</li> <li>• Prevención de ataques que realicen una llamada al sistema operativo.</li> <li>• Prevención de ataques que traten de acceder a carpetas dentro del servidor web.</li> <li>• Prevención de ataques que exploten la identificación de URL.</li> </ul> <p><b>C.</b> Elaboración de políticas para el desarrollo de aplicaciones en internet</p> <ul style="list-style-type: none"> <li>• Autenticación del usuario</li> <li>• Administración de sesiones del usuario.</li> <li>• Encriptación de datos corruptibles.</li> <li>• Protección con comandos y métodos de HTTP.</li> <li>• Prevención de ataques tipo Cross Site Scripting.</li> </ul>
--	--	--	--	--	--	---

C: Conceptual

P: Procedimental

A: Actitudinal

<b>Resultado de aprendizaje:</b>	<b>2.2</b> Instala tecnología de seguridad protegiendo la información y equipo de cómputo contra amenazas a su integridad.	30 horas
----------------------------------	--	----------

Actividades de evaluación	C	P	A	Evidencias a recopilar	Ponderación	Contenidos
<b>2.2.1</b> Instala tecnología de seguridad reportando su efecto en la integridad de la información.  COEVALUACIÓN.	✓	✓	✓	<ul style="list-style-type: none"> <li>Reporte de resultados de la instalación de tecnología de seguridad.</li> <li>Rúbrica.</li> </ul>	<b>30%</b>	<p><b>A.</b> Instalación de herramientas de seguridad en redes de computadoras</p> <ul style="list-style-type: none"> <li>Restricciones a los dispositivos ADSL (hardening).               <ul style="list-style-type: none"> <li>Eliminar servicios de entrada salida innecesarios.</li> <li>Restricción en listas de control de acceso.</li> <li>Privilegios de acceso a módems y routers, así como al personal.</li> <li>Acceso físico a los dispositivos.</li> <li>No ejecución de archivos de programa de dudoso origen</li> <li>Ejecución de applets de Java y activex.</li> </ul> </li> <li>Configuración de de seguridad en modems y dispositivos ADSL.</li> <li>Configuración de seguridad en enlaces ADSL.</li> </ul> <p><b>B.</b> Instalación de herramientas de seguridad en redes VPN y Windows</p> <ul style="list-style-type: none"> <li>Uso de protocolos               <ul style="list-style-type: none"> <li>PPTP</li> <li>L2F</li> <li>L2TP</li> </ul> </li> </ul>

					<ul style="list-style-type: none"> <li>• Redes basadas en SSL (Secure Socket Layers).</li> <li>• Recomendaciones de seguridad de Microsoft.</li> </ul> <p><b>C.</b> Aplicación de seguridad a componentes físicos en oficinas de la organización.</p> <ul style="list-style-type: none"> <li>• Protocolo WEP</li> <li>• Protocolo WPA</li> <li>• Estándar RSN</li> <li>• Estándar 802.1x</li> <li>• Detección de intentos de intrusión</li> <li>• Separación de la red inalámbrica de la red local interna</li> </ul> <p><b>D.</b> Instalación de tecnología de seguridad en servicios de internet</p> <ul style="list-style-type: none"> <li>• Actualización parches de seguridad</li> <li>• Seguridad en función de la zona de trabajo             <ul style="list-style-type: none"> <li>- Intranet</li> <li>- Internet</li> <li>- Sitios de confianza</li> <li>- Sitios restringidos</li> </ul> </li> <li>• Control de cookies</li> <li>• Discriminación en la descarga desde internet</li> <li>• Evasión a sitios dudosos</li> </ul>
--	--	--	--	--	---

						<ul style="list-style-type: none"> <li>• Evaluación enlaces incluidos en correo electrónico</li> <li>• Control de contenido activo en páginas WEB</li> <li>• Opciones avanzadas de seguridad en explorador</li> <li>• Control de certificados</li> <li>• Medidas contra SPAM</li> <li>• Medidas contra PHISING.</li> </ul> <p><b>E.</b> Comunicación de políticas operativas de seguridad informática.</p> <ul style="list-style-type: none"> <li>• Acceso a los sistemas</li> <li>• Operación del equipo</li> <li>• Desarrollo de programas</li> <li>• Configuración de redes</li> <li>• Norma ISO 14000.</li> </ul>
<p><b>Sesión para recapitulación y entrega de evidencias.</b></p>						

**C:** Conceptual

**P:** Procedimental

**A:** Actitudinal

## 2.5. Referencias

### Básicas:

- Gómez Vieites, Álvaro. **Enciclopedia de la seguridad informática**. Alfaomega RA-MA, México 2007.
- Ariganello, Ernesto. **Técnicas de Configuración de Routers Cisco**, Alfaomega Grupo Editor, 2008.
- Roebuck, Kevin, **Wireless Security**, Editorial Tebbo, 2011.

### Complementarias:

- Comer, Douglas E. **Redes Globales de Información con Internet y TCP/ IP**. Prentice Hall, México, 2000.
- Cisco Networking Academy; Cisco Systems, **Fundamentos de seguridad de redes**, Pearson Alhambra, 2005.

### Páginas web:

- Ataques informáticos (DNS seguro)**, Disponible en: <http://www.dnssec.net>, [12/10/15]
- Ataques informáticos (KeyGhost)**, Disponible en: <http://www.keyghost.com>, [12/10/15]
- Escáner de vulnerabilidad, video demostrativo**, Disponible en: <http://www.youtube.com/watch?v=3RgOtv4v8E>, [12/10/15]
- Herramientas para el reconocimiento de sistemas y escaneo de puertos (Netscantools)**, Disponible en: <http://www.nwpsw.com/>, [12/10/15]
- Identificación de riesgos y tipos de hackers**, Disponible en: <http://es.kioskea.net/contents/ataques/typologie-pirates.php3>, [12/10/15]
- Información técnica seguridad**, Disponible en: <http://www.textoscientificos.com/>, [12/10/15]
- Listas de seguridad, herramientas de seguridad y escaneo**, disponible en: <http://www.insecure.org/>, [12/10/15]
- Medidas de seguridad**, Disponible en: [http://www.windowsecurity.com/whitepapers/security\\_secure\\_internet\\_data\\_transmission.html](http://www.windowsecurity.com/whitepapers/security_secure_internet_data_transmission.html), [12/10/15]



**Metodología de intrusión de red**, Disponible en: <http://es.kioskea.net/contents/attaques/methodologie.php3>, [12/10/15]

**Parámetros de configuración de un dispositivo inalámbrico**, Disponible en: [http://www.usr.com/support/9108/9108-es-ug/wui\\_internet.htm](http://www.usr.com/support/9108/9108-es-ug/wui_internet.htm),  
[12/10/15]

**Recomendaciones de seguridad por Microsunsystems**, Disponible en: [http://www.sun.com/bigadmin/content/developer/howtos/generic\\_host.jsp](http://www.sun.com/bigadmin/content/developer/howtos/generic_host.jsp),  
[12/10/15]

**Security focus**, Disponible en: <http://www.securityfocus.com/>, [12/10/15]

**Squid, software usado como proxy en seguridad**, Disponible en: [http://www.deckle.co.za/squid-users-guide/Terminology\\_and\\_Technologies](http://www.deckle.co.za/squid-users-guide/Terminology_and_Technologies),  
[12/10/15]