# I. Guía pedagógica del módulo
# Aplicación de herramientas de seguridad en hardware y software

# Contenido

## 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 en el desarrollo de competencias previstas en los programas de estudio.

La finalidad que tiene esta guía es facilitar el aprendizaje de los alumnos, encauzar sus acciones y reflexiones y proporcionar situaciones en las que desarrollará las competencias. El docente debe asumir conscientemente un rol que facilite el proceso de aprendizaje, proponiendo y cuidando un encuadre que favorezca un ambiente seguro en el que los alumnos puedan aprender, tomar riesgos, equivocarse extrayendo de sus errores lecciones significativas, apoyarse mutuamente, establecer relaciones positivas y de confianza, crear relaciones significativas con adultos a quienes respetan no por su estatus como tal, sino como personas cuyo ejemplo, cercanía y apoyo emocional es valioso.

Es necesario destacar que el desarrollo de la competencia se concreta en el aula, ya que formar con un enfoque en competencias significa crear experiencias de aprendizaje para que los alumnos adquieran la capacidad de movilizar, de forma integral, recursos que se consideran indispensables para saber resolver problemas en diversas situaciones o contextos, e involucran las dimensiones cognitiva, afectiva y psicomotora; por ello, los programas de estudio, describen las competencias a desarrollar, entendiéndolas como la combinación integrada de conocimientos, habilidades, actitudes y valores que permiten el logro de un desempeño eficiente, autónomo, flexible y responsable del individuo en situaciones específicas y en un contexto dado. En consecuencia, la competencia implica la comprensión y transferencia de los conocimientos a situaciones de la vida real; ello exige relacionar, integrar, interpretar, inventar, aplicar y transferir los saberes a la resolución de problemas. Esto significa que el contenido, los medios de enseñanza, las estrategias de aprendizaje, las formas de organización de la clase y la evaluación se estructuran en función de la competencia a formar; es decir, el énfasis en la proyección curricular está en lo que los alumnos tienen que aprender, en las formas en cómo lo hacen y en su aplicación a situaciones de la vida cotidiana y profesional.

Considerando que el alumno está en el centro del proceso formativo, se busca acercarle elementos de apoyo que le muestren qué competencias va a desarrollar, cómo hacerlo y la forma en que se le evaluará. Es decir, mediante la guía pedagógica el alumno podrá autogestionar su aprendizaje a través del uso de estrategias flexibles y apropiadas que se transfieran y adopten a nuevas situaciones y contextos e ir dando seguimiento a sus avances a través de una autoevaluación constante, como base para mejorar en el logro y desarrollo de las competencias indispensables para un crecimiento académico y personal.

## 2. Datos de identificación de la norma

| | | | |
|---|---|---|---|
| **Título:** | | | |
| **Unidad (es) de Norma Técnica de Competencia Laboral:** | | | |
| | | | |
| **Código:** | | **Nivel de competencia:** | |
| | | | |

## 3. Generalidades pedagógicas

Con el propósito de difundir los criterios a considerar en la instrumentación de la presente guía entre los docentes y personal académico de planteles y Colegios Estatales, se describen **algunas consideraciones** respecto al desarrollo e intención de las competencias expresadas en los módulos correspondientes a la formación básica, propedéutica y profesional.

Los principios asociados a la **concepción constructivista** del aprendizaje mantienen una estrecha relación con los de la **educación basada encompetencias**, la cual se ha concebido en el Colegio como el enfoque idóneo para orientar la formación ocupacional de los futuros profesionales técnicos y profesionales técnicos bachiller. Este enfoque constituye una de las opciones más viables para lograr la vinculación entre la educación y el sector productivo de bienes y servicios.
En los programas de estudio se proponen una serie de contenidos que se considera conveniente abordar para obtener los **Resultados de Aprendizaje establecidos**; sin embargo, se busca que este planteamiento le dé al docente la posibilidad de **desarrollarlos con mayor libertad y creatividad**.

En este sentido, se debe considerar que el papel que juegan el alumno y el docente en el marco del Modelo Académico del CONALEP tenga, entre otras, las siguientes características:

| El alumno: | El docente: |
|---|---|
| ❖ Mejora su capacidad para resolver problemas.<br>❖ Aprende a trabajar en grupo y comunica sus ideas.<br>❖ Aprende a buscar información y a procesarla.<br>❖ Construye su conocimiento.<br>❖ Adopta una posición crítica y autónoma.<br>❖ Realiza los procesos de autoevaluación y coevaluación. | ❖ Organiza su formación continua a lo largo de su trayectoria profesional.<br>❖ Domina y estructura los saberes para facilitar experiencias de aprendizaje significativo.<br>❖ Planifica los procesos de enseñanza y de aprendizaje atendiendo al enfoque por competencias, y los ubica en contextos disciplinares, curriculares y sociales amplios.<br>❖ Lleva a la práctica procesos de enseñanza y de aprendizaje de manera efectiva, creativa e innovadora a su contexto institucional.<br>❖ Evalúa los procesos de enseñanza y de aprendizaje con un enfoque formativo.<br>❖ Construye ambientes para el aprendizaje autónomo y colaborativo.<br>❖ Contribuye a la generación de un ambiente que facilite el desarrollo sano e integral de los estudiantes.<br>❖ Participa en los proyectos de mejora continua de su escuela y apoya la gestión institucional. |

En esta etapa se requiere una mejor y mayor organización académica que apoye en forma relativa la actividad del alumno, que en este caso es mucho mayor que la del docente; lo que no quiere decir que su labor sea menos importante. **El docente en lugar de transmitir vertical y unidireccionalmente los conocimientos, es un mediador del aprendizaje**, ya que:

- Planea y diseña experiencias y actividades necesarias para la adquisición de las competencias previstas. Asimismo, define los ambientes de aprendizaje, espacios y recursos adecuados para su logro.
- Proporciona oportunidades de aprendizaje a los alumnos apoyándose en metodologías y estrategias didácticas pertinentes a los Resultados de Aprendizaje.
- Ayuda también al alumno a asumir un rol más comprometido con su propio proceso, invitándole a tomar decisiones.
- Facilita el aprender a pensar, fomentando un nivel más profundo de conocimiento.
- Ayuda en la creación y desarrollo de grupos colaborativos entre los alumnos.
- Guía permanentemente a los alumnos.
- Motiva al alumno a poner en práctica sus ideas, animándole en sus exploraciones y proyectos.

Considerando la importancia de que el docente planee y despliegue con libertad su experiencia y creatividad para el desarrollo de las competencias consideradas en los programas de estudio y especificadas en los Resultados de Aprendizaje, en las competencias de las Unidades de Aprendizaje, así como en la competencia del módulo; **podrá proponer y utilizar todas las estrategias didácticas que considere necesarias** para el logro de estos fines educativos, con la recomendación de que fomente, preferentemente, las estrategias y técnicas didácticas que se describen en este apartado.

Al respecto, entenderemos como estrategias didácticas los planes y actividades orientados a un desempeño exitoso de los resultados de aprendizaje, que incluyen estrategias de enseñanza, estrategias de aprendizaje, métodos y técnicas didácticas, así como, acciones paralelas o alternativas que el docente y los alumnos realizarán para obtener y verificar el logro de la competencia; bajo este tenor, **la autoevaluación debe ser considerada también como una estrategia por excelencia para educar al alumno en la responsabilidad y para que aprenda a valorar, criticar y reflexionar sobre el proceso de enseñanza y su aprendizaje individual.**

Es así como la selección de estas estrategias debe orientarse hacia un enfoque constructivista del conocimiento y estar dirigidas a que los alumnos observen y estudien su entorno, con el fin de generar nuevos conocimientos en contextos reales y el desarrollo de las capacidades reflexivas y críticas de los alumnos.

Desde esta perspectiva, a continuación se describen brevemente los tipos de aprendizaje que guiarán el diseño de las estrategias y las técnicas que deberán emplearse para el desarrollo de las mismas:

## TIPOS DE APRENDIZAJES.

***Aprendizaje Significativo***

Se fundamenta en una concepción constructivista del aprendizaje, la cual se nutre de diversas concepciones asociadas al cognoscitivismo, como la teoría psicogenética de Jean Piaget, el enfoque sociocultural de Vygotsky y la teoría del aprendizaje significativo de Ausubel.

Dicha concepción sostiene que el ser humano tiene la disposición de aprender verdaderamente sólo aquello a lo que le encuentra sentido en virtud de que está vinculado con su entorno o con sus conocimientos previos. Con respecto al comportamiento del alumno, se espera que sean capaces de desarrollar aprendizajes significativos, en una amplia gama de situaciones y circunstancias, lo cual equivale a "aprender a aprender", ya que de ello depende la construcción del conocimiento.

***Aprendizaje Colaborativo.***

El aprendizaje colaborativo puede definirse como el conjunto de métodos de instrucción o entrenamiento para uso en grupos, así como de estrategias para propiciar el desarrollo de habilidades mixtas (aprendizaje y desarrollo personal y social). En el aprendizaje colaborativo cada miembro del grupo es **responsable de su propio aprendizaje, así como del de los restantes miembros del grupo** (Johnson, 1993.)

Más que una técnica, el aprendizaje colaborativo es considerado una filosofía de interacción y una forma personal de trabajo, que implica el manejo de aspectos tales como el **respeto a las contribuciones y capacidades individuales de los miembros del grupo** (Maldonado Pérez, 2007). Lo que lo distingue de otro tipo de situaciones grupales, es el desarrollo de la interdependencia positiva entre los alumnos, es decir, de una toma de conciencia de que **sólo es posible lograr las metas individuales de aprendizaje si los demás compañeros del grupo también logran las suyas**.

El aprendizaje colaborativo surge a través de transacciones entre los alumnos, o entre el docente y los alumnos, en un proceso en el cual cambia la responsabilidad del aprendizaje, del docente como experto, al alumno, y asume que el docente es también un sujeto que aprende. Lo más importante en la formación de grupos de trabajo colaborativo es vigilar que los elementos básicos estén claramente estructurados en cada sesión de trabajo. Sólo de esta manera se puede lograr que se produzca, tanto el esfuerzo colaborativo en el grupo, como una estrecha relación entre la colaboración y los resultados (Johnson & F. Johnson, 1997).

Los elementos básicos que deben estar presentes en los grupos de trabajo colaborativo para que éste sea efectivo son:

- la interdependencia positiva.
- la responsabilidad individual.
- la interacción promotora.
- el uso apropiado de destrezas sociales.
- el procesamiento del grupo.

Asimismo, el trabajo colaborativo se caracteriza principalmente por lo siguiente:

- Se desarrolla mediante **acciones de cooperación, responsabilidad, respeto y comunicación**, en forma sistemática, entre los integrantes del grupo y subgrupos.
- Va **más allá que sólo el simple trabajo en equipo** por parte de los alumnos. Básicamente se puede orientar a que los alumnos intercambien información y trabajen en tareas hasta que todos sus miembros las han entendido y terminado, aprendiendo a través de la colaboración.
- Se distingue por el desarrollo de una **interdependencia positiva entre los alumnos**, en donde se tome conciencia de que sólo es posible lograr las metas individuales de aprendizaje si los demás compañeros del grupo también logran las suyas.
- Aunque en esencia esta estrategia promueve la actividad en pequeños grupos de trabajo, se debe cuidar en el planteamiento de las actividades que **cada integrante obtenga una evidencia personal para poder integrarla a su portafolio de evidencias**.

***Aprendizaje Basado en Problemas.***

Consiste en la presentación de **situaciones reales o simuladas** que requieren la aplicación del conocimiento, en las cuales el **alumno debe analizar la situación y elegir o construir una o varias alternativas para su solución** (Díaz Barriga Arceo, 2003). Es importante aplicar esta estrategia ya que **las competencias se adquieren en el proceso de solución de problemas** y en este sentido, el alumno aprende a solucionarlos cuando se enfrenta a problemas de su vida cotidiana, a problemas vinculados con sus vivencias dentro del Colegio o con la profesión. Asimismo, el alumno se apropia de los conocimientos, habilidades y normas de comportamiento que le permiten la aplicación creativa a nuevas situaciones sociales, profesionales o de aprendizaje, por lo que:

- Se puede trabajar en forma individual o de grupos pequeños de alumnos que se reúnen a analizar y a resolver un problema seleccionado o diseñado especialmente para el logro de ciertos resultados de aprendizaje.
- Se debe presentar primero el problema, se identifican las necesidades de aprendizaje, se busca la información necesaria y finalmente se regresa al problema con una solución o se identifican problemas nuevos y se repite el ciclo.
- Los problemas deben estar diseñados para motivar la búsqueda independiente de la información a través de todos los medios disponibles para el alumno y además generar discusión o controversia en el grupo.
- El mismo diseño del problema debe estimular que los alumnos utilicen los aprendizajes previamente adquiridos.
- El diseño del problema debe comprometer el interés de los alumnos para examinar de manera profunda los conceptos y objetivos que se quieren aprender.
- El problema debe estar en relación con los objetivos del programa de estudio y con problemas o situaciones de la vida diaria para que los alumnos encuentren mayor sentido en el trabajo que realizan.
- Los problemas deben llevar a los alumnos a tomar decisiones o hacer juicios basados en hechos, información lógica y fundamentada, y obligarlos a justificar sus decisiones y razonamientos.
- Se debe centrar en el alumno y no en el docente.

**TÉCNICAS**

***Método de proyectos.***

Es una técnica didáctica que incluye actividades que pueden requerir que los alumnos **investiguen, construyan y analicen información** que coincida con los objetivos específicos de una tarea determinada en la que se **organizan actividades desde una perspectiva experiencial**, donde el alumno aprende a través de la práctica personal, activa y directa con el propósito de aclarar, reforzar y construir aprendizajes (Intel Educación).

Para definir proyectos efectivos se debe considerar principalmente que:

- Los alumnos son el centro del proceso de aprendizaje.
- Los proyectos se enfocan en resultados de aprendizaje acordes con los programas de estudio.
- Las preguntas orientadoras conducen la ejecución de los proyectos.
- Los proyectos involucran múltiples tipos de evaluaciones continuas.
- El proyecto tiene conexiones con el mundo real.
- Los alumnos demuestran conocimiento a través de un producto o desempeño.
- La tecnología apoya y mejora el aprendizaje de los alumnos.
- Las destrezas de pensamiento son integrales al proyecto.

Para el presente módulo se hacen las siguientes recomendaciones:

- Integrar varios módulos mediante el método de proyectos, lo cual es ideal para desarrollar un trabajo colaborativo.
- En el planteamiento del proyecto, cuidar los siguientes aspectos:
  - ✓ Establecer el alcance y la complejidad.
  - ✓ Determinar las metas.
  - ✓ Definir la duración.
  - ✓ Determinar los recursos y apoyos.
  - ✓ Establecer preguntas guía. Las preguntas guía conducen a los alumnos hacia el logro de los objetivos del proyecto. La cantidad de preguntas guía es proporcional a la complejidad del proyecto.
  - ✓ Calendarizar y organizar las actividades y productos preliminares y definitivos necesarias para dar cumplimiento al proyecto.
- Las actividades deben ayudar a responsabilizar a los alumnos de su propio aprendizaje y a **aplicar competencias adquiridas** en el salón de clase **en proyectos reales**, cuyo planteamiento se basa en un problema real e **involucra distintas áreas**.

- El proyecto debe implicar que los alumnos **participen en un proceso de investigación**, en el que **utilicen diferentes estrategias de estudio**; puedan participar en el proceso de planificación del propio aprendizaje y les ayude a ser flexibles, reconocer al "otro" y comprender su propio entorno personal y cultural. Así entonces se debe favorecer el desarrollo de **estrategias de indagación, interpretación y presentación del proceso seguido**.
- De acuerdo a algunos teóricos, mediante el método de proyectos los alumnos buscan soluciones a problemas no convencionales, cuando llevan a la práctica el hacer y depurar preguntas, debatir ideas, hacer predicciones, diseñar planes y/o experimentos, recolectar y analizar datos, establecer conclusiones, comunicar sus ideas y descubrimientos a otros, hacer nuevas preguntas, crear artefactos o propuestas muy concretas de orden social, científico, ambiental, etc.
- En la gran mayoría de los casos los proyectos se llevan a cabo **fuera del salón de clase** y, dependiendo de la orientación del proyecto, en muchos de los casos pueden **interactuar con sus comunidades** o permitirle un **contacto directo con las fuentes de información** necesarias para el planteamiento de su trabajo. Estas experiencias en las que se ven involucrados hacen que aprendan a manejar y usar los recursos de los que disponen como el tiempo y los materiales.
- Como medio de evaluación se recomienda que todos los proyectos tengan **una o máspresentaciones del avance para evaluar resultados** relacionados con el proyecto.
- Para conocer acerca del progreso de un proyecto se puede:
    - ✓ Pedir reportes del progreso.
    - ✓ Presentaciones de avance,
    - ✓ Monitorear el trabajo individual o en grupos.
    - ✓ Solicitar una bitácora en relación con cada proyecto.
    - ✓ Calendarizar sesiones semanales de reflexión sobre avances en función de la revisión del plan de proyecto.

***Estudio de casos.***

El estudio de casos es una técnica de enseñanza en la que los alumnos **aprenden sobre la base deexperiencias y situaciones de la vida real**, y se permiten así, construir su propio aprendizaje en un contexto que los aproxima a su entorno. Esta técnica se basa en la participación activa y en procesos colaborativos y democráticos de discusión de la situación reflejada en el caso, por lo que:

- Se deben representar situaciones problemáticas diversas de la vida para que se estudien y analicen.
- Se pretende que los alumnos generen soluciones validas para los posibles problemas de carácter complejo que se presenten en la realidad futura.
- Se deben proponer datos concretos para reflexionar, analizar y discutir en grupo y encontrar posibles alternativas para la solución del problema planteado. Guiar al alumno en la generación de alternativas de solución, le permite desarrollar la habilidad creativa, la capacidad de innovación y representa un recurso para conectar la teoría a la práctica real.

- Debe permitir reflexionar y contrastar las propias conclusiones con las de otros, aceptarlas y expresar sugerencias.

El estudio de casos es pertinente usarlo cuando se pretende:

- Analizar un problema.
- Determinar un método de análisis.
- Adquirir agilidad en determinar alternativas o cursos de acción.
- Tomar decisiones.

Algunos teóricos plantean las siguientes fases para el estudio de un caso:

- **Fase preliminar:** Presentación del caso a los participantes
- **Fase de eclosión:** "Explosión" de opiniones, impresiones, juicios, posibles alternativas, etc., por parte de los participantes.
- **Fase de análisis:** En esta fase es preciso llegar hasta la determinación de aquellos hechos que son significativos. Se concluye esta fase cuando se ha conseguido una síntesis aceptada por todos los miembros del grupo.
- **Fase de conceptualización:** Es la formulación de conceptos o de principios concretos de acción, aplicables en el caso actual y que permiten ser utilizados o transferidos en una situación parecida.

***Interrogación.***

Consiste en llevar a los alumnos a la **discusión y al análisis de situaciones o información**, con base en preguntas planteadas y formuladas por el docente o por los mismos alumnos, con el fin de explorar las capacidades del pensamiento al activar sus procesos cognitivos; se recomienda **integrar esta técnica de manera sistemática y continua** a las anteriormente descritas y al abordar cualquier tema del programa de estudio.

***Participativo-vivenciales.***

Son un conjunto de elementos didácticos, sobre todo los que exigen un grado considerable de **involucramiento y participaciónde todos los miembros del grupo** y que sólo tienen como límite el grado de imaginación y creatividad del facilitador.

Los ejercicios vivenciales son una alternativa para llevar a cabo el proceso enseñanza-aprendizaje, no sólo porque facilitan la transmisión de conocimientos, sino porque además permiten **identificar y fomentar aspectos de liderazgo, motivación, interacción y comunicación del grupo**, etc., los cuales son de vital importancia para la organización, desarrollo y control de un grupo de aprendizaje.

Los ejercicios vivenciales resultan ser una situación planeada y estructurada de tal manera que representan una experiencia muy atractiva, divertida y hasta emocionante. El juego significa apartarse, salirse de lo rutinario y monótono, para asumir un papel o personaje a través del cual el individuo pueda manifestar lo que verdaderamente es o quisiera ser sin temor a la crítica, al rechazo o al ridículo.
El desarrollo de estas experiencias se encuentra determinado por los conocimientos, habilidades y actitudes que el grupo requiera revisar o analizar y por sus propias vivencias y necesidades personales.

## 4. Enfoque del módulo

La competencia que se desarrolla en este módulo implica que el alumno instale 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.

Las competencias que se pretenden fomentar consideran actividades tales como identificarvulnerabilidades comprendidas por riesgos y amenazas en la seguridad del hardware y software con base a los alertamientos que emite el equipo,evaluar la integridad de la información y operación del equipo de cómputo conforme recomendaciones técnicas de seguridad contra riesgos y amenazas, establecer recomendaciones de tecnología de seguridad en hardware y software, así como instalar tecnología de seguridad protegiendo la información y equipo de cómputo contra amenazas a su integridad, basándose en las recomendaciones técnicas, simultáneamente que se familiariza con los sitios especializados en información técnica relacionada con esta tecnología, con la finalidad que pueda obtener continua y permanentemente información y recomendaciones actualizadas, para enfrentar la generación y evolución de amenazas continua y permanente.

El módulo considera el desarrollo de un proceso formativo secuencial, aprovechando los conocimientos previos del alumno, que le permita realizar actividades profesionales especializadas en pequeñas y medianas empresas, como microempresario o contratista de otras con mayor presencia en el mercado, dedicadas a la instalación y mantenimiento de redes, mantenimiento de equipo de cómputo, implementación de seguridad a en el harware y software, construcción de redes de telecomunicación. En base a esto, se requiere el desarrollo de competencias en la operación e instalación de medios de comunicación en general, operación y monitoreo del hardware y software de cómputo y comunicaciones, como módems, tarjetas de comunicaciones de redes e inalámbricas, tranceivers, routers, switches, puentes y gateways (puertas de enlace), servidores con distintos propósitos, así como laaplicación de estándares internacionales que los regulan, una actualización y autocapacitación permanente en materia de seguridad.

Dado la naturaleza de formación integral, el módulo también fomenta en el alumno el desarrollo de las competencias disciplinares básicas y genéricas tales como la interpretación y emisión de mensajes pertinentes en distintos contextos mediante el uso de medios, códigos y herramientas apropiados para el desarrollo de algunos temas, estableciendo una postura personal sobre los temas abordados e identificando su relevancia general en su formación, considerando otros puntos de vista de manera crítica y reflexiva, y manteniendo relaciones interpersonales positivas con sus maestros y compañeros de grupo; mostrando una actitud respetuosa hacia la interculturalidad y la diversidad de creencias, valores, ideas y prácticas sociales; desarrollando habilidades matemáticas; desarrollando innovaciones y proponiendo soluciones a problemas a partir de métodos establecidos en este campo específico de la seguridad en el hardware y software.

## 5. Orientaciones didácticas y estrategias de aprendizaje por unidad

| **Unidad I:** | Producción de imágenes y sonidos en formato digital. |
|---|---|

**Orientaciones didácticas (Dirigidas al Docente)**

En esta unidad el alumno desarrolla la competencia en identificación de vulnerabilidades comprendidas por riesgos (acciones omisas o incompletas internas en la organización) y amenazas (actividades de agentes externos a la organización contra la integridad de la información) y la evaluación a la integridad de la información relacionada con el hardware y software de cómputo. Asimismo, se desarrollan las competencias genéricas aplicables de manera natural a las competencias profesionales expresadas en los Resultados de Aprendizaje (RA), con el fin de promover una formación integral en el alumno, por lo que, durante todo el módulo, se fomenta:

- La autonomía, responsabilidad y cuidado de sí mismo, mediante el autoconocimiento que cada alumno va desarrollando, tanto de sus cualidades, como de las áreas en que debe trabajar para su reforzamiento, determinando las acciones de corto, mediano y largo plazo, necesarias para la consecución de los objetivos definidos, considerando los factores sociales, económicos y personales que pueden influir positiva o negativamente en los objetivos contemplados para planear, elegir alternativas y administrar los recursos con los que cuenta.
- Que el alumno proponga soluciones a problemas reales o hipotéticos, con base en actividades de búsqueda de información objetiva y veraz, aplicación de lo aprendido, e innovación en los métodos establecidos. Asimismo, se promueve el análisis crítico y fundamentado.
- El interés y el respeto por la diversidad cultural en todas sus manifestaciones y que el alumno conozca puntos de vista diferentes sobre asuntos de interés público y personal, como condición para conformar el criterio personal de manera libre y sustentada.
- El compromiso con el respeto a la persona, sin distinción de género, y la promoción de la igualdad de oportunidades para hombres y mujeres, asumiendo el alumno el papel de agente de cambio en el proceso de apertura de espacios de participación social y laboral de los que tradicionalmente se ha excluido al género femenino.
- Que el alumno sea capaz de automotivarse en el logro de metas personales y académicas, de desarrollar la capacidad para regular y manejar sus propios impulsos y necesidades, asumir sus propios sentimientos y emociones y encauzarlos positivamente.
- Que sea capaz de continuar aprendiendo de manera cada vez más eficaz y autónoma de acuerdo a los propios objetivos y necesidades, lo que implica aprender a autorregular su proceso de aprendizaje y a resolver diversas problemáticas de la vida académica y profesional, realizando de manera sistemática la planificación de las actividades de aprendizaje, la regulación de su proceso de aprendizaje y la evaluación de los resultados obtenidos tras la aplicación de la estrategia seleccionada.
- Que desarrolle capacidades para establecer una comunicación asertiva y efectiva, en diversos contextos, así como para identificar canales alternos

| **Unidad I:** | Producción de imágenes y sonidos en formato digital. |
|---|---|

**Orientaciones didácticas (Dirigidas al Docente)**

y plurales que diversifiquen la obtención de la información y los enfoques con que ésta es tratada, utilizando una segunda lengua en situaciones cotidianas y en la consulta e interpretación de documentos técnicos.

- Que aprenda a desempeñarse en situaciones de aprendizaje cooperativo y colaborativo, interactuando y trabajando para el logro de los objetivos y metas de aprendizaje del grupo, lo que contribuye también al desarrollo personal y social del alumno.
- Que participe activamente en la democracia, traducida en una mayor equidad en diversos ámbitos sociales y profesionales de su entorno. Todo ello con capacidad de tolerancia y flexibilidad de criterio para alcanzar consensos.
- Que incorpore medidas de seguridad e higiene en el desempeño de sus actividades profesionales.
- Que adquiera el compromiso social de sustentabilidad, aplicable más allá de lo relativo al medio ambiente, orientándose a la satisfacción de las necesidades actuales, sin prejuicio de las futuras generaciones en el plano social, tecnológico, económico, cultural y cualquier otro que se relacione con la preservación y bienestar de la especie humana.
- Que aprenda a minimizar el impacto de sus actividades cotidianas sobre el medio ambiente; consuma responsablemente; se desempeñe con seguridad, calidad y ética en espacios naturales y urbanos; elimine contaminantes o las fuentes de riesgo antes de que se generen, y seleccione y emplee materiales reciclables y biodegradables.
- Que aprenda a movilizar sus recursos personales (conocimientos, habilidades, actitudes y valores) y utilizar estrategias efectivas de aprendizaje continuo para ingresar, mantenerse, desarrollarse y “navegar” en el mundo del trabajo, a lo largo de su trayectoria laboral, ya sea en contextos de trabajo dependientes como independientes

Por otro lado, el docente diseña actividades que promueven el desarrollo y formación integral del estudiante y realiza el acompañamiento en la identificación de problemas que son una barrera en su aprendizaje y desarrollo de competencias, para ayudarlo a que descubra su potencial y que enfrente y supere los retos de la vida utilizando sus competencias, la confianza en sí mismo y se mantenga firme en la consecución de sus metas.

Para el efecto, en la presente unidad se emplearán las técnicas participo – vivenciales y de la interrogación, bajo el enfoque de aprendizaje significativo y colaborativo, descritos en el apartado 3 de la presente guía.

**Actividades sugeridas:**

1. Inicia la sesión presentándose ante el grupo. Da una introducción general del módulo y analiza en conjunto los resultados de aprendizaje que se pretenden lograr. Establece la forma de trabajo en clase y explica cómo se llevarán a cabo las actividades de evaluación, considerando las rúbricas correspondientes. Asimismo, invita a los alumnos a practicar los valores de respeto, dignidad, la no-violencia, la responsabilidad, el orden, la

| **Unidad I:** | Producción de imágenes y sonidos en formato digital. |
|---|---|

**Orientaciones didácticas (Dirigidas al Docente)**

limpieza y el trabajo en equipo en todas sus actividades y relaciones que establezcan.

2. Realiza una evaluación diagnóstica sobre medios de comunicación básica, manejo de paquetería de cómputo, operación y diagnóstico en el equipo de cómputo y redes locales, para identificar los aspectos que son necesarios reforzar. Solicita a los alumnos, su compromiso para estudiar lo necesario para alcanzar la competencia del módulo. Orienta al grupo en la definición de metas de aprendizaje y estrategias para alcanzarlas, haciendo uso de sus habilidades, valores y fortalezas.
3. Discute las configuraciones de hardware y software de cómputo y comunicaciones asociadas con él, induce la participación de los alumnos en la identificación de riesgos y amenazas en los componentes físicos, programas de cualquier naturaleza instalados en el equipo, induciendo a que describan las causas que permiten los mismos. Solicita a los alumnos, que elaboren una tabla que informe por cada componente tanto hardware como software, el riesgo que genera, la condición por la cual lo genera, incluyendo las normas de seguridad para el desarrollo de software, así como el agente externo al que está expuesto y la condición que genera esta exposición.
4. Dirige la utilización de herramientas y comandos de monitoreo en el tráfico de red hacia el equipo, particularmente en el enlace ADSL, por la conexión y riesgo permanente que existe. Solicita el uso de las herramientas de Microsoft, con la finalidad que desarrollen la competencia en la identificación de riesgos y amenazas.
5. Propicia 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. Solicita a los alumnos complementen la información con la que cuentan respecto, acerca de la identificación de actividades que representan riesgos y amenazas.
6. **Orienta y apoya la realización de la práctica No. 1"Identifica riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo, elaborando un reporte de resultados", correspondiente a la actividad de evaluación 1.1.1.**
7. Realiza una demostraciónpráctica sobre la identificación de agentes externos, desde conductos de intrusión hasta suplantación de identidad, que son amenazas al equipo y a la integridad de la información. Solicita a los alumnos ejemplos de identificación de estas amenazas, para discutirlos en el grupo y consolidar su aprendizaje en identificación de atentados a la integridad de información.
8. Realiza en coordinación con el grupo actividades de identificación de debilidades en la instalación y las comunicaciones, iniciando con los protocolos innecesarios en la instalación y concluye con la omisión o usos inadecuados de WEP/WAP. Solicita a los alumnos el monitoreo y descripción delos efectos en la integridad de la información, que provoca el no ser atendidos.
9. **Orienta y apoya la realización de la práctica No. 2** "**Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación", correspondiente a la actividad de evaluación 1.2.1.**
10. Comenta en clase los resultados de las evaluaciones realizadas, efectuando una coevaluación enfocada tanto al proceso ejecutado como a los resultados obtenidos.

| Estrategias de aprendizaje (dirigidas al alumno) | Recursos académicos |
|---|---|
| • Expone sus expectativas del curso y analiza las actividades de aprendizaje, los criterios de evaluación y el método de aprendizaje. Plantea sus dudas y toma nota sobre los puntos explicados por el docente. Se compromete a practicar los valores de respeto, dignidad, la no-violencia, la responsabilidad, el orden, la limpieza y el trabajo en equipo en todas sus actividades y relaciones que establezca.<br>• Contesta la evaluación diagnóstica sobre medios de comunicación básica, manejo de paquetería de cómputo, operación y diagnóstico en el equipo de cómputo y redes locales, para contribuir a identificar los aspectos que son necesarios reforzar. Se compromete a estudiar lo necesario para alcanzar la competencia del módulo. Define metas de aprendizaje y estrategias para alcanzarlas, haciendo uso de sus habilidades, valores y fortalezas.<br>• Participa activamente en la discusiónde las configuraciones de hardware y software de cómputo y comunicaciones asociadas con él. Participa en la identificación de riesgos y amenazas en los componentes físicos, programas de cualquier naturaleza instalados en el equipo, describiendo sus causas. Y elabora una tabla en la que informa por cada componente tanto hardware como software, el riesgo que genera, la condición por la cual lo genera, incluyen las normas de seguridad para el desarrollo de software, así como el agente externo al que está expuesto y la condición que genera esta exposición, presentándola al grupo para enriquecerla con la discusión y aportaciones de sus compañeros.<br>• Utiliza 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.<br>• Participa 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. Complementa la información con la que cuentan respecto de la identificación de actividades, que representan riesgos y amenazas.<br>• **Realiza la práctica No. 1 "Identifica riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo, elaborando un reporte de resultados", correspondiente a la actividad de evaluación 1.1.1.** | • Programa de estudios.<br>• Instrumento de evaluación diagnóstica.<br>• Tutoriales.<br>• Software de aplicación específica.<br>• Gómez Vieites,Álvaro. Enciclopedia de la seguridad informática.Alfaomega RA-MA, México 2007.<br>• Ariganello, Ernesto. Técnicas de Configuración de Routers Cisco, Alfaomega Grupo Editor, 2008.<br>• Roebuck, Kevin, Wireless Security, Editorial Tebbo, 2011.<br>• Ataques informáticos (DNS seguro), Disponible en: http://www.dnssec.net, [12/10/15]<br>• Ataques informáticos (KeyGhost), Disponible en: http://www.keyghost.com, [12/10/15]<br>• Escáner de vulnerabilidad, video demostrativo, Disponible en: http://www.youtube.com/watch?v=3RgOtjv4v8E, [12/10/15]<br>• Herramientas para el reconocimiento de sistemas y escaneo de puertos (Netscantools), Disponible en: http://www.nwpsw.com/, [12/10/15]<br>• Identificación de riesgos y tipos de hackers, |

| Estrategias de aprendizaje (dirigidas al alumno) | Recursos académicos |
|---|---|
| • Realiza ejemplos de identificación de amenazas de agentes externos, desde conductos de intrusión hasta suplantación de identidad, y los discute en el grupo.<br>• Realiza 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. Monitorea y describe los efectos en la integridad de la información que provoca, el no ser atendido.<br>• **Realiza la práctica No. 2 "Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación", correspondiente a la actividad de evaluación 1.2.1.**<br>• Realiza una coevaluación con el docente enfocada tanto al proceso ejecutado como a los resultados obtenidos | Disponible en: http://es.kioskea.net/contents/attaques/typologie-pirates.php3, [12/10/15]<br>• Información técnica seguridad, Disponible en: http://www.textoscientificos.com/, [12/10/15]<br>• Listas de seguridad, herramientas de seguridad y escaneo, disponible en: http://www.insecure.org/, [12/10/15]<br>• Medidas de seguridad, Disponible en:http://www.windowsecurity.com/whitepapers/security_secure_internet_data_transmission.html, [12/10/15]<br>• Metodología de intrusión de red, Disponible en: http://es.kioskea.net/contents/attaques/methodologie.php3, [12/10/15] |

| **Unidad II** | Implementación de tecnología de seguridad en hardware y software del equipo de cómputo. |
|---|---|

## Orientaciones didácticas (Dirigidas al docente)

En esta unidad el alumno desarrolla las competencias relativas aestablecer recomendaciones de tecnología de seguridad en hardware y software e instalar la misma protegiendo la información y equipo de cómputo contra amenazas a su integridad. Asimismo, se refuerzan las competencias genéricas de trabajo en equipo, análisis y solución de problemas y se promueve los valores: responsabilidad, disciplina, tolerancia y liderazgo, apoyando al estudiante en su desarrollo integra y en la consecución de sus metas, fortaleciendo su seguridad y confianza en el mismo con sus logros.

Para esto, en la presente unidad se emplearán las técnicas participativo – vivenciales, bajo el enfoque de aprendizaje significativo y colaborativo, descritos en el apartado 3 de la presente guía.

**Actividades sugeridas:**

1. Integra equipos de trabajo asignando un riesgo o amenaza a cada uno, con la finalidad de preparar recomendaciones para enfrentarlos.Solicita a cada equipo presentar sus recomendaciones ante el grupo, generando análisis y complementarlas, con las aportaciones de todos los equipos.
2. Dirige a los alumnos para planear actividades contra agentes externos o internos, que intentan violar la integridad de la operación del equipo y de la información. Solicita la conclusión del plan con una investigación vía internet, enriqueciéndolas con consultas sobre recomendaciones técnicas de especialistas en seguridad.
3. Orienta la búsqueda de recursos relacionados con diversos temas del módulo en la biblioteca digital de la Red Académica del CONALEP. Disponibles en: http://sied.conalep.edu.mx/bv3/.
4. Demuestra las debilidades que pueden existir en el desarrollo de aplicaciones de internet, estimula a los alumnos en la generación de ideas sobre cómo enfrentarlas, integrándolas en un documento de políticas de seguridad en el desarrollo de aplicaciones en internet.
5. **Orienta y apoya la realización de la práctica No. 3 “Establece recomendaciones de seguridad identificando sus efectos”, correspondiente a la actividad de evaluación 2.1.1.**
6. Realiza la demostración práctica de la instalación de herramientas de seguridad en redes de computadoras y aleatoriamente, selecciona a los alumnos, para que instalen uno a uno cada una de las herramientas analizadas en el curso, de tal manera que se logre la cobertura total con los integrantes del grupo. Solicita la elaboraciónde un díptico sobre las herramientas de seguridad y su instalación.
7. Asigna una investigación sobre la instalación de herramientas de seguridad en redes VPN y Windows para que la realicen en cualquier fuente disponible, con la finalidad de que se discuta y se haga una demostración en clase. Con base en los comentarios generados solicita que se complemente el díptico anterior con el procedimiento de instalación de herramientas de seguridad.

| **Unidad II** | Implementación de tecnología de seguridad en hardware y software del equipo de cómputo. |
|---|---|

**Orientaciones didácticas (Dirigidas al docente)**

8. Aplica las herramientas de seguridad en los componentes físicos del aula de cómputo, asigna los equipos de trabajo la aplicación desde la instalación de protocolo WEP, hasta separar la red inalámbrica de la red local interna. Solicita la elaboración de un reporte del procedimiento realizado y los resultados obtenidos.
9. Guía a los estudiantes en la instalación de tecnología de seguridad en los servicios de internet; pide por equipos de trabajo la instalación de la tecnología de seguridad.
10. Asigna a los equipos de trabajo la elaboración de 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. Solicita a cada equipo de trabajo, realizar la presentación de su propuesta para recibir retroalimentación del docente e integrantes del grupo con la finalidad de complementarla.
11. **Orienta y apoya la realización de la práctica No. 4 "Instala tecnología de seguridad reportando su efecto en la integridad de la información", correspondiente a la actividad de evaluación 2.2.1. En la rúbrica correspondiente se incluye una Coevaluación.**
12. Aplica un cuestionario sobre los aspectos relevantes de la Unidad, solicitando su respuesta en forma individual y posteriormente permite que los alumnos circulen por el aula con el fin de compartir los aprendizajes adquiridos con sus compañeros, propiciando la participación de todo el grupo en un clima de respeto, colaboración y confianza.

| **Estrategias de aprendizaje (dirigidas al alumno)** | **Recursos académicos** |
|---|---|
| **El alumno:**<br>• Integrado en equipos de trabajo presenta sus recomendaciones ante el grupo y las complementa con las aportaciones de todos los equipos.<br>• Revisa y utiliza los recursos relacionados con diversos temas del módulo en la biblioteca digital de la Red Académica del CONALEP, disponibles en: http://sied.conalep.edu.mx/bv3/<br>• Concluye 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.<br>• Genera ideas sobre cómo enfrentar las debilidades que pueden existir en el desarrollo de | • Tuoriales.<br>• Software de aplicación específica.<br>• Gómez Vieites,Álvaro. Enciclopedia de la seguridad informática.Alfaomega RA-MA, México 2007.<br>• Ariganello, Ernesto. Técnicas de Configuración de Routers Cisco, Alfaomega Grupo Editor, 2008.<br>• Roebuck, Kevin, Wireless Security, Editorial |

| Estrategias de aprendizaje (dirigidas al alumno) | Recursos académicos |
|---|---|
| aplicaciones de internet, integrándolas en un documento de políticas de seguridad.<br>• **Realización la práctica No. 3 "Establece recomendaciones de seguridad identificando sus efectos", correspondiente a la actividad de evaluación 2.1.1.**<br>• Elabora un díptico sobre las herramientas de seguridad en redes de computadoras y su instalación.<br>• Realiza una investigación en cualquier fuente disponible sobre la instalación de herramientas de seguridad en redes VPN y Windows, y las realiza en aula en forma demostrativa para todos los compañeros de clase. Complementa el díptico anterior con el procedimiento de instalación de herramientas de seguridad.<br>• Elabora 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.<br>• Organizado en equipos instala la tecnología de seguridad en los servicios de internet.<br>• Elabora 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. Realiza la presentación de su propuesta, para recibir retroalimentación del docente e integrantes del grupo y complementarla.<br>• **Realiza la práctica No. 4 "Instala tecnología de seguridad reportando su efecto en la integridad de la información", correspondiente a la actividad de evaluación 2.2.1 y participa en la actividad de Coevaluación.**<br>• **Contesta el** cuestionario de manera individual sobre los aspectos relevantes de la Unidad, y posteriormente circula por el aula con el fin de compartir los aprendizajes adquiridos con sus compañeros propiciando la participación de todos en un clima de respeto, colaboración y confianza | Tebbo, 2011.<br>• Ataques informáticos (DNS seguro), Disponible en: http://www.dnssec.net, [12/10/15]<br>• Ataques informáticos (KeyGhost), Disponible en: http://www.keyghost.com, [12/10/15]<br>• Escáner de vulnerabilidad, video demostrativo, Disponible en: http://www.youtube.com/watch?v=3RgOtjv4v8E, [12/10/15]<br>• Herramientas para el reconocimiento de sistemas y escaneo de puertos (Netscantools), Disponible en: http://www.nwpsw.com/, [12/10/15]<br>• Identificación de riesgos y tipos de hackers, Disponible en: http://es.kioskea.net/contents/attaques/typologie-pirates.php3, [12/10/15]<br>• Información técnica seguridad, Disponible en: http://www.textoscientificos.com/, [12/10/15]<br>• Listas de seguridad, herramientas de seguridad y escaneo, disponible en: http://www.insecure.org/, [12/10/15]<br>• Medidas de seguridad, Disponible en:http://www.windowsecurity.com/whitepapers/security_secure_internet_data_transmission.html, [12/10/15]<br>Metodología de intrusión de red, Disponible en: http://es.kioskea.net/contents/attaques/methodolo |

| Estrategias de aprendizaje (dirigidas al alumno) | Recursos académicos |
|---|---|
| | gie.php3, [12/10/15] |

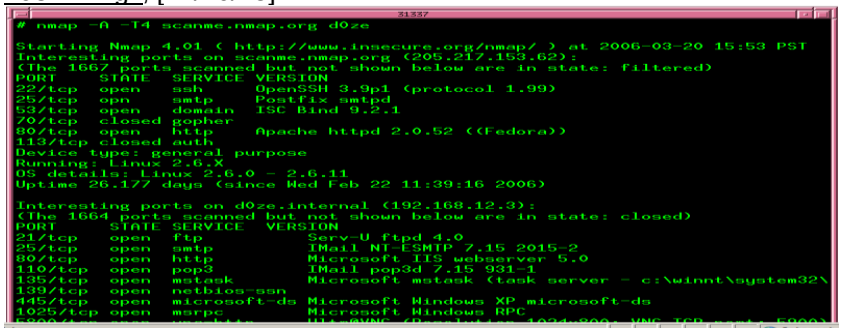
## 6. Prácticas/Ejercicios /Problemas/Actividades

| | | | |
|---|---|---|---|
| **Unidad de aprendizaje:** | Diagnóstico de riesgos y amenazas en la seguridad del equipo. | **Número:** | 1 |
| **Práctica:** | Identifica riesgos y amenazas en la seguridad del hardware y software en un equipo de cómputo, elaborando un reporte de resultados | **Número:** | 1 |
| **Propósito de la práctica:** | Identificar el nivel de protección del equipo con fines de evaluación del estado operacional del software de seguridad. | | |
| **Escenario:** | Taller o laboratorio | **Duración** | 2 horas |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| • 5 computadoras de escritorio con sistema operativo Windows vista o Windows 7, equipadas con tarjeta de comunicaciones de red local, tarjeta de comunicaciones inalámbricas<br>• 3 con sistema Mac OS (Apple), equipadas con tarjeta de comunicaciones de red local, tarjeta de comunicaciones inalámbricas.<br>• 1 manual por cada equipo de cómputo.<br>• 1 enlace ADSL (infinitum por ejemplo).<br>• Modem-router 2wire, con entradas USB, LAN y conexión inalámbrica<br>• Switch o hub, para incrementar el número de puertos del modem-router<br>• Router CISCO 1801 o dispositivo ADSL similar<br>• Enlace de banda ancha de 2 Mb mínimo. | •  Aplica las siguientes medidas de seguridad e higiene:<br>• Retira objetos metálicos en manos y cuello.<br>• Planea cualquier actividad en equipo energizado, antes de manipularlo para evitar shock eléctrico que cause daños a la integridad física del individuo y daños al equipo.<br>• Observa las medidas de seguridad e higiene propias del plantel y del laboratorio.<br>• Consulta manuales, catálogos, sitios especializados de internet en la identificación de los componentes de hardware involucrados directa o indirectamente en la práctica.<br>• Identifica el software de seguridad instalado en el equipo, utilizado en la protección del mismo.<br><br>**Identificación de riesgos en el equipo.**<br>Utiliza comandos de monitoreo para identificar el estado de:<br>• Antivirus<br>• Cortafuegos |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| | • Antimalware<br><br>**Elabora un reporte donde incluye:**<br>• Los sitios dudosos accesados en la última semana.<br>• Servicios se encuentra habilitados.<br>• Archivos de dudosa procedencia que se han ejecutado.<br>• *Applets* que se han ejecutado en el equipo.<br>• Estado de la administración de actualizaciones de seguridad.<br>• Estado operacional del software de protección.<br>• Identifica sitios de identidad desconocida, que potencialmente pueden conducto para atentar contra la seguridad del equipo, visitados en los últimos tres meses y determina si los sitios visitados son potencialmente una amenaza a la seguridad del equipo.<br>• Identifica el origen de los sitios identificados.<br>• Monitorea el tipo de archivos que se han ejecutado en los últimos tres meses o hasta donde la configuración del equipo lo permita.<br>• Evalúa de manera integral yde acuerdo con la información colectada,los siguientes aspectos:<br><br>**Identificación de amenazas en hardware y software**<br>Utiliza las herramientas de identificación de amenazas:<br>• MSAT (evaluación de seguridad de Microsoft)<br>• IIS (herramienta de bloqueo)<br>• Reporteador de puertos (portreporter)<br>• Muestreo de seguridad de la red (networksecurityscan).<br><br>Reporta resultados obtenidos con el uso de las herramientas.<br>Interpreta los resultados e informa esta interpretación. |

| | | | |
|---|---|---|---|
| **Unidad de aprendizaje:** | Diagnóstico de riesgos y amenazas en la seguridad del equipo. | **Número:** | 1 |
| **Práctica:** | Elabora un diagnóstico de la integridad de la información, identificando amenazas y debilidades de la instalación | **Número:** | 2 |
| **Propósito de la práctica:** | Elaborar compendio de seguridad y protección informática con base a consultas a sitios especializados en internet. | | |
| **Escenario:** | Taller o laboratorio | **Duración** | 3 horas |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| • Computadora con procesador de texto y software de presentación<br>• 5 Computadoras de escritorio con sistema operativo Windows vista o Windows 7, equipadas con tarjeta de comunicaciones de red local, tarjeta de comunicaciones inalámbricas<br>• Enlace de banda ancha de 2 Mb mínimo<br>• 1 manual por cada equipo de cómputo. | • Observa las medidas de seguridad e higiene propias del plantel y del laboratorio.<br>• Consulta manuales, catálogos, sitios especializados de internet en la identificación de los componentes de hardware involucrados directa o indirectamente en la práctica.<br>• Navega en internet con la finalidad de identificar sitios especializados en seguridad y protección informática.<br>**Diagnóstico de amenazas a la información.**<br>• Identifica las formas en que los siguientes agentes externos atentan contra la integridad de la información.<br>• Hackers<br>Utiliza la herramienta Nstaten el símbolo de DOS, describelos resultados y los interpreta.<br>Baja la herramienta Nmap del sitio http://nmap.org/images/nmap-401-demoscan-798x774.gif, [12/10/15]<br>  |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| | Instalar e interpreta los resultados, usándolo cuando esté establecida la comunicación con otra computadora, observa la pantalla que aparecen como respuesta en Fig. 1.<br><br>Identifica la tecnología y las formas de identificación de:<br>• Crakers<br>• Sniffers<br>• Phreakers<br>• Spammers.<br>• Creadores de virus<br>• Personal interno<br>• Intrusos remunerados.<br><br>Aplica la utilería igremote, explica su objetivo, lo que se puede hacer e interpreta los resultados.<br>• Virus: de boot, de archivos ejecutables, de lenguaje JAVA y de macros.<br>• Troyanos<br>• Rootkits<br>• Gusanos<br>• Spyware<br>• Malware<br>• Espionaje<br>• Modificación de información<br>• Spam<br>• Suplantación de identidad.<br>• Ingresa al sitio y utilizar las técnicas y herramientas mencionadas,http://www.rootkit.cl/hacking [12/10/15]<br>• Busca en internet programas de intrusión, identifica los nombres y describe lo que pueden hacer. |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| | **Diagnóstico de riesgos originados por las debilidades de instalación**<br><br>Identifica y describe:<br>• Protocolos de red existentes y cuáles no son necesarios<br>• Versión del IOS, ¿está actualizada?<br>• Archivos e impresoras compartidos usando TCP/IP<br>• NetBIOS habilitado sobre TCP<br>• Red o sistema informático no aislado de otras redes o sistemas<br>• Contraseñas potencialmente débiles, ¿cómo son? ¿Cómo deberían ser?<br>• Versión Antivirus, ¿está actualizada?<br>• Navegador , tipo y versión, ¿Cuál es la última versión?.<br>• Archivos de programa ejecutándose, ¿se conoce su origen? ¿de cuáles no se conoce el origen?<br>• Servicios de red, ¿todos se utilizan? ¿cuáles no se utilizan?.<br>• ¿Rutas estáticas configuradas?¿ en dónde es necesario? ¿en dónde no?<br>• Ejecución de applets de Java y activex, ¿cuáles se ejecutan? ¿es correcto?<br>• Respaldos de información ¿se realizan?¡¿con que frecuencia?¿es la frecuencia correcta?¿cuál fue la última ocasión que se respaldó información?<br>• WEP / WPA (Wireless Equivalent privacy/WiFi Protected Acces), ¿estáconfigurada? ¿Por qué si o porque no?<br>• ¿Cómo se puede conocer la IP a través del correo electrónico? ¿para qué nos sirve conocer la IP de otra computadora?<br>• Buscar la X originating IP [.....] en el código fuente del mensaje d correo electrónico.<br><br>**Evaluación de la situación de seguridad.**<br><br>• Considera los resultados del apartado anterior, con la finalidad de analizar la información para enfrentar los siguientes puntos:<br><br>• Identifica amenazas (agentes externos) de intrusión, confirmando cuál de las siguientes se pueden presentar explicando su respuesta:<br><br>• Conductos de intrusión.<br>– Virus y troyanos. |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| | • .Correo electrónico.<br>• Navegación por servidores web.<br>• Intercepción pasiva (eavesdropping).<br>– Sniffers<br>• Espionaje de información (snooping)<br>• Modificación de la información (tampering).<br>• Envío de correos electrónicos con nuestra identidad.<br>• Saturación de servidores web.<br>• Suplantación de identidad (spoofing).<br><br>Describe riesgos originados por debilidades en la instalación o seguridad identificados en el apartado anterior, confirmando cuál de las siguientes se pueden presentar, explicando su respuesta:<br><br>• Protocolos de red no necesarios.<br>• Archivos e impresoras compartidos usando TCP/IP.<br>• NetBIOS habilitado sobre TCP<br>• Red o sistema informático no aislado de otras redes o sistemas.<br>• Contraseñas potencialmente débiles.<br>• Antivirus desactualizada o inapropiado.<br>• Navegador con versiones no recientes.<br>• Ejecución de archivos de programa de dudoso origen.<br>• Ejecución de applets de Java y activex.<br>• Backups no actualizados.<br>• WEP / WPA. |

| | | | |
|---|---|---|---|
| **Unidad de aprendizaje:** | Implementación de tecnología de seguridad en hardware y software del equipo de cómputo. | **Número:** | 1 |
| **Práctica:** | Establece recomendaciones de seguridad identificando sus efectos | **Número:** | 3 |
| **Propósito de la práctica:** | Realizar recomendaciones de seguridad al identificar los efectos en un plan de acción. | | |
| **Escenario:** | Taller o laboratorio | Duración | 3 horas |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| • Computadora con procesador de texto y software de presentación.<br>• 5 computadoras de escritorio con sistema operativo Windows vista o Windows 7, equipadas con tarjeta de comunicaciones de red local, tarjeta de comunicaciones inalámbricas.<br>• Manual Two WireInstalallation guide.<br>• 1 manual por cada equipo de cómputo.<br>• 1 manual por cada componente de comunicaciones.<br>• 1 enlace ADSL (infinitum por ejemplo).<br>• Modem-router 2wire, con entradas USB, LAN y conexión inalámbrica.<br>• *Switch* o *hub,* para incrementar el número de puertos del modem-router.<br>• *Router* CISCO 1801 o dispositivo ADSL similar.<br>• Enlace de banda ancha de 2 Mb mínimo. | •  Aplica las siguientes medidas de seguridad e higiene:<br>• Retira objetos metálicos en manos y cuello<br>• Planea cualquier actividad en equipo energizado, antes de manipularlo para evitar shock eléctrico que cause daños a la integridad física del individuo y daños al equipo<br>• Observa las medidas de seguridad e higiene propias del plantel y del laboratorio<br>• Consulta manuales, catálogos, sitios especializados de internet en la identificación de los componentes de hardware involucrados directa o indirectamente en la práctica.<br>• Identifica la diferencia entre un riesgo y una amenaza a la protección de las instalaciones de cómputo.<br>• Identifica las herramientas disponibles para identificar el estado de protección contra amenazas.<br><br>**Recomendaciones contra vulnerabilidades.**<br>Considera información necesaria para establecer las recomendaciones contra vulnerabilidades a manera de un plan de proyecto, de manera secuencial en el tiempo de instalación, de acuerdo con los siguientes aspectos:<br>• Autorización y registro de usuarios<br>• Control de acceso a usuarios locales y remotos<br>• Certificados digitales |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| | • Servidores de autenticación<br>• Administración de contraseñas<br>• Reconocimiento de firmas manuscritas<br>• Huellas dactilares<br>• Recomendaciones de criptografía<br>• Algoritmos en protocolos<br><br>**Definición de acciones de seguridad**<br><br>Propone políticas de seguridad describiendo su validez y efectos e informa que vulnerabilidad atenúa o elimina, cada una de las siguientes acciones:<br><br>• Denegación de servicio<br>• Modificación al contenido de mensajes<br>• Suplantación de actividad.<br>• Conexión no autorizada a equipos y servidores.<br>• Prevención de ataques que realicen una llamada al sistema operativo<br>• Prevención de ataques que traten de accesar a carpetas dentro del servidor web<br>• Prevención de ataques que exploten la identificación de URL<br>• Elaboración de políticas para el desarrollo de aplicaciones en internet<br><br>Plan de acción sobre recomendaciones contra vulnerabilidad<br><br>Elabora el plan de acción como reporte, el cual contempla:<br>• Problema<br>• Causas probables<br>• Acciones a desarrollar.<br>• Soluciones a implantar.<br>• Mecanismo de implantación de soluciones.<br>• Marcas y proveedores de las soluciones a implantar. |

| | | | |
|---|---|---|---|
| **Unidad de aprendizaje:** | Implementación de tecnología de seguridad en hardware y software del equipo de cómputo. | **Número:** | 1 |
| **Práctica:** | Instala tecnología de seguridad reportando su efecto en la integridad de la información | **Número:** | 4 |
| **Propósito de la práctica:** | Evaluar la tecnología de protección y seguridad con que cuenta un equipo de cómputo. | | |
| **Escenario:** | Taller o laboratorio | **Duración** | 3 horas |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| • Computadora con procesador de texto y software de presentación<br>• 5 Computadoras de escritorio con sistema operativo Windows vista o Windows 7, equipadas con tarjeta de comunicaciones de red local, tarjeta de comunicaciones inalámbricas<br>• Manual Two WireInstalallation guide<br>• 1 manual por cada equipo de cómputo.<br>• 1 manual por cada componente de comunicaciones<br>• 1 enlace ADSL (infinitum por ejemplo).<br>• Modem-router 2wire, con entradas USB, LAN y conexión inalámbrica<br>• Switch o hub, para incrementar el número de puertos del modem- | •  Aplica las siguientes medidas de seguridad e higiene:<br>• Retira objetos metálicos en manos y cuello.<br>• Planea cualquier actividad en equipo energizado, antes de manipularlo para evitar shock eléctrico que cause daños a la integridad física del individuo y daños al equipo.<br>• Observa las medidas de seguridad e higiene propias del plantel y del laboratorio.<br>• Consulta las siguientes fuente, complementándolas si lo considera conveniente, relacionadas con el equipo de cómputo y de comunicaciones con que cuenta el laboratorio o taller y el plantel:<br>• Manuales.<br>• Boletines técnicos.<br>• Información del fabricante que no se encuentra en los manuales.<br>• Sitios especializados de internet.<br>• Foros especializados en seguridad<br><br>**Instalación de herramientas de seguridad en redes.**<br>Instala, ejecuta y describe la forma de implantar las siguientes acciones:<br>• Restricciones a los dispositivos ADSL (hardening).<br>– Eliminar servicios de entrada salida innecesarios.<br>– Restricción en listas de control de acceso.<br>– Autorizar acceso físico a los dispositivos.<br>– Eliminar ejecución de archivos de programa de dudoso origen<br>– Restringir ejecución de applets de Java y activex. |

| Materiales, herramientas, instrumental, maquinaria y equipo | Desempeños |
|---|---|
| router<br>• Router CISCO 1801 o dispositivo ADSL similar<br>• Enlace de banda ancha de 2 Mb mínimo | – Configurar seguridad en modems y dispositivos ADSL.<br><br>• Instalación de herramientas de seguridad en redes VPN y Windows<br>– Definir uso de protocolos<br>– Instalar redes basadas en SSL (Secure Socket Layers).<br>– Aplicar recomendaciones de seguridad de Microsoft.<br><br>**Instalación de seguridad en componentes físicos de oficina**<br>Considera en la instalación de tecnología de seguridad en componentes físicos de oficinas:<br>– Protocolo WEP<br>– Protocolo WPA<br>– Estándar RSN<br>– Estándar 802.1x<br>– Detección de intentos de intrusión<br>– Separación de la red inalámbrica de la red local interna.<br><br>**Acciones de seguridad para acceso a servicios de internet**<br>• Ejecuta, describe y reporta las siguientes acciones:<br>– Actualización parches de seguridad<br>– Control de cookies<br>– Control en la descarga desde internet<br>– Evasión a sitios dudosos<br>– Evaluación enlaces incluidos en correo electrónico<br>– Control de contenido activo en páginas WEB<br>– Control de certificados<br>– Medidas contra SPAM<br>– Medidas contra PHISING. |

# II. Guía de evaluación del módulo Aplicación de herramientas de seguridad en hardware y software

## 7. 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 guía en la evaluación de las competencias adquiridas por los alumnos, asociadas a los Resultados de Aprendizaje; en donde además, describe las técnicas y los instrumentos a utiliza y la ponderación de cada actividad de evaluación. Los Resultados de Aprendizaje se definen tomando como referentes: las competencias genéricas que va adquiriendo el alumno para desempeñase en los ámbitos personal y profesional que le permitan convivir de manera amónica con el medio ambiente y la sociedad; las disciplinares, esenciales para que los alumnos puedan desempeñase eficazmente en diversos ámbitos, desarrolladas en torno a áreas del conocimiento y las profesionales que le permitan un desempeño eficiente, autónomo, flexible y responsable de su ejercicio profesional y de actividades laborales específicas, en un entorno cambiante que exige la multifuncionalidad.

La importancia de la evaluación de competencias, bajo un enfoque de **mejora continua**, reside en que es un proceso por medio del cual se obtienen y analizan las evidencias del desempeño de un alumno con base en la guía de evaluación y rúbrica, para emitir un juicio que conduzca a toma decisiones.

La evaluación de competencias se centra en el desempeño real de los alumnos, soportado por evidencias válidas y confiables frente al referente que es la guía de evaluación, la cual, en el caso de competencias profesionales, está asociada con una norma técnica de competencia laboral (NTCL), de institución educativa o bien, una normalización específica de un sector o área y no en contenidos y/o potencialidades.

El **Modelo de Evaluación** se caracteriza porque es **Confiable** (queaplica el mismo juicio para todos los alumnos), **Integral** (involucra las dimensiones intelectual, social, afectiva, motriz y axiológica), **Participativa** (incluye autoevaluación, coevaluación y heteroevaluación), **Transparente** (congruente con los aprendizajes requeridos por la competencia), **Válida** (las evidencias deben corresponder a la guía de evaluación).

**Evaluación de los Aprendizajes.**

Durante el proceso de enseñanza - aprendizaje es importante considera tres categorías 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 alumnos. Permite también establecer vínculos socio-afectivos entre el docente y su grupo. El alumno a su vez podrá obtener información sobre los aspectos donde deberá hacer énfasis en su dedicación. El docente podrá **identificar las características del grupo y orientar adecuadamente sus estrategias**. En esta etapa pueden utilizase mecanismos informales de recopilación de información.

La evaluación **formativa** se realiza durante todo el proceso de aprendizaje del alumno, en forma constante, ya sea al finaliza cada actividad de aprendizaje o en la integración de varias de éstas. Tiene como finalidad **informa a los alumnos de sus avances** con respecto a los aprendizajes que deben alcanza 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 trabaja colaborativamente. Asimismo, el docente puede asumir nuevas estrategias que contribuyan a mejorar los resultados del grupo.

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 bien 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.

**Heteroevaluación, Coevaluación y Autoevaluación**

En esta nueva versión (02) de la guía de evaluación se están incluyendo de manera formal tres modalidades de evaluación, que según la persona que evalúa se denominan: heteroevaluación, coevaluación y autoevaluación.

La **heteroevaluación:** Es aquella que se realiza por personas externas al grupo escolar: representantes del sector productivo, docentes ajenos al grupo o cualquier otra persona o grupo colegiado con el dominio suficiente de la competencia, desempeño o producto que se pretenda evaluar. La heteroevaluación permite:

- Demostrar que el alumno adquirió la competencia a evaluar, en diversos contextos y ante cualquier persona o instancia evaluadora.
- Evidenciar ante agentes no integrantes del proceso enseñanza-aprendizaje las competencias desarrolladas, otorgando cierta objetividad a la evaluación.

La **coevaluación** se llevará a cabo entre pares de alumnos, pudiendo ser el evaluador un alumno o grupo de alumnos; es decir, evaluadores y evaluados intercambian su papel alternativamente. La coevaluación permite al alumno y al docente:

- Identificar los logros personales y grupales.
- Fomentar la participación, reflexión y crítica constructiva ante situaciones de aprendizaje.
- Mejorar la responsabilidad individual y de grupo.
- Emitir juicios valorativos acerca de otros en un ambiente de libertad, compromiso y respeto.

La **autoevaluación** se refiere a la valoración que hace el alumno sobre su propia actuación o desempeño y se refiere al grado de dominio de una competencia o resultado de aprendizaje alcanzado por él mismo. Le permite al alumno:

- Reconocer sus posibilidades y limitaciones, así como definir las acciones necesarias para mejorar su aprendizaje.

En el Apartado 9 de esta guía de evaluación se incluyen los lineamientos definidos de manera institucional para su aplicación. Es importante destacar que los planteles tienen la facultad de **instrumentar** estas modalidades de evaluación, de acuerdo con las condiciones particulares de su entorno.

**Actividades de Evaluación**

Los programas de estudio están conformados por Unidades de Aprendizaje (UA) que agrupan Resultados de Aprendizaje (RA) vinculados estrechamente y que requieren irse desarrollando paulatinamente. Dado que se establece un resultado, es necesario comprobar que efectivamente éste se ha alcanzado, de tal suerte que en la descripción de cada unidad se han definido las actividades de evaluación indispensables para evaluar los aprendizajes de cada uno de los RA que conforman las unidades.

Esto no implica que no se puedan desarrollar y evaluar otras actividades planteadas por el docente, pero es importante no confundir con las actividades de aprendizaje que realiza constantemente el alumno para contribuir a que logre su aprendizaje y que, aunque se evalúen con fines formativos, no se registran formalmente en el **Sistema de Administración Escolar SAE**. El **registro formal** procede sólo para las actividades descritas en los programas y planes de evaluación.

De esta manera, los RA tienen asignada una actividad de evaluación, considerando que puede haber casos en que se incluirán dos o más RA en una sola actividad de evaluación, cuando ésta sea integradora; misma a la que se le ha determinado una ponderación con respecto a la Unidad a la cual pertenece. Ésta a su vez, tiene una ponderación que, sumada con el resto de Unidades, **conforma el 100%.** Es decir, para considera que se ha adquirido la competencia correspondiente al módulo de que se trate, deberá **ir acumulando** dichos porcentajes a lo largo del período para esta en condiciones de acredita el mismo. Cada una de estas ponderaciones dependerá de la relevancia que tenga la AE con respecto al RA y éste a su vez, con respecto a la Unidad de Aprendizaje. Estas ponderaciones las asignará el especialista diseñador del programa de estudios.

La ponderación que se asigna en cada una de las actividades queda asimismo establecida en la **Tabla de ponderación**, la cual está desarrollada en una hoja de cálculo que permite, tanto al alumno como al docente, ir observando y calculando los avances en términos de porcentaje, que se van alcanzando (ver apartado 7 de esta guía).

Esta tabla de ponderación contiene los Resultados de Aprendizaje y las Unidades a las cuales pertenecen. Asimismo indica, en la columna de actividades de evaluación, la codificación asignada a ésta desde el programa de estudios y que a su vez queda vinculada al Sistema de Evaluación Escolar SAE. Las columnas de aspectos a evalúa, corresponden al tipo de aprendizaje que se evalúa: **C = conceptual; P = Procedimental y A = Actitudinal**. Las siguientes tres columnas indican, en términos de porcentaje: la primera el **peso específico** asignado desde el programa de estudios para esa actividad; la segunda, **peso logrado**, es el nivel que el alumno alcanzó con base en las evidencias o desempeños demostrados; la tercera, **peso acumulado**, se refiere a la suma de los porcentajes alcanzados en las diversas actividades de evaluación y que deberá acumula a lo largo del ciclo escolar.

Otro elemento que complementa a la matriz de ponderación es la **rúbrica o matriz de valoración**, que establece los **indicadores y criterios** a considerapara evaluar, ya sea un producto, un desempeño o una actitud y la cual se explicará a continuación.

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 toma en cuenta como **mínimo indispensable**para evalúa si se ha logrado el resultado de aprendizaje esperado y, por otro, los criterios o **niveles de calidad o satisfacción alcanzados**. En las celdas centrales se describen los criterios que se van a utilizapara evalúa esos indicadores, explicando cuáles son las características de cada uno.

Los criterios que se han establecido son: **Excelente**, en el cual, además de cumplir con los estándares o requisitos establecidos como necesarios en el logro del producto o desempeño, es propositivo, demuestra iniciativa y creatividad, o que va más allá de lo que se le solicita como mínimo, aportando

elementos adicionales en pro del indicador; **Suficiente**, si cumple con los estándares o requisitos establecidos como necesarios para demostrar que se ha desempeñado adecuadamente en la actividad o elaboración del producto. Es en este nivel en el que podemos decir que se ha adquirido la competencia. **Insuficiente**, para cuando no cumple con los estándares o requisitos mínimos establecidos para el desempeño o producto.

**Evaluación mediante la matriz de valoración o rúbrica**

Un punto medula en esta metodología es que al alumno se le proporcione el **Plan de evaluación**, integrado por la **Tabla de ponderación y las Rúbricas**, con el fin de que pueda conocer qué se le va a solicita y cuáles serán las características y niveles de calidad que deberá cumplir para demostrar que ha logrado los resultados de aprendizaje esperados. Asimismo, él tiene la posibilidad de autorregular su tiempo y esfuerzo para recupera los aprendizajes no logrados.

Como se plantea en los programas de estudio, en una **sesión de clase previa a finaliza la unidad**, el docente debe hacer una **sesión de recapitulación** con sus alumnos con el propósito de valora si se lograron los resultados esperados; con esto se pretende que el alumno tenga la oportunidad, en caso de no lograrlos, de rehacer su evidencia, realiza actividades adicionales o repetir su desempeño nuevamente, con el fin de recuperase de inmediato y no espera hasta que finalice el ciclo escolar acumulando deficiencias que lo pudiesen lleva a no logra finalmente la competencia del módulo y, por ende, no aprobarlo.

La matriz de valoración o rúbrica tiene asignadas a su vez valoraciones para cada indicador a evalúa, con lo que el docente tendrá los elementos para evaluar objetivamente los productos o desempeños de sus alumnos. Dichas valoraciones están también vinculadas al SAE y a la matriz de ponderación. Cabe señala que **el docente no tendrá que realizar operaciones matemáticas para el registro de los resultados de sus alumnos**, simplemente deberá maca en cada celda de la rúbrica aquélla que más se acerca a lo que realizó el alumno, ya sea en una hoja de cálculo que emite el SAE o bien, a través de la Web.

## 8. Tabla de ponderación

| UNIDAD | RA | ACTIVIDAD DE EVALUACIÓN | ASPECTOS A EVALUA | | | % Peso Específico | % Peso Logrado | % Peso Acumulado |
|---|---|---|---|---|---|---|---|---|
| | | | C | P | A | | | |
| **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 a los alertamientos que emite el equipo. | 1.1.1 | ▲ | ▲ | ▲ | 20% | | |
| | **1.2** Evalúa la integridad de la información y operación del equipo de cómputo conforme 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** Instala tecnología de seguridad protegiendo la información y equipo de cómputo contra amenazas a su integridad. | 2.2.1 | ▲ | ▲ | ▲ | 30% | | |
| **% PESO PARA LA UNIDAD** | | | | | | **55%** | | |
| **PESO TOTAL DEL MÓDULO** | | | | | | **100%** | | |

## 9. Materiales para el desarrollo de actividades de evaluación

## 10. Matriz de valoración ó rúbrica

### MATRIZ DE VALORACIÓN O RÚBRICA

| | | | | | |
|---|---|---|---|---|---|
| **Siglema:** | AHSH | **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 a los alertamientos que emite el equipo. | | | **Actividad de evaluación:** | 1.1.1 Identifica riesgos y amenazas en laseguridad del hardware y software en un equipo de cómputo, elaborando un reporte de resultados. |

| **INDICADORES** | **%** | **C R I T E R I O S** | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| **Identificación de riesgos en el equipo.** | **50%** | Utiliza comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware.<br>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.<br>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.<br>Responde en forma inmediata para | Utiliza comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware.<br>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.<br>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:<br>• Utilizar comandos de monitoreo para identificar el estado de: antivirus, cortafuegos y antimalware.<br>• 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.<br>• Identificar sitios de identidad |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| | | manejar situaciones imprevistas, durante la identificación de riesgos en el equipo. | | desconocida, que pueden atentar contra la seguridad del equipo, y determinar si son potencialmente una amenaza a la seguridad del equipo. |
| **Identificación de amenazas en hardware y software** | **50%** | Utiliza las herramientas de MSAT (evaluación de seguridad de Microsoft).<br>Utiliza las herramientas de IIS (herramienta de bloqueo).<br>Utiliza las herramientas del reporteador de puertos (portreporter).<br>Utiliza las herramientas del muestreo de seguridad de la red (networksecurityscan).<br>Reporta resultados obtenidos con el uso de las herramientas.<br>Realiza la interpretación de los resultados.<br>Acepta las observaciones y sugerencias brindadas por el docente y por sus compañeros para mejorar su trabajo. | Utiliza las herramientas de MSAT (evaluación de seguridad de Microsoft).<br>Utiliza las herramientas de IIS (herramienta de bloqueo).<br>Utiliza las herramientas del reporteador de puertos (portreporter).<br>Utiliza las herramientas del muestreo de seguridad de la red (networksecurityscan).<br>Reporta resultados obtenidos con el uso de las herramientas.<br>Realiza la interpretación de los resultados. | Omite alguna de las siguientes actividades:<br>• Utilizar las herramientas de MSAT (evaluación de seguridad de Microsoft).<br>• Utilizar las herramientas de IIS (herramienta de bloqueo).<br>• Utilizar las herramientas del reporteador de puertos (portreporter).<br>• Utilizar las herramientas del muestreo de seguridad de la red (networksecurityscan)<br>• Reportar resultados obtenidos con el uso de las herramientas.<br>• Realizar la interpretación de los resultados. |
| | **100%** | | | |

## MATRIZ DE VALORACIÓN O RÚBRICA

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Siglema:** | AHSH | **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 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** | **Suficiente** | **Insuficiente** |
| **Diagnóstico de amenazas a la información** | **45%** | 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.<br><br>Aplica la utilería igremote, explica su objetivo e interpreta los resultados en: virus, troyanos, r*ootkits g*usanos, s*pyware, malware, e*spionaje, modificación de información, spam y suplantación de identidad.<br><br>Ingresa al sitio http://www.rootkit.cl/hackingy utiliza sus técnicas y herramientas.<br><br>Busca en internet programas de | 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.<br><br>Aplica la utilería igremote, explica su objetivo e interpreta los resultados en: virus, troyanos, r*ootkits g*usanos, s*pyware, malware, e*spionaje, modificación de información, spam y suplantación de identidad.<br><br>Ingresa al sitio http://www.rootkit.cl/hacking y utiliza sus técnicas y herramientas.<br><br>Busca en internet programas de intrusión, identifica y describe lo que | Omite alguna de las siguientes actividades:<br><br>• 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.<br><br>• 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 |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| | | intrusión, identifica y describe lo que pueden hacer.<br>Utiliza las tecnologías de la información para procesar e interpretar información en el diagnóstico de este tipo de amenazas. | pueden hacer. | identidad.<br>• Ingresar al sitio http://www.rootkit.cl/hacking [12/10/15] y utilizar sus técnicas y herramientas.<br>• Buscar en internet programas de intrusión, identificar y describir lo que pueden hacer. |
| **Diagnóstico de riesgos originados por las debilidades de instalación** | **55%** | Diagnostica y describe los riesgos originados por debilidades de instalación de protocolos de red no necesarios.<br>Diagnostica y describe los riesgos originados por debilidades de instalación o actualización de la versión del BIOS.<br>Diagnostica y describe los riesgos originados por debilidades de instalación de servicios compartidos.<br>Diagnostica y describe los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados.<br>Es responsable con su trabajo y realiza sus labores con exactitud y precaución al diagnosticar riesgos originados por las debilidades de instalación. | Diagnostica y describe los riesgos originados por debilidades de instalación de protocolos de red no necesarios.<br>Diagnostica y describe los riesgos originados por debilidades de instalación o actualización de la versión del BIOS.<br>Diagnostica y describe los riesgos originados por debilidades de instalación de servicios compartidos.<br>Diagnostica y describe los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados. | Omite alguna de las siguientes actividades:<br>• Diagnosticar y describir los riesgos originados por debilidades de instalación de protocolos de red no necesarios.<br>• Diagnosticar y describir los riesgos originados por debilidades de instalación o actualización de la versión del BIOS.<br>• Diagnosticar y describir los riesgos originados por debilidades de instalación de servicios compartidos.<br>• Diagnosticar y describir los riesgos originados por debilidades de instalación de sistemas de seguridad no actualizados. |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | Excelente | Suficiente | Insuficiente |
| | 100% | | | |

## MATRIZ DE VALORACIÓN O RÚBRICA

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Siglema:** | AHSH | **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** | **Suficiente** | **Insuficiente** |
| **Recomendaciones contra vulnerabilidades** | **50%** | Recomienda medidas de protección y preservación de la información.<br>Autoriza y registra usuarios.<br>Controla el acceso a usuarios locales y remotos.<br>Establece certificados digitales y servidores de autentificación.<br>Administra contraseñas y reconocimiento de firmas manuscritas y huellas dactilares.<br>Describe los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya.<br>Se muestra seguro y convincente al hacer alguna recomendación contra las posibles vulnerabilidades a sus compañeros y el | Recomienda medidas de protección y preservación de la información.<br>Autoriza y registra usuarios.<br>Controla el acceso a usuarios locales y remotos.<br>Establece certificados digitales y servidores de autentificación.<br>Administra contraseñas y reconocimiento de firmas manuscritas y huellas dactilares.<br>Describe los resultados esperados de las recomendaciones, así como sus efectos secundarios cuando los haya. | Omite alguna de las siguientes actividades:<br>• Recomendar medidas de protección y preservación de la información.<br>• Autorizar y registrar usuarios.<br>• Controlar el acceso a usuarios locales y remotos.<br>• Establecer certificados digitales y servidores de autentificación.<br>• Administrar contraseñas y reconocimiento de firmas manuscritas y huellas dactilares.<br>• Describir los resultados esperados de las |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| | | docente. | | recomendaciones, así como sus efectos secundarios cuando los haya. |
| **Definición de acciones de seguridad** | **50%** | Propone políticas de seguridad describiendo su validez y efectos.<br>Establece protocolos por denegación de servicio o modificación al contenido de mensajes.<br>Define criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores.<br>Previene ataques que realicen una llamada al sistema operativo.<br>Previene ataques que traten de accesar a carpetas dentro del servidor web<br>Previene ataques que exploten la identificación de URL<br>Elabora el plan de acción como reporte.<br>Recomienda reglas, procedimientos y actitudes relativas a la protección de la información. | Propone políticas de seguridad describiendo su validez y efectos.<br>Establece protocolos por denegación de servicio o modificación al contenido de mensajes.<br>Define criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores.<br>Previene ataques que realicen una llamada al sistema operativo.<br>Previene ataques que traten de accesar a carpetas dentro del servidor web<br>Previene ataques que exploten la identificación de URL<br>Elabora el plan de acción como reporte. | Omite alguna de las siguientes actividades:<br>• Proponer políticas de seguridad describiendo su validez y efectos.<br>• Establecer protocolos por denegación de servicio o modificación al contenido de mensajes.<br>• Definir criterios para identificar la suplantación de actividad o conexión no autorizada a equipos y servidores.<br>• Prevenir ataques que realicen una llamada al sistema operativo.<br>• Prevenir ataques que traten de accesar a carpetas dentro del servidor web<br>• Prevenir ataques que exploten la identificación de URL.<br>• Elaborar el plan de acción como reporte. |
| | **100%** | | | |

## MATRIZ DE VALORACIÓN O RÚBRICA

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

| **INDICADORES** | **%** | **C R I T E R I O S** | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| **Instalación de herramientas de seguridad en redes.** | **25%** | Instala, ejecuta y describe la forma de implantar acciones en la instalación de tecnología de seguridad en redes.<br><br>Considera restricciones a los dispositivos ADSL (hardening).<br><br>Instala herramientas de seguridad en redes VPN y Windows.<br><br>Identifica la acción más sólida en la seguridad de redes.<br><br>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.<br><br>Considera restricciones a los dispositivos ADSL (hardening).<br><br>Instala herramientas de seguridad en redes VPN y Windows.<br><br>Identifica la acción más sólida en la seguridad de redes. | Omite alguna de las siguientes actividades:<br>• Instalar, ejecutar y describir la forma de implantar acciones en la instalación de tecnología de seguridad en redes.<br>• Considerar restricciones a los dispositivos ADSL (hardening).<br>• Instalar herramientas de seguridad en redes VPN y Windows.<br>• Identificar la acción más sólida en la seguridad de redes. |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| **Instalación de seguridad en componentes físicos de oficina.** | **30%** | Considera en la instalación de tecnología de seguridad en componentes físicos de oficinas:<br>• Protocolo WEP<br>• Protocolo WPA<br>• Estándar RSN<br>• Estándar 802.1x<br>Detecta intentos de intrusión.<br>Separa la red inalámbrica de la red local interna.<br>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. | Considera en la instalación de tecnología de seguridad en componentes físicos de oficinas:<br>• Protocolo WEP<br>• Protocolo WPA<br>• Estándar RSN<br>• Estándar 802.1x<br>Detecta intentos de intrusión.<br>Separa la red inalámbrica de la red local interna. | Omite alguna de las siguientes actividades:<br>• Considerar en la instalación de tecnología de seguridad en componentes físicos de oficinas: Protocolos WEP y WPA y los estándares RSN y 802.1x.<br>• Detectar intentos de intrusión.<br>• 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.<br>Actualiza parches de seguridad y control de cookies.<br>Realiza el control en la descarga desde internet.<br>Evade sitios dudosos.<br>Evalúa enlaces incluidos en correo | Ejecuta, describe y reporta la implantación de acciones de seguridad.<br>Actualiza parches de seguridad y control de cookies.<br>Realiza el control en la descarga desde internet.<br>Evade sitios dudosos.<br>Evalúa enlaces incluidos en correo | Omite alguna de las siguientes actividades:<br>• Ejecutar, describir y reportar la implantación de acciones de seguridad.<br>• Actualizar parches de seguridad y control de cookies. |

| INDICADORES | % | C R I T E R I O S | | |
|---|---|---|---|---|
| | | **Excelente** | **Suficiente** | **Insuficiente** |
| | | electrónico.<br>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. | electrónico. | • Realizar el control en la descarga desde internet.<br>• Evadir sitios dudosos.<br>• Evaluar enlaces incluidos en correo electrónico. |
| **Coevaluación**<br>1. Enfrenta las dificultades que se le presentan y es consciente de sus valores, fortalezas y debilidades.<br>5. Sigue instrucciones y procedimientos de manera reflexiva, comprendiendo como cada uno de sus pasos contribuye al alcance de un objetivo. | **10%** | Detecta los obstáculos para alcanzar sus metas y busca la forma y los recursos para superarlos con responsabilidad.<br>Usa sus conocimientos para evitar riesgos o daños.<br>Atiende las instrucciones y los procedimientos para alcanzar los objetivos planteados.<br>Evalúa el trabajo realizado e identifica oportunidades de mejora. | Detecta los obstáculos para alcanzar sus metas y busca la forma y los recursos para superarlos con responsabilidad.<br>Atiende las instrucciones y los procedimientos para alcanzar los objetivos planteados. | Omite alguna de las siguientes actividades:<br>• Detectar los obstáculos para alcanzar sus metas y buscar la forma y los recursos para superarlos con responsabilidad.<br>• Atender las instrucciones y los procedimientos para alcanzar los objetivos planteados. |
| | **100%** | | | |