Guía pedagógica y de evaluación 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

I. Guía pedagógica

1. Descripción

La Guía Pedagógica, es un documento que integra elementos técnico-metodológicos planteados de acuerdo con los principios y lineamientos del **Modelo Académico del CONALEP,** para orientar la práctica educativa del docente y el proceso de aprendizaje en el alumnado en el desarrollo de habilidades previstas en los programas de estudio.

Tomando en consideración el Marco Curricular Común de la Educación Media Superior (MCCEMS) el docente asume el rol de diseñador didáctico, innovador educativo, agente de transformación social, el cual se rige por principios orientadores, acompañando al estudiantado hacia una participación activa que potencialice su desarrollo; identificando los intereses y necesidades de aprendizaje que le lleven a resolver desafíos en su contexto, favoreciendo con ello el modelo de una escuela abierta, que atienda a la diversidad cultural, lingüística, de género, a la interacción entre grupos sociales, la coherencia entre los valores y objetivos de cada módulo.

Considerando al alumnado como protagonista para la transformación social, a través del desarrollo de un pensamiento crítico, analítico y flexible, se busca acercarle elementos de apoyo que le muestren cómo desarrollar **habilidades**, **conocimientos, actitudes y valores** en un contexto específico. Mediante la guía pedagógica el alumno podrá **autogestionar su aprendizaje** por medio del uso de estrategias flexibles y apropiadas que se puedan transferir y adoptar a nuevas situaciones y contextos, e ir dando seguimiento a sus avances a través de la autoevaluación, la coevaluación y la evaluación formativa.

2. Generalidades pedagógicas

Nuestro modelo académico se fundamenta en una base pedagógica centrada en la teoría constructivista con un enfoque humanista, que reconoce la diversidad local, regional, nacional e internacional; combinado con el nuevo MCCEMS permite mantener una didáctica que apuesta por el desarrollo de la voluntad de aprender y por la conexión entre el contenido teórico y la realidad.

Se pretende fomentar un aprendizaje, situado, profundo y significativo, que promueva la transversalidad mediante el desarrollo de estrategias de enseñanza basadas en proyectos integradores, que articulen los conocimientos con las unidades de aprendizaje y con los recursos socioemocionales, orientando a la formación integral del estudiantado.

El alumnado asume un rol protagónico en el proceso educativo, involucrándose en la resolución de problemas económicos, políticos, sociales y ambientales para contribuir a la construcción de un mundo más justo, pacífico y sostenible, bajo el acompañamiento, orientación y conducción del docente, quien, basándose en su experiencia, buscará combinar estrategias didácticas que incorporen materiales y recursos significativos para el aprendizaje del estudiante.

De acuerdo con lo anterior, se debe considerar que el papel que juega el alumnado y el personal docente en el marco del Modelo Académico del CONALEP tenga, entre otras, las siguientes características:

El alumnado:
❖ Gestiona su aprendizaje permanente. ❖ Mejora su capacidad para resolver problemas. ❖ Trabaja de forma colaborativa. ❖ Se comunica asertivamente. ❖ Busca información actualizada de fuentes confiables. ❖ Construye su conocimiento. ❖ Adopta una posición crítica, autónoma y propositiva. ❖ Realiza responsablemente los procesos de autoevaluación y coevaluación. ❖ Se vuelve agente de transformación social. ❖ Actúa con valores y principios éticos. ❖ Practica hábitos saludables para el autocuidado. ❖ Construye un pensamiento crítico, analítico y flexible.

El personal docente:
❖ Considera necesidades e intereses de los estudiantes que propicien la motivación y participación activa. ❖ Domina y estructura los saberes para facilitar experiencias de aprendizaje. ❖ Planifica los procesos de enseñanza dirigidos al logro de resultados de aprendizaje de manera efectiva, creativa e innovadora aplicado a su contexto. ❖ Evalúa los aprendizajes con un enfoque formativo, retroalimentando para la búsqueda de la mejora continua. ❖ Construye ambientes para el aprendizaje autónomo y colaborativo. ❖ Contribuye a la generación de un ambiente que facilite el desarrollo sano e integral de los estudiantes. ❖ Propone proyectos integradores en búsqueda de la transversalidad, para la solución de problemáticas contextuales, vinculadas a la comunidad generando el sentido de la experimentación pedagógica. ❖ Utiliza tecnologías de la información y comunicación, tecnologías de aprendizaje y conocimiento, tecnologías del empoderamiento y participación, como recursos didácticos. ❖ Agente de transformación social. ❖ Participa de forma colaborativa en el trabajo de academias.

3. Orientaciones didácticas

Para el logro del propósito de cada **unidad de aprendizaje** del módulo, se recomienda al personal docente lo siguiente:

- Identificar los componentes básicos de los resultados de aprendizaje para realizar la planeación didáctica, seleccionando actividades pertinentes y contextualizadas, considerando los elementos con los que se puede trabajar el contenido y que promuevan la reflexión, el diálogo y la discusión.
- Plantear el objetivo de cada actividad, asegurando su contextualización de acuerdo con las características de la comunidad, municipio, región y estados, y aplicando métodos y estrategias que favorezcan aprendizajes significativos.
- Abordar conocimientos previos a través de actividades diseñadas para explorar saberes e ideas precedentes, seleccionando aquellas que activen la atención del estudiantado y promuevan la participación.
- Retroalimentar las actividades y trabajos del estudiantado para orientar sobre sus avances y áreas de mejora, promoviendo la coevaluación, autoevaluación y heteroevaluación para favorecer una retroalimentación formativa y asertiva.
- Plantear actividades dirigidas al trabajo directo con la comunidad, como complemento a lo revisado en clase, y fomentar el aprendizaje práctico fuera del aula, incluyendo dinámicas con la comunidad y familiares.
- Aplicar la transversalidad buscando proyectos que se interrelacionen de forma horizontal y vertical basado en el mapa curricular.
- Promover la coevaluación, autoevaluación y heteroevaluación para favorecer la retroalimentación formativa y asertiva
- Crear o mantener un repositorio de información digital donde el estudiantado pueda consultar los materiales necesarios.
- Ajustes razonables: Realizar adaptaciones en las prácticas de instrucción y evaluación para estudiantes con necesidades especiales, eliminando barreras y permitiendo su plena participación.
- Ambiente educativo inclusivo: Fomentar un entorno educativo inclusivo y accesible para todos los estudiantes, asegurando la comunicación efectiva entre docentes, padres y especialistas para atender las necesidades específicas de cada estudiante.
- Promover la transparencia, honestidad y responsabilidad en las acciones cotidianas de los estudiantes, desarrollando su pensamiento crítico a través de debates y análisis éticos.
- Motivar a los estudiantes a participar activamente en la vida comunitaria, comprender sus derechos y deberes, y realizar proyectos que integren principios de derechos humanos y respeto mutuo.

- Igualdad: Mantener y promover una postura que fomente la inclusión y valoración de la diversidad, integrando información sobre igualdad y no discriminación Asegurar entornos educativos inclusivos y seguros, especialmente para mujeres, niñas, adolescentes y personas en situación de vulnerabilidad, impulsando la cultura de paz y respeto en toda la comunidad escolar
- Durante el desarrollo del módulo, se recomienda considerar la Didáctica de la Formación Socioemocional y los acuerdos del MCCEMS, a fin de Integrar en sus prácticas educativas los Recursos Socioemocionales y Ámbitos de la Formación socioemocional del currículum ampliado, enfatizando la formación de estudiantes responsables y comprometidos con su bienestar y el de su comunidad. Los acuerdos se pueden encontrar en las siguientes ligas:
    - Acuerdo número 09/05/24 que modifica el diverso número 09/08/23 por el que se establece y regula el Marco Curricular Común de la Educación Media Superior. https://sep.gob.mx/work/models/sep1/Resource/26394/1/images/a09_05_24.pdf
    - Acuerdo número 09/08/23 por el que se establece y regula el Marco Curricular Común de la Educación Media Superior. https://www.dof.gob.mx/nota_detalle.php?codigo=5699835&fecha=25/08/2023#gsc.tab=0
    - Anexo del Acuerdo número 09/08/23 por el que se establece y regula el Marco Curricular Común de la Educación Media Superior. https://www.dof.gob.mx/2023/SEP/ANEXO_ACUERDO_MCCEMS.pdf

4. Estrategias de aprendizaje

Para el desarrollo del resultado de aprendizaje 1.1, se recomienda al alumnado:

- Participar en una lluvia de ideas sobre medios de comunicación básica
- Elaborar un listado de los diferentes tipos de manejo de paquetería de cómputo
- Contestar la siguiente pregunta: ¿Cómo se lleva a cabo la operación y diagnóstico en el equipo de cómputo y redes locales?
- Participar activamente en un debate sobre las configuraciones de hardware, software y comunicaciones asociadas con él, identificando riesgos y amenazas describiendo sus causas y efectos.
- Elaborar un organizador gráfico sobre los riesgos de hardware y software, las causas y efectos

ANÁLISIS DE RIESGOS			
	RIESGO	**CAUSAS**	**EFECTOS**
HARDWARE			
SOFTWARE			

- Presentar en plenaria las normas que rigen el desarrollo de sistemas de información.
- Utilizar las herramientas y comandos de monitoreo en el tráfico de red hacia el equipo, en particular en el enlace ADSL, por la conexión y riesgo permanente que existe. Aplica las herramientas de Microsoft en la identificación de riesgos y amenazas.
- Participar en una discusión para evaluar las actividades que se realizan en el equipo y en los sistemas de información que representan una amenaza al software y a la integridad de información en caso de no controlarse y adoptar las medidas adecuadas.
- **Realizar la actividad de evaluación 1.1.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 1.2, se recomienda al alumnado:

- Describir ejemplos de identificación de amenazas de agentes externos, desde conductos de intrusión hasta suplantación de identidad, y discutir con el grupo.

- Realizar actividades de identificación de debilidades en la instalación y las comunicaciones, iniciando con los protocolos innecesarios en la instalación y la omisión o usos inadecuados de WEP/WAP.
- Monitorear y describir los efectos en la integridad de la información que provoca, el no ser atendido.
- **Realizar la actividad de evaluación 1.2.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 2.1, se recomienda al alumnado:

- Concluir el plan contra agentes externos o internos, que intentan violar la integridad de la operación del equipo y de la información, con una investigación vía internet, y lo enriquece con consultas sobre recomendaciones técnicas de especialistas en seguridad.
- Generar ideas sobre cómo enfrentar las debilidades que pueden existir en el desarrollo de aplicaciones de internet, integrándolas en un documento de políticas de seguridad.
- **Realizar la actividad de evaluación 2.1.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 2.2, se recomienda al alumnado:

- Elaborar un tríptico en el que se describen las herramientas de seguridad en redes de computadoras y su instalación.
- Realizar una investigación en fuentes de información sugeridas sobre la instalación de herramientas de seguridad en redes VPN y Windows.
- Demostrar el dominio de la instalación de alguna de las herramientas investigadas.
- Elaborar un reporte del procedimiento de aplicación de herramientas de seguridad desde la instalación de protocolo WEP, hasta separar la red inalámbrica de la red local interna y los resultados obtenidos.
- Instalar por equipos la tecnología de seguridad en los servicios de internet.
- Elaborar una propuesta de políticas de seguridad relacionadas con el acceso a los sistemas, operación del equipo, desarrollo de programas, configuración de redes y la aplicación de la Norma ISO 14000, así como el plan de comunicación hacia la organización.
- Realizar la presentación de su propuesta, para recibir retroalimentación del docente e integrantes del grupo y complementarla.
- **Realizar la actividad de evaluación 2.2.1 considerando la rúbrica correspondiente**

5. Autonomía didáctica

De acuerdo con el MCCEMS, las y los docentes tienen la facultad de decidir estrategias pedagógicas basadas en el contexto y las necesidades del estudiantado, utilizando el PAEC, las progresiones de aprendizaje, resultados de aprendizaje o competencias laborales, para planificar y retroalimentar los procesos de enseñanza. La flexibilidad permite adaptar estos programas a la diversidad de contextos educativos y características tanto del estudiantado como del personal docente.

Con ello, se reconoce que la función del personal docente implica, ante todo, una labor de investigación y promoción del autoaprendizaje; fomentando actividades que consideren el aprendizaje contextualizado, colaborativo, participativo y lúdico, así como el diálogo, el trabajo en equipo y la utilización pertinente, sostenible y responsable de las tecnologías de la información, comunicación, conocimiento y aprendizaje digital (TICCAD), en los procesos de la vida cotidiana con una perspectiva crítica de los contenidos y materiales disponibles en medios electrónicos, plataformas virtuales y redes sociales.

En este sentido, el personal docente seleccionará y realizará prácticas y actividades transversales que garanticen un mayor desarrollo de aprendizajes y habilidades, basadas en su experiencia, el contexto del grupo, la comunidad y el desempeño del estudiantado, priorizando las corrientes pedagógicas actuales y las tecnologías de información y comunicación (TIC), las tecnologías del aprendizaje y conocimiento (TAC) y las tecnologías del empoderamiento y la participación (TEP) como herramientas de apoyo al proceso de enseñanza – aprendizaje. De igual manera, se espera que el estudiantado asuma su responsabilidad y tome un papel activo en el proceso de desarrollo de habilidades, conocimientos, actitudes y valores que le permitirán ingresar al mundo laboral y participar de manera destacada en la sociedad.

II. Guía de evaluación

6. Descripción

La guía de evaluación es un documento que define el proceso de recolección y valoración de las evidencias requeridas por el módulo desarrollado y tiene el propósito de orientar en la evaluación de las habilidades, conocimientos y actitudes adquiridos por el estudiantado, asociados a los Resultados de Aprendizaje; en donde, además, se describen las técnicas y los instrumentos a utilizar, así como la ponderación de cada actividad de evaluación.

Durante el proceso de enseñanza - aprendizaje es importante considerar tres finalidades de evaluación: diagnóstica, formativa y sumativa.

La **evaluación diagnóstica** nos permite establecer un punto de partida fundamentado en la detección de la situación en la que se encuentran nuestros estudiantes. Permite también establecer vínculos socio-afectivos entre el docente y su grupo. El estudiantado a su vez podrá obtener información sobre los aspectos donde deberá hacer énfasis en su dedicación. El docente podrá identificar intereses, necesidades y características del grupo para orientar adecuadamente sus estrategias. En esta etapa pueden utilizarse mecanismos informales de recopilación de información.

La **evaluación formativa** se realiza durante todo el proceso de aprendizaje del estudiantado, de manera constante, ya sea al finalizar cada actividad de aprendizaje o en la integración de varias de éstas. Tiene como finalidad informar al estudiantado de sus avances con respecto a los aprendizajes que deben alcanzar y advertirle sobre dónde y en qué aspectos tiene debilidades o dificultades para poder regular sus procesos. Aquí se admiten errores, se identifican y se corrigen; es factible trabajar colaborativamente. Asimismo, el personal docente puede asumir nuevas estrategias que contribuyan a mejorar los resultados del grupo, entendiendo que la evaluación es un proceso que construye para retroalimentar y tomar decisiones orientadas a la mejora continua, en distintos rubros.

Finalmente, la **evaluación sumativa** es adoptada básicamente por una función social, ya que mediante ella se asume una acreditación, una promoción, un fracaso escolar, índices de deserción, etc., a través de criterios estandarizados y claramente definidos. Las evidencias se elaboran en forma individual, puesto que se está asignando, convencionalmente, un criterio o valor. Manifiesta la síntesis de los logros obtenidos por ciclo o período escolar.

Con respecto al agente o responsable de llevar a cabo la evaluación, se distinguen tres categorías: la **autoevaluación** que se refiere a la valoración que hace el alumno sobre su propia actuación, lo que le permite reconocer sus posibilidades, limitaciones y cambios necesarios para mejorar su aprendizaje. Los roles de evaluador y evaluado coinciden en la misma persona.

La **coevaluación** es aquella en la que las y los alumnos se evalúan mutuamente, es decir, evaluadores y evaluados intercambian su papel alternativamente; las y los alumnos en conjunto, participan en la valoración de los aprendizajes logrados, ya sea por algunos de sus miembros o del grupo en su conjunto; la coevaluación permite al alumnado y al profesorado:

- Identificar los logros personales y grupales
- Fomentar la participación, reflexión y crítica constructiva ante situaciones de aprendizaje
- Opinar sobre su actuación dentro del grupo
- Desarrollar actitudes que promuevan la integración del grupo
- Mejorar su responsabilidad e identificación con el trabajo
- Emitir juicios valorativos acerca de otros en un ambiente de libertad, compromiso y responsabilidad

La **heteroevaluación** es el tipo de evaluación que con mayor frecuencia se utiliza, donde el docente es quien evalúa, su variante externa, se da cuando agentes no integrantes del proceso enseñanza-aprendizaje son los evaluadores, otorgando cierta objetividad por su no implicación.

En dos rúbricas diferentes de la guía de evaluación se establece un indicador específico para la autoevaluación y coevaluación; a su vez, la heteroevaluación queda establecida en una rúbrica que podría ser evaluada por un experto o docente que no haya impartido el módulo a ese grupo.

Cada uno de los Resultados de Aprendizaje (RA) tiene asignada al menos una actividad de evaluación (AE), a la que se le ha determinado una ponderación con respecto a su complejidad y relevancia. Las ponderaciones de las AE deberán sumar 100%.

7. Tabla de ponderación

La ponderación que se asigna en cada una de las actividades de evaluación se representa en la Tabla de ponderación que, además, contiene los Resultados y Unidades de aprendizaje a las cuales pertenecen. La columna “Actividad de evaluación” indica la codificación asignada a ésta desde el programa de estudios y que a su vez queda vinculada al Sistema de Evaluación Escolar (SAE). Asimismo, la columna “Peso específico”, señala el porcentaje definido para cada actividad; la columna “Peso logrado” es el nivel que la o el alumno alcanzó con base en las evidencias o desempeños demostrados; y la columna “Peso acumulado” se refiere a la suma de los porcentajes alcanzados en las diversas actividades de evaluación a lo largo del ciclo escolar.

Unidad de aprendizaje	Resultado de Aprendizaje	Actividad de Evaluación	% Peso Específico	% Peso Logrado	% Peso Acumulado
1. Diagnóstico de riesgos y amenazas en la seguridad del equipo.	**1.1** Identifica riesgos y amenazas en la seguridad del hardware y software con base en las advertencias que emite el equipo.	**1.1.1**	**20%**		
	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.	**1.2.1**	**25%**		
% PESO PARA LA UNIDAD			**45 %**		
2. Implementación de tecnología de seguridad en hardware y software del equipo de cómputo.	**2.1** Establece recomendaciones de tecnología de seguridad en hardware y software orientada a la protección y preservación de la integridad de la información.	**2.1.1**	**25%**		
	2.2 Implementa tecnología de seguridad protegiendo la integridad de la información y el equipo de cómputo contra amenazas.	**2.2.1**	**30%**		
% PESO PARA LA UNIDAD			**55%**		
PESO TOTAL DEL MÓDULO			**100%**		

8. Matriz de valoración o rúbrica

Otro elemento que complementa a la Tabla de ponderación es la rúbrica o matriz de valoración, que establece los indicadores y criterios a considerar para evaluar una habilidad, destreza o actitud. Una matriz de valoración o rúbrica es, como su nombre lo indica, una matriz de doble entrada en la cual se establecen, por un lado, los indicadores o aspectos específicos que se deben tomar en cuenta como mínimo indispensable para evaluar si se ha logrado el resultado de aprendizaje esperado y, por otro, los criterios o niveles de calidad o satisfacción alcanzados. En las columnas centrales se describen los criterios que se van a utilizar para evaluar esos indicadores, explicando cuáles son las características de cada uno. Los criterios que se han establecido son:

- ✓ **Excelente**, ha alcanzado el resultado de aprendizaje, además de cumplir con los estándares o requisitos establecidos como necesarios en el logro de la habilidad, destreza o actitud, es decir, va más allá de lo que se solicita como mínimo, aportando elementos adicionales en pro del indicador.
- ✓ **Bueno,** ha alcanzado el resultado de aprendizaje, es decir, cumple con los estándares o requisitos establecidos como necesarios para demostrar el logro de la habilidad, destreza o actitud.
- ✓ **Suficiente,** ha alcanzado el resultado de aprendizaje con áreas de mejora.
- ✓ **Insuficiente**, no ha logrado alcanzar el resultado de aprendizaje.

Siglema:	**AHSH-20**	**Nombre del módulo:**	**Aplicación de herramientas de seguridad en hardware y software.**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
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.			**Actividad de evaluación:**	**1.1.1** Elabora un reporte de resultados identificando riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Riesgos en el hardware y software	**35**	Utiliza comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware. Elabora un reporte en el que describe: sitios dudosos accesados, servicios habilitados, archivos de dudosa procedencia, Applets que se han ejecutado en el equipo, estado de seguridad. Identifica sitios de identidad desconocida, que pueden atentar contra la seguridad del equipo, y determina si son potencialmente una amenaza a la seguridad del equipo. Responde en forma inmediata para manejar situaciones imprevistas, durante la identificación de riesgos en el equipo.	Utiliza comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware. Elabora un reporte en el que describe: sitios dudosos accesados, servicios habilitados, archivos de dudosa procedencia, Applets que se han ejecutado en el equipo, estado de seguridad. Identifica sitios de identidad desconocida, que pueden atentar contra la seguridad del equipo, y determina si son potencialmente una amenaza a la seguridad del equipo.	Omite alguna de las siguientes actividades: Utilizar comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware. Elaborar un reporte en el que describe**:** sitios dudosos accesados, servicios habilitados, archivos de dudosa procedencia, *Applets* que se han ejecutado en el equipo, estado de seguridad. Identificar sitios de identidad desconocida, que pueden atentar contra la seguridad del equipo, y determinar si son potencialmente una amenaza a la seguridad del equipo.	Omite dos o más de las siguientes actividades: Utilizar comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware. Elaborar un reporte en el que describe**:** sitios dudosos accesados, servicios habilitados, archivos de dudosa procedencia, *Applets* que se han ejecutado en el equipo, estado de seguridad. Identificar sitios de identidad desconocida, que pueden atentar contra la seguridad del equipo, y determinar si son potencialmente una amenaza a la seguridad del equipo.
Amenazas en hardware y software	**40**	Utiliza las herramientas de MSAT (evaluación de seguridad de Microsoft). Utiliza las herramientas de IIS (herramienta de bloqueo).	Utiliza las herramientas de MSAT (evaluación de seguridad de Microsoft). Utiliza las herramientas de IIS (herramienta de bloqueo).	Omite alguna de las siguientes actividades: • Utilizar las herramientas de MSAT (evaluación de seguridad de Microsoft).	Omite tres o más de las siguientes actividades: • Utilizar las herramientas de MSAT (evaluación de seguridad de Microsoft).

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		Utiliza las herramientas del reporteador de puertos (portreporter). Utiliza las herramientas del muestreo de seguridad de la red (networksecurityscan). Reporta resultados obtenidos con el uso de las herramientas. Realiza la interpretación de los resultados. Acepta las observaciones y sugerencias brindadas por el docente y por sus compañeros para mejorar su trabajo.	Utiliza las herramientas del reporteador de puertos (portreporter). Utiliza las herramientas del muestreo de seguridad de la red (networksecurityscan). Reporta resultados obtenidos con el uso de las herramientas. Realiza la interpretación de los resultados.	• Utilizar las herramientas de IIS (herramienta de bloqueo). • Utilizar las herramientas del reporteador de puertos (portreporter). • Utilizar las herramientas del muestreo de seguridad de la red (networksecurityscan) • Reportar resultados obtenidos con el uso de las herramientas. • Realizar la interpretación de los resultados.	• Utilizar las herramientas de IIS (herramienta de bloqueo). • Utilizar las herramientas del reporteador de puertos (portreporter). • Utilizar las herramientas del muestreo de seguridad de la red (networksecurityscan) • Reportar resultados obtenidos con el uso de las herramientas. • Realizar la interpretación de los resultados.
Reporte **COEVALUACIÓN**	**15**	La información es precisa y se presenta con rigor académico. Todo el contenido es relevante y está bien explicado. El análisis es profundo y muestra una comprensión completa del tema.	La información es mayormente precisa y se presenta con cierto rigor académico. La mayoría del contenido es relevante y está bien explicado. El análisis es bueno y muestra una comprensión adecuada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Parte del contenido es relevante y está explicado. El análisis es superficial y muestra una comprensión limitada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Poco contenido es relevante o está explicado. El análisis es muy superficial y muestra una comprensión muy limitada del tema.
Desempeño	**10**	El alumno muestra interés durante la elaboración del trabajo solicitado, presenta los ejercicios, actividades y tareas en tiempo solicitado. Siempre de forma correcta	Presenta los ejercicios, actividades y tareas en tiempo, en la mayoría de las ocasiones realizado de forma correcta.	Suele presentar los ejercicios, actividades y tareas en tiempo y forma. Entre un 50% y 60% de las ocasiones de forma correcta.	Omite presentar los ejercicios, actividades y tareas en tiempo y forma. Casi siempre lo hace de forma incorrecta.
	100				

Siglema:	**AHSH-20**	**Nombre del módulo:**	**Aplicación de herramientas de seguridad en hardware y software.**	**Nombre del alumno:**	
Docente evaluador:				**Grupo:**	**Fecha:**
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.			**Actividad de evaluación:**	**1.2.1** Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación.

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Amenazas a la información	**35**	Identifica y diagnostica formas en que estos agentes externos atentan contra la integridad de la información: hackers, crakers, sniffers, phreakers, spammers, piratas informáticos, creadores de virus, personal interno e intrusos remunerados. Aplica la utilería igremote, explica su objetivo e interpreta los resultados en: virus, troyanos, rootkits gusanos, spyware, malware, espionaje, modificación de información, spam y suplantación de identidad. Busca en internet programas de intrusión, identifica y describe lo que pueden hacer. Utiliza las tecnologías de la información para procesar e interpretar información en el diagnóstico de este tipo de amenazas.	Identifica y diagnostica formas en que estos agentes externos atentan contra la integridad de la información: hackers, crakers, sniffers, phreakers, spammers, piratas informáticos, creadores de virus, personal interno e intrusos remunerados. Aplica la utilería igremote, explica su objetivo e interpreta los resultados en: virus, troyanos, rootkits gusanos, spyware, malware, espionaje, modificación de información, spam y suplantación de identidad. Busca en internet programas de intrusión, identifica y describe lo que pueden hacer.	Omite alguna de las siguientes actividades: Identificar y diagnosticar formas en que estos agentes externos atentan contra la integridad de la información: hackers, crakers, sniffers, phreakers, spammers, piratas informáticos, creadores de virus, personal interno e intrusos remunerados. Aplicar la utilería igremote, explicar su objetivo e interpretar los resultados en: virus, troyanos, rootkits gusanos, spyware, malware, espionaje, modificación de información, spam y suplantación de identidad. Buscar en internet programas de intrusión, identificar y describir lo que pueden hacer.	Excluye dos o más de las siguientes actividades. Identificar y diagnosticar formas en que estos agentes externos atentan contra la integridad de la información: hackers, crakers, sniffers, phreakers, spammers, piratas informáticos, creadores de virus, personal interno e intrusos remunerados. Aplicar la utilería igremote, explicar su objetivo e interpretar los resultados en: virus, troyanos, rootkits gusanos, spyware, malware, espionaje, modificación de información, spam y suplantación de identidad. Buscar en internet programas de intrusión, identificar y describir lo que pueden hacer.
Riesgos originados por las debilidades de instalación	**45**	Diagnostica y describe los riesgos originados por debilidades de instalación de protocolos de red no necesarios.	Diagnostica y describe los riesgos originados por debilidades de instalación de	Omite alguna de las siguientes actividades: Diagnosticar y describir los riesgos originados por	Omite tres de las siguientes actividades: Diagnosticar y describir los riesgos originados por

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
		Diagnostica y describe los riesgos originados por debilidades de instalación o actualización de la versión del BIOS. Diagnostica y describe los riesgos originados por debilidades de instalación de servicios compartidos. Diagnostica y describe los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados. Es responsable con su trabajo y realiza sus labores con exactitud y precaución al diagnosticar riesgos originados por las debilidades de instalación.	protocolos de red no necesarios. Diagnostica y describe los riesgos originados por debilidades de instalación o actualización de la versión del BIOS. Diagnostica y describe los riesgos originados por debilidades de instalación de servicios compartidos. Diagnostica y describe los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados.	debilidades de instalación de protocolos de red no necesarios. Diagnosticar y describir los riesgos originados por debilidades de instalación o actualización de la versión del BIOS. Diagnosticar y describir los riesgos originados por debilidades de instalación de servicios compartidos. Diagnosticar y describir los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados.	debilidades de instalación de protocolos de red no necesarios. Diagnosticar y describir los riesgos originados por debilidades de instalación o actualización de la versión del BIOS. Diagnosticar y describir los riesgos originados por debilidades de instalación de servicios compartidos. Diagnosticar y describir los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados.
Diagnóstico	**10**	La información es precisa y se presenta con rigor académico. Todo el contenido es relevante y está bien explicado. El análisis es profundo y muestra una comprensión completa del tema.	La información es mayormente precisa y se presenta con cierto rigor académico. La mayoría del contenido es relevante y está bien explicado. El análisis es bueno y muestra una comprensión adecuada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Parte del contenido es relevante y está explicado. El análisis es superficial y muestra una comprensión limitada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Poco contenido es relevante o está explicado. El análisis es muy superficial y muestra una comprensión muy limitada del tema.
Desempeño	**10**	El alumno muestra interés durante la elaboración del trabajo solicitado, presenta los ejercicios, actividades y tareas en tiempo solicitado. Siempre de forma correcta	Presenta los ejercicios, actividades y tareas en tiempo, en la mayoría de las ocasiones realizado de forma correcta.	Suele presentar los ejercicios, actividades y tareas en tiempo y forma. Entre un 50% y 60% de las ocasiones de forma correcta.	Omite presentar los ejercicios, actividades y tareas en tiempo y forma. Casi siempre lo hace de forma incorrecta.
	100				

Siglema:	**AHSH-20**	**Nombre del módulo:**	**Aplicación de herramientas de seguridad en hardware y software.**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
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.			**Actividad de evaluación:**	**2.1.1** Establece recomendaciones de seguridad identificando sus efectos a través de un reporte de resultados		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Recomendaciones contra vulnerabilidades	**40**	Recomienda medidas de protección y preservación de la información. Autoriza y registra usuarios. Controla el acceso a usuarios locales y remotos. Establece certificados digitales y servidores de autentificación. Administra contraseñas y reconocimiento de firmas manuscritas y huellas dactilares. Describe los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya. Se muestra seguro y convincente al hacer alguna recomendación contra las posibles vulnerabilidades a sus compañeros y el docente.	Recomienda medidas de protección y preservación de la información. Autoriza y registra usuarios. Controla el acceso a usuarios locales y remotos. Establece certificados digitales y servidores de autentificación. Administra contraseñas y reconocimiento de firmas manuscritas y huellas dactilares. Describe los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya.	Omite alguna de las siguientes actividades: Recomendar medidas de protección y preservación de la información. Autorizar y registrar usuarios. Controlar el acceso a usuarios locales y remotos. Establecer certificados digitales y servidores de autentificación. Administrar contraseñas y reconocimiento de firmas manuscritas y huellas dactilares. Describir los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya.	Omite tres o más de las siguientes actividades: Recomendar medidas de protección y preservación de la información. Autorizar y registrar usuarios. Controlar el acceso a usuarios locales y remotos. Establecer certificados digitales y servidores de autentificación. Administrar contraseñas y reconocimiento de firmas manuscritas y huellas dactilares. Describir los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya.
Definición de acciones de seguridad	**40**	Propone políticas de seguridad describiendo su validez y efectos. Establece protocolos por denegación de servicio o	Propone políticas de seguridad describiendo su validez y efectos. Establece protocolos por denegación de servicio o	Omite alguna de las siguientes actividades: Proponer políticas de seguridad describiendo su validez y efectos.	Omite tres o más de las siguientes actividades: Proponer políticas de seguridad describiendo su validez y efectos.

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
		modificación al contenido de mensajes. Define criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores. Previene ataques que realicen una llamada al sistema operativo. Previene ataques que traten de accesar a carpetas dentro del servidor web Previene ataques que exploten la identificación de URL Elabora el plan de acción como reporte. Recomienda reglas, procedimientos y actitudes relativas a la protección de la información.	modificación al contenido de mensajes. Define criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores. Previene ataques que realicen una llamada al sistema operativo. Previene ataques que traten de accesar a carpetas dentro del servidor web Previene ataques que exploten la identificación de URL Elabora el plan de acción como reporte.	Establecer protocolos por denegación de servicio o modificación al contenido de mensajes. Definir criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores. Prevenir ataques que realicen una llamada al sistema operativo. Prevenir ataques que traten de accesar a carpetas dentro del servidor web Prevenir ataques que exploten la identificación de URL. Elaborar el plan de acción como reporte.	Establecer protocolos por denegación de servicio o modificación al contenido de mensajes. Definir criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores. Prevenir ataques que realicen una llamada al sistema operativo. Prevenir ataques que traten de accesar a carpetas dentro del servidor web Prevenir ataques que exploten la identificación de URL. Elaborar el plan de acción como reporte.
Reporte **AUTOEVALUACIÓN**	**10**	La información es precisa y se presenta con rigor académico. Todo el contenido es relevante y está bien explicado. El análisis es profundo y muestra una comprensión completa del tema.	La información es mayormente precisa y se presenta con cierto rigor académico. La mayoría del contenido es relevante y está bien explicado. El análisis es bueno y muestra una comprensión adecuada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Parte del contenido es relevante y está explicado. El análisis es superficial y muestra una comprensión limitada del tema.	La información es algo precisa y se presenta con algo de rigor académico. Poco contenido es relevante o está explicado. El análisis es muy superficial y muestra una comprensión muy limitada del tema.
Desempeño	**10**	El alumno muestra interés durante la elaboración del trabajo solicitado, presenta los ejercicios, actividades y tareas en tiempo solicitado. Siempre de forma correcta	Presenta los ejercicios, actividades y tareas en tiempo, en la mayoría de las ocasiones realizado de forma correcta.	Suele presentar los ejercicios, actividades y tareas en tiempo y forma. Entre un 50% y 60% de las ocasiones de forma correcta.	Omite presentar los ejercicios, actividades y tareas en tiempo y forma. Casi siempre lo hace de forma incorrecta.
	100				

Siglema:	**AHSH-20**	**Nombre del módulo:**	**Aplicación de herramientas de seguridad en hardware y software.**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**2.2** Implementa tecnología de seguridad protegiendo la información y equipo de cómputo contra amenazas a su integridad.			**Actividad de evaluación:**	**2.2.1** Instala y configura tecnología de seguridad reportando su efecto en la integridad de la información. **HETEROEVALUACIÓN**		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Herramientas de seguridad en redes.	**25**	Instala, ejecuta y describe la forma de implantar acciones en la instalación de tecnología de seguridad en redes. Considera restricciones a los dispositivos ADSL (hardening). Instala herramientas de seguridad en redes VPN y Windows. Identifica la acción más sólida en la seguridad de redes. Pregunta cuando tiene dudas para instalar las herramientas de seguridad y consulta la posibilidad de poner en práctica sus ideas o sugerencias.	Instala, ejecuta y describe la forma de implantar acciones en la instalación de tecnología de seguridad en redes. Considera restricciones a los dispositivos ADSL (hardening). Instala herramientas de seguridad en redes VPN y Windows. Identifica la acción más sólida en la seguridad de redes.	Omite alguna de las siguientes actividades: Instalar, ejecutar y describir la forma de implantar acciones en la instalación de tecnología de seguridad en redes. Considerar restricciones a los dispositivos ADSL (hardening). Instalar herramientas de seguridad en redes VPN y Windows. Identificar la acción más sólida en la seguridad de redes.	Omite dos o más de las siguientes actividades: Instalar, ejecutar y describir la forma de implantar acciones en la instalación de tecnología de seguridad en redes. Considerar restricciones a los dispositivos ADSL (hardening). Instalar herramientas de seguridad en redes VPN y Windows. Identificar la acción más sólida en la seguridad de redes.
Componentes físicos de oficina.	**30**	Considera en la instalación de tecnología de seguridad en componentes físicos de oficinas: □ Protocolo WEP □ Protocolo WPA □ Estándar RSN □ Estándar 802.1x Detecta intentos de intrusión.	Considera en la instalación de tecnología de seguridad en componentes físicos de oficinas: □ Protocolo WEP □ Protocolo WPA □ Estándar RSN □ Estándar 802.1x	Omite alguna de las siguientes actividades: Considerar en la instalación de tecnología de seguridad en componentes físicos de oficinas: Protocolos WEP y WPA y los estándares RSN y 802.1x. Detectar intentos de intrusión.	Omite dos de las siguientes actividades: Considerar en la instalación de tecnología de seguridad en componentes físicos de oficinas: Protocolos WEP y WPA y los estándares RSN y 802.1x. Detectar intentos de intrusión.

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		Separa la red inalámbrica de la red local interna. Detecta problemas o errores cometidos durante la instalación de tecnologías de seguridad para oficinas, analiza las causas que los originaron y plantea las posibles soluciones para evitar repetirlas.	Detecta intentos de intrusión. Separa la red inalámbrica de la red local interna.	Separar la red inalámbrica de la red local interna.	Separar la red inalámbrica de la red local interna.
Acciones de seguridad para acceso a servicios de internet	**35**	Ejecuta, describe y reporta la implantación de acciones de seguridad. Actualiza parches de seguridad y control de cookies. Realiza el control en la descarga desde internet. Evade sitios dudosos. Evalúa enlaces incluidos en correo electrónico. Reporta la complejidad de la implantación de cada medida de seguridad, ordenándolas jerárquicamente, de mayor a menor, así como su relación con el beneficio a la seguridad para acceso a servicios de internet que aporta.	Ejecuta, describe y reporta la implantación de acciones de seguridad. Actualiza parches de seguridad y control de cookies. Realiza el control en la descarga desde internet. Evade sitios dudosos. Evalúa enlaces incluidos en correo electrónico.	Omite alguna de las siguientes actividades: • Ejecutar, describir y reportar la implantación de acciones de seguridad. • Actualizar parches de seguridad y control de cookies. • Realizar el control en la descarga desde internet. • Evadir sitios dudosos. • Evaluar enlaces incluidos en correo electrónico.	Omite tres de las siguientes actividades: • Ejecutar, describir y reportar la implantación de acciones de seguridad. • Actualizar parches de seguridad y control de cookies. • Realizar el control en la descarga desde internet. • Evadir sitios dudosos. • Evaluar enlaces incluidos en correo electrónico.
Desempeño	**10**	El alumno muestra interés durante la elaboración del trabajo solicitado, presenta los ejercicios, actividades y tareas en tiempo solicitado. Siempre de forma correcta	Presenta los ejercicios, actividades y tareas en tiempo, en la mayoría de las ocasiones realizado de forma correcta.	Suele presentar los ejercicios, actividades y tareas en tiempo y forma. Entre un 50% y 60% de las ocasiones de forma correcta.	Omite presentar los ejercicios, actividades y tareas en tiempo y forma. Casi siempre lo hace de forma incorrecta.
	100				