I. Guía Pedagógica del Módulo
Aplicación de la seguridad informática

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

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.

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 más presentaciones 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 de experiencias 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. 1

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 participación de 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

En un mundo globalizado, es necesario que el estudiante obtenga las herramientas útiles para desarrollar su labor profesional al momento de dejar el aula, es por ello que el módulo de **Aplicación de la seguridad informática**, contribuye a la formación del conocimiento y aplicación de los parámetros y estándares de protección utilizados a través de herramientas informáticas que cuiden de la integridad de la información almacenada en equipos de cómputo y de comunicaciones, así como en dispositivos internos o externos.

Asimismo, las estrategias de aprendizaje aquí planteadas, van en caminadas a dotar al estudiante del dominio para realizar las actividades correspondientes a una eficiente administración de seguridad informática.

La formación profesional del PT y PT-B en Informática, está diseñada con un enfoque de procesos, lo cual implica un desarrollo en la adquisición de competencias profesionales para establecer modelos de seguridad, identificar situaciones de contingencia e implementar acciones correctivas que contribuyan a resguardar la información de ataques de virus, hackers y de todos aquellos procedimientos manuales o automáticos encaminados a extraer de manera no autorizada la información; actuando con responsabilidad, eficacia y calidad, en tiempo y forma.

Además, estas competencias se complementan con la incorporación de otras competencias básicas y genéricas que refuerzan la formación tecnológica y científica, y fortalecen la formación integral de los estudiantes; que los prepara para comprender los procesos productivos en los que está involucrado para enriquecerlos, transformarlos, resolver problemas, ejercer la toma de decisiones y desempeñarse en diferentes ambientes laborales, con una actitud creadora, crítica, responsable y propositiva; de la misma manera, fomenta el trabajo en equipo, el desarrollo pleno de su potencial en los ámbitos profesional y personal y la convivencia de manera armónica con el medio ambiente y la sociedad.

La tarea docente en este módulo tendrá que diversificarse, a fin de que los docentes realicen funciones preceptoras, las que consistirán en la guía y acompañamiento de los alumnos durante su proceso de formación académica y personal y en la definición de estrategias de participación que fomenten su desarrollo integral, adquiriendo conocimientos, que durante la interacción con usuarios de los sistemas, pueda poner en práctica para proteger su información.

Por último, es necesario que al final de cada unidad de aprendizaje se considere una sesión de clase en la cual se realice la recapitulación de los aprendizajes logrados, en lo general, por los alumnos, con el propósito de verificar que éstos se han alcanzado o, en caso contrario, determinar las acciones de mejora pertinentes. Cabe señalar que en esta sesión el alumno que haya obtenido insuficiencia en sus actividades de evaluación o desee mejorar su resultado, tendrá la oportunidad de entregar nuevas evidencias.

5. Orientaciones didácticas y estrategias de aprendizaje por unidad

Unidad I	Aplica estándares de protección de la información.

Orientaciones Didácticas

La unidad uno está avocada a la aplicación de estándares de seguridad informática de acuerdo con riesgos identificados en el marco de las buenas prácticas del uso de la tecnología. Se incluyen en esta unidad resultados de aprendizaje asociados al desarrollo de competencias necesarias para determinar riesgos de seguridad informática y la elaboración de un plan de seguridad acorde a estándares de protección. con base en las características del equipo y las necesidades del usuario. El desarrollo de esta unidad proporcionará al alumno elementos básicos que le permitirán desarrollar las actividades y prácticas propias de esta competencia y apoyar a la unidad subsecuente, por eso se propone que el docente lleve a cabo lo siguiente:

- Iniciar el módulo, fijando las expectativas, los resultados esperados y beneficios que obtendrá el alumno al concluir satisfactoriamente el programa.
- .Explicar el propósito, mapa y contenidos a trabajar durante el semestre, y la forma en que se abordaran las unidades.
- Realizar una técnica grupal para asegurar la integración del grupo y generar un clima de confianza que les permita a todos los alumnos expresarse de manera libre y espontánea, con la seguridad de que cuentan el respeto y colaboración de sus compañeros.
- Enfatizar la importancia de la responsabilidad (del alumno) en el cumplimiento de tareas a que se compromete, en especial cuando trabaja en equipo y su contribución impacta el desempeño grupal.
- Al final de cada sesión o resultado especifico de acuerdo a su plan de trabajo, efectuar la recapitulación de lo aprendido y verificación oportuna del aprovechamiento de los integrantes del grupo.
- Revisar que el alumno aplique las competencias adquiridas en previos módulos respecto a sistemas y aplicaciones en informática.
- Incentivar el razonamiento lógico - práctico individual y por equipo de trabajo.
- Fomentar el pensamiento analítico, inductivos/deductivos en el aprendizaje, relacionando los temas de este módulo, con las medidas de seguridad que adoptamos en otras actividades, como el manejo de documentos ya impresos, el uso de tarjetas de crédito, etc.
- Formar equipos de trabajo y fomentar una activa obtención de información para su presentación de manera estructurada.

- Se recomienda abordar el primer resultado de aprendizaje mediante labores de investigación realizando consultas a materiales bibliográficos e internet, y la exposición de temas ante el grupo, con el objetivo de formar su criterio respecto a los riesgos informáticos a que están expuestas las personas y usuarios de una empresa, mediante la contrastación de ideas con sus compañeros. Para el manejo de cuentas y de carpetas, se recomienda el uso del laboratorio para la revisión de las capacidades disponibles en el sistema operativo de red, al igual que en el sistema operativo propio de la computadora.
- Para el segundo resultado de aprendizaje, llamado: elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección, se sugiere la activa interacción en equipos de trabajo, para la generación de un documento denominado plan de seguridad informática. Durante el desarrollo de estas actividades es conveniente que el alumno tenga contacto con una persona responsable de los sistemas y redes informáticos de una empresa, de la institución o de algún centro de negocios para incluir dentro de su documento los aspectos que vayan cambiando por los avances tecnológicos y en relación a la normatividad aplicable más reciente.
- Asimismo, es necesario el revisar la normatividad correspondiente con el tema y definir cual de ella es la que consideran que aplican o deben de aplicar las empresas de su comunidad.
- Facilitar la visita a un centro de cómputo de una empresa, con el objetivo de entrevistarse con el responsable de la seguridad informática y conocer los estándares que utilizan, la forma en que implementan su seguridad y si han experimentado ataques informáticos, así como la solución que han dado a éstos problemas.

Fortalece las siguientes competencias transversales

- Se conoce y valora a sí mismo y aborda problemas y retos teniendo en cuenta los objetivos que persigue, analizando críticamente los factores que influyen en la prevención y medidas de seguridad de equipos y recursos informáticos.
- Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados mediante el manejo de las tecnologías de la información y la comunicación para obtener información sobre estándares de protección de información y expresar ideas.

Estrategias de Aprendizaje	Recursos Académicos
• Participar en el encuadre del programa al inicio de la unidad, aportando preguntas y propuestas para tomar acuerdos sobre la forma de trabajar durante el desarrollo del módulo, con la finalidad de cumplir con el objetivo planteado. • Elaborar una bitácora para el registro de las actividades en clase, de manera que se pueda recurrir a ella de manera constante, ésta puede ser en papel o digital. • Organizar equipo de dos o más integrantes para la realización de trabajos y tareas, asignando responsabilidades y adquiriendo compromisos por los resultados finales.	**Materiales de apoyo:** • Licencia de antivirus para Windows • Manuales operativos de las herramientas de seguridad utilizadas. **Básica:** • Hernández Enrique, Auditoria **y seguridad de la función informática informática** México,

- Recopilar información en fuentes confiables de universidades, instituciones dedicadas al ámbito informático.
- Trabajar en equipo y configura un mecanismo en Internet para interactuar entre ellos y centralizar toda la información que generan, comparten y utilizan.
- Realizar labores de investigación en fuentes bibliográficas y sitios de Internet para identificar todos los riesgos informáticos a que está expuesta una persona y una empresa. Identificar las fuentes de consulta y verificar que la información considerada es actual, reciente y su contenido aporta información puntual.
- Realizar búsquedas de información en organizaciones de seguridad informática extranjeras y en idioma Inglés con el objetivo de familiarizarse con los términos en dicho idioma, practicar otra competencia transversal y enriquecer su investigación con información diferente y quizá no disponible en español
- Realizar la actividad 1 "Identifica riesgos de seguridad"
- Analizar casos de problemas de seguridad sufridos por empresas y el impacto que tuvieron.
- **Realizar la actividad de evaluación 1.1.1 donde elabora un informe del análisis de riesgos de seguridad informática de una organización mediana o grande, detectando riesgos de acuerdo con el impacto en la confidencialidad, integridad o disponibilidad de la información.**
- Visitar una empresa para conocer su centro de cómputo y conocer la forma en que diseñaron su plan de seguridad informática, los estándares que tomaron en cuenta y sus experiencias respecto a ataques sufridos.
- Interactuar con los otros equipos de trabajo, mediante internet y en clase, para contrastar sus investigaciones.
- Efectuar un levantamiento por grupos de trabajo de los recursos informáticos (y sus características) con que cuenta en su laboratorio.
- Realizar la actividad 2 "Levantamiento de información empresarial con fines de protección informática".
- Realizar la actividad 3 "Mejores prácticas para protección informática".
- Elaborar presentaciones ejecutivas en clase, de sus resultados y conclusiones.

Alfaomega, 2011

- Wlalker, Andy, **Seguridad, Spam, Spyware y Virus**, 1a. Edición, España, Anaya Multimedia, 2006.
- Terán David, **Administración estrategica de la función informática Alfaomega, 2011**

Complementaria:

- Piattini, Mario; Del Peso, Emilio; del Peso, Mar, **Auditoría De Tecnologías Y Sistemas De Información**, México, Alfaomega, 2008
- Piattini, Mario; Del Peso, Emilio, **Auditoría Informática - Un Enfoque Práctico** - 2ª ed. Ampliada Y Revisada, México, Alfaomega, 2001
- Ramos Varón, Antonio Angel, **Protege tu PC,** 1a. Edición, España, Anaya Multimedia, 2004.

Paginas Web:

- **Biblioteca digital CONALEP.- Cursos Calidad, Seguridad Informática Disponible en: http://sied.conalep.edu.mx/bv3/** y http://www.cursos-en-mexico.com.mx/cursos/calidad-seguridad-informatica?gclid=CKnwlpTPjKoCFU976wodnE6rzA **(14/07/15),**
- Definicion de Seguridad informática - ¿qué es Seguridad informática? Concepto del término seguridad informática **Disponible en:** http://www.alegsa.com.ar/Dic/seguridad%20informatica.php **(14/07/15),**

• **Realizar la actividad de evaluación 1.2.1. donde elabora un plan de seguridad informática basado en estándares internacionales estableciendo mecanismos de protección a la información, así como métricas de evaluación del mismo.** • Generar documentos, como el plan de seguridad de cómputo y otros documentos de los módulos de este semestre, aplicando las capacidades avanzadas del presentador gráfico y procesador de palabras • Comentar en clase los resultados de las actividades de evaluación realizadas, efectuando una coevaluación enfocada tanto al proceso ejecutado como a los resultados obtenidos	

Unidad 2	Administra herramientas de seguridad informática.

Orientaciones Didácticas

Esta subsecuente unidad se enfoca en la administración de herramientas de seguridad informática que incluye resultados de aprendizaje asociados al desarrollo de competencias necesarias que nos permitan administrar las herramientas de seguridad mediante su instalación, configuración y seguimiento a la operación. El desarrollo de esta unidad proporcionará al alumno elementos básicos que le permitirán desarrollar las actividades y prácticas propias de esta competencia, por eso se propone que el docente lleve a cabo lo siguiente:

- Explicar el propósito y la forma en que se abordará la unidad.
- Enfatizar la importancia de la responsabilidad (del alumno) en el cumplimiento de tareas a que se compromete, en especial cuando trabaja en equipo y su contribución impacta el desempeño grupal.
- Al final de cada sesión o resultado especifico de acuerdo a su plan de trabajo, efectuar la recapitulación de lo aprendido y verificación oportuna del aprovechamiento de los integrantes del grupo.
- Revisar que el alumno aplique las competencias adquiridas en previos módulos respecto a sistemas y aplicaciones en informática.
- Formar equipos de trabajo y fomentar una activa obtención de información para su presentación de manera estructurada.
- Incentivar el razonamiento lógico - práctico de manera individual y por equipo de trabajo, para la definición de elementos de verificación de auditoría informática.
- Orientar en la eficiente instalación de las herramientas de seguridad.
- Facilitar la posibilidad de aplicar el aprendizaje del alumno en una empresa, negocio o ámbito académico.
- Se recomienda abordar el primer resultado de aprendizaje mediante la activa interacción en equipos de trabajo, verificando que su laboratorio cuenta con las aplicaciones necesarias (ya sea licenciadas o bajando software libre) para la instalación y configuración de herramientas de seguridad informática, de acuerdo a lo especificado en el modelo o plan de seguridad de cómputo.
- Para el segundo resultado de aprendizaje, se recomienda que un equipo de trabajo busque vulnerar la seguridad establecida por otro equipo diferente, documentando sus resultados, de tal forma que cuando el equipo atacado genere y analice sus reportes, pueda determinar la efectividad de sus herramientas, tanto para mantener la seguridad, como para detectar los ataques sufridos.
- Se recomienda revisar las mejores prácticas desarrolladas por despachos enfocados a funciones de auditorías y definir cuales son aplicables en las empresas de su entorno.
- Facilitar la entrevista con especialistas en certificaciones en seguridad y auditorías, de la forma en que despliegan estos trabajos y si posible, el análisis de algunos ejemplos y casos de estudio.

- Se recomienda abordar el tercer resultado de aprendizaje mediante labores de investigación en sitios de Internet en español o inglés y mediante la interacción (del alumno) con profesionales; así como utilizar el laboratorio para aplicar los procedimientos sobre las computadoras y herramientas de seguridad configuradas; también.

Fortalece las siguientes competencias transversales

- Sustenta una postura personal sobre temas de interés y relevancia general, considerando otros puntos de vista de manera crítica y reflexiva, eligiendo fuentes de información más relevantes sobre estándares y buenas prácticas de seguridad en cómputo y discrimina entre ellas de acuerdo a su relevancia y confiabilidad.
- Participa y colabora de manera efectiva en equipos diversos. proponiendo maneras de prevenir y solucionar un problemas relacionados a riesgos mediante el desarrollo de un plan de contingencias, definiendo un curso de acción con pasos específicos.

Estrategias de Aprendizaje	Recursos Académicos
• Participar en el encuadre del programa al inicio de la unidad, aportando preguntas y propuestas para tomar acuerdos sobre la forma de trabajar durante el desarrollo del módulo, con la finalidad de cumplir con el objetivo planteado. • Realiza la práctica número 1 “Configuración de parámetros de protección”. • Trabajar en equipo de dos o tres personas considerando los recursos de su laboratorio de cómputo o informática, instalar y probar diferentes herramientas de seguridad informática. • Identificar los parámetros de seguridad que ha configurado y experimenta su comportamiento. • Instalar y configurar herramientas informáticas acorde con los estándares y buenas prácticas de seguridad en cómputo. • Realiza la práctica número 2 “Ejecución de herramientas de seguridad informática”. • Con la guía del docente, se asigna al estudiante y su equipo de trabajo, el entorno de seguridad configurado por otro equipo, con el objetivo de vulnerar su seguridad, ya sea mediante intentos de acceso no autorizado, sustraer información, suplantar usuarios, etc. • **Realizar la actividad de evaluación 2.1.1. donde instala y configura herramientas informáticas de manera segura y en apego al manual determinado.** • Da seguimiento a la operación de las herramientas informáticas configuradas en su plan y genera los reportes de su operación, después de que otro equipo de trabajo intentó romper	**Materiales de apoyo:** • Licencia de antivirus para Windows • Manuales operativos de las herramientas de seguridad utilizadas. **Básica:** • Terán David, **Administración estrategica de la función informática** Alfaomega, 2011 **Complementaria:** • Piattini, Mario; Del Peso, Emilio; del Peso, Mar, **Auditoría De Tecnologías Y Sistemas De Información**, México, Alfaomega, 2008 **Páginas Web:** • **Biblioteca digital CONALEP.- Cursos Calidad, Seguridad Informática Disponible en: http://sied.conalep.edu.mx/bv3** y http://www.cursos-en-mexico.com.mx/cursos/calidad-seguridad-informatica?gclid=CKnwlpTPjKoCFU976wodnE

su seguridad. • Realiza la actividad 4 donde “Administra herramientas de seguridad informática”. • Realizar análisis comparativos, considerando los reportes generados por las herramientas y con las acciones emprendidas por el equipo de trabajo ‘atacante’. • Elaborar documentos descriptivos, de la efectividad de las herramientas y de los cambios a realizar para aumentar la efectividad del plan de seguridad. • Realiza la actividad 5 donde “Monitoreo de herramientas de protección”. • De acuerdo a las posibilidades, aplica lo aprendido en la configuración de seguridad, en tu equipo de cómputo personal y si tienes oportunidad en una empresa. • **Realizar la actividad de evaluación 2.2.1. donde monitorea la operación de las herramientas informáticas a fin de garantizar su funcionamiento.** • Utilizar el laboratorio de cómputo o informática para aplicar el proceso de revisión del plan de seguridad configurado en la unidad de aprendizaje anterior, determinando las modificaciones necesarias al plan y sus herramientas. • Realiza la práctica número 3 “Interpretación de estadísticas y resultados obtenidos con las herramientas de seguridad informática”. • Realiza la práctica número 4 “Afinación de parámetros de configuración de herramientas de seguridad informática”. • **Realizar la actividad de evaluación 2.3.1 donde revisa las configuraciones de equipos y redes de comunicación evaluando el cumplimiento de las políticas del plan de seguridad, así como determinar nuevos requerimientos.** • Finalizar el proceso de la seguridad, aplicando en el laboratorio, los cambios necesarios para mantener la seguridad, de acuerdo a resultados obtenidos. • **Realizar la actividad de evaluación 2.3.2 donde modifica la configuración de las herramientas de seguridad informática e/o instala herramientas de acuerdo con nuevos requerimientos** • Participar en el cierre del módulo a partir de la recapitulación y conclusiones obtenidas no solamente en esta unidad sino en la anterior que la precede, para obtener nuevas experiencias adquiridas en su futuro quehacer profesional.	6rzA **(14/07/15),**

6. Prácticas/Ejercicios /Problemas/Actividades

Nombre del Alumno:		**Grupo:**	
Unidad de Aprendizaje 1:	Aplica estándares de protección de la información		
Resultado de Aprendizaje:	Determina riesgos de seguridad informática con base en las características del equipo y las necesidades del usuario.		
Actividad núm. 1:	Identifica riesgos de seguridad		

NOTA El docente organizará equipos de trabajo y adecua la actividad de acuerdo con los recursos con los que disponga.

Instrucciones:

- Clasifica, en equipo de trabajo, los riesgos informáticos a que esta expuesta una empresa y realiza una breve descripción de cada uno de ellos, considerando:
  - Los riesgos lógicos y qué parámetros los caracterizan.
    -Códigos maliciosos.
    -Spam.
    -Piratería.
    -Fuga de información.
    -Ingeniería social.
    -Intrusos informáticos
  - Los riesgos físicos y los parámetros que los caracterizan.
- Genera una tabla de riesgos, y en conjunto con las generadas por otros equipos de trabajo, se exponen en clase y mediante un análisis comparativo, genera una tabla común y enriquecida de riesgos.

Nombre del Alumno:		**Grupo:**	

Unidad de Aprendizaje 1:	Aplica estándares de protección de la información.
Resultado de Aprendizaje:	Elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección.
Actividad núm. 2:	Levantamiento de información empresarial con fines de protección informática.

NOTA El docente organizará equipos de trabajo y adecua la actividad de acuerdo con los recursos con los que disponga.

Instrucciones:

- Define en clase, con ayuda del docente, la información a revisar para determinar el grado de riesgo en una empresa, considerando:
  - Procesos principales de la empresa.
  - Políticas aplicadas
    - De cuenta
    - De auditoría
    - Restricciones a usuarios
    - Restricciones de software
    - Firewall
    - Antivirus
    - Antispyware
    - Permisos en carpetas y documentos compartidos
    - Actualizaciones de sistema operativo y aplicaciones.
    - Respaldos de información

Nombre del Alumno:		**Grupo:**	
Unidad de Aprendizaje 1:	Aplica estándares de protección de la información		
Resultado de Aprendizaje:	Elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección.		
Actividad núm. 3:	Mejores prácticas para protección informática		

NOTA El docente organizará equipos de trabajo y adecua la actividad de acuerdo con los recursos con los que disponga.

Instrucciones:

1. Integra equipos de trabajo de dos o tres personas, de acuerdo con la disponibilidad de equipos de cómputo.
2. Selecciona del siguiente listado uno de los estándares o mejores prácticas para realizar una investigación de sus características.
3. Para su asignación se recomienda una dinámica de integración, por ejemplo un sorteo.
    - ITIL
    - EII
    - Cobit
    - ISM3
    - BS 17799
    - Serie ISO 27000
    - ISO 20000
- Realiza la búsqueda de información en internet correspondiente al objetivo, enfoque, alcance y características principales del estándar asignado.
- Elabora una síntesis de la información encontrada. Recuerda que se tiene que leer y decidir que información es relevante, eliminando aquella se que repite o que no aporta nada a lo que se pretende transmitir. (sintetizar no es cortar y pegar)
- Comparte la información con la obtenida por los otros equipos y realiza un análisis comparativo, en plenaria.

4. Con lo anterior, genera el plan inicial de seguridad, en el cual define qué se va a proteger y contra qué, el personal responsable y las actividades que realiza en el proceso de seguridad, para la ejecución del plan.
5. En clase, expone sus dudas, observaciones y consideraciones, de acuerdo a su análisis comparativo, y recibe retroalimentación.

Unidad de Aprendizaje:	Administra herramientas de seguridad informática	Número:	2
Práctica:	Configuración de parámetros de protección	Número:	1
Propósito de la práctica:	Usar la aplicación y forma de configurar los parámetros de protección de las herramientas de seguridad informática.		
Escenario:	Laboratorio de cómputo o informática.	Duración	3 horas

Materiales, Herramientas, Instrumental, Maquinaria y Equipo	**Desempeños**
• Equipo de cómputo Core Duo o superior • Conexión de internet • Sistema operativo windows xp o superior. • Software: Antivirus (mc affe, panda, BitDefender o cualquiera del que se disponga • Dispositivo de almacenamiento (USB)	• Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje **NOTA al** docente: Coordinará la realización de la práctica y organizará equipos de trabajo. **NOTA al alumno:** Realizará un respaldo de la información que generes en el centro de cómputo de tu escuela con algún dispositivo de almacenamiento. 1. Verifica que el equipo de cómputo esté conectado a la corriente eléctrica. 2. Verifica que haya corriente eléctrica en el contacto. 3. Prende el equipo de cómputo de acuerdo al manual del fabricante. 4. Verifica que el equipo de cómputo tenga instalado el sistema operativo Windows XP o superior. 5. Introduce el software antivirus en el equipo de cómputo. 6. Sigue las instrucciones de instalación del software antivirus. 7. Revisa los parámetros de configuración predeterminados que presenta el software referentes a: ▪ Antivirus ▪ Cortafuegos ▪ Antispam ▪ Antispyware ▪ Ejecución automática al momento de encender el equipo

	▪ Niveles de protección medio ▪ Actualización activada ▪ Periodicidad ▪ Manejo de elementos de pop ups abiertos 8. Documenta la configuración de los parámetros predeterminados. 9. Identifica el desempeño del equipo de acuerdo a los parámetros predeterminados. 10. Modifica los parámetros de configuración predeterminados, considerando lo siguiente: ▪ Ejecución manual ▪ Niveles de protección bajo ▪ Actualización desactivada ▪ Manejo de elementos pop ups cerrados 11. Identifica y revisa los avisos de operación del antivirus correspondiente a los cambios efectuados. 12. Cierra la sesión de usuario del equipo y reiniciarlo. 13. Evalúa el desempeño del equipo de acuerdo a los parámetros modificados, ya que en general a menor protección menor uso de recursos del equipo de cómputo con un mayor riesgo de seguridad. 14. De acuerdo a la documentación de la configuración predeterminada, regresa los parámetros a su estado inicial. 15. Cierra la sesión de trabajo del software antivirus 16. Apaga apropiadamente el equipo de cómputo una vez que se haya concluido la práctica. 17. Documenta los resultados obtenidos al cambiar los parámetros de configuración.  ADVERTENCIA DE RIESGO ELÉCTRICO

Unidad de Aprendizaje:	Administra herramientas de seguridad informática.	Número:	2
Práctica:	Ejecución de herramientas de seguridad informática	Número:	2
Propósito de la práctica:	Realizar la ejecución práctica de las herramientas de seguridad informáticas indispensables para proteger el equipo de cómputo y la integridad de la información almacenada en el mismo.		
Escenario:	Laboratorio de cómputo o informática	Duración	3 horas

Materiales, Herramientas, Instrumental, Maquinaria y Equipo	Desempeños
• Equipo de cómputo Core Duo o superior • Conexión de internet • Sistema operativo windows xp o superior. • Software: Antivirus (mc affe, panda, BitDefender o cualquiera del que se disponga • Dispositivo de almacenamiento (USB)	• Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje **NOTA al** docente: Coordinará la realización de la práctica y organizará equipos de trabajo. **NOTA al alumno:** Realizará un respaldo de la información que generes en el centro de cómputo de tu escuela con algún dispositivo de almacenamiento. 1. Verifica que el equipo de cómputo esté conectado a la corriente eléctrica. 2. Verifica que haya corriente eléctrica en el contacto. 3. Prende el equipo de cómputo de acuerdo al manual del fabricante. 4. Verifica que el equipo de cómputo tenga instalado el sistema operativo Windows XP o superior. 5. Verifica que el equipo de cómputo tenga instalado un software antivirus. 6. Ejecuta la revisión de virus en el equipo de cómputo en la unidad C. 7. Identifica los virus detectados por el software antivirus, obteniendo en internet la información referente. 8. Investiga si existen otras alternativas de software antivirus que sean más eficientes que el que utilizaste en la práctica a fin de identificar las herramientas de seguridad informáticas más adecuadas en cada situación. 9. Documenta los resultados obtenidos en la práctica.

	10. Ejecuta la operación de limpieza y cuarentena de los virus detectados. 11. Cierra la sesión de trabajo del software antivirus 12. Apaga apropiadamente el equipo de cómputo una vez que se haya concluido la práctica.  ADVERTENCIA DE RIESGO ELÉCTRICO

Nombre del Alumno:		**Grupo:**	

Unidad de Aprendizaje 2:	Administra herramientas de seguridad informática.
Resultado de Aprendizaje:	Instala y configura herramientas informáticas acorde con los estándares y buenas prácticas de seguridad en cómputo.
Actividad núm. 4:	Aplicación de herramientas de seguridad.

NOTA El docente organizará equipos de trabajo y adecua la actividad de acuerdo con los recursos con los que disponga.

Instrucciones:

1. Determina las herramientas de seguridad informática que utilizará, mediante la interacción con su equipo de trabajo, considerando los requerimientos de
   - El ambiente local de cómputo.
   - El ambiente de comunicación al exterior.
2. Genera una lista de herramientas y componentes que instalará.
3. .Expone al grupo, la justificación de dichas herramientas de acuerdo al plan de seguridad considerado, mediante una presentación con el uso del presentador gráfico.
4. Cada equipo de trabajo, instala algunas de las herramientas de seguridad, observando todas las indicaciones y requisitos establecidos en los manuales correspondientes.
5. Comparte con el grupo su experiencia de instalación y documenta los procedimientos realizados y requerimientos considerados, para cada herramienta.
6. Elabora una lista de parámetros que instaló con los valores o datos que correspondan, para satisfacer los requerimientos del plan de seguridad.
7. Realiza, con su equipo de trabajo y con ayuda del presentador gráfico, una presentación al grupo con el reporte de las configuraciones consideradas y participa en el análisis y discusión para completar las configuraciones que incluyan :
   - El sistema operativo y servidores.
   - El manejo de cuentas.
   - El manejo de carpetas y archivos compartidos.
   - EL manejo de antivirus y spyware.
   - Firewall local y perimetral.

- Detección de intrusos.

8. Define la bitácora para registrar:
   - Quien accesó y sus comentarios.
   - Que acciones y comandos ejecutó.
   - Cuando lo realizó (fecha y hora).
9. Configura los parámetros de las herramientas que instaló.
10. Analiza y define, con su equipo de trabajo, la forma de intentar violar la seguridad de las herramientas instaladas por otros equipos e intenta romper dicha seguridad establecida.

Para monitorear la actividad de las herramientas de seguridad, se recomienda lo realice un equipo diferente al que lo instaló; así, el alumno práctica y genera la habilidad para manejar las diversas herramientas.

- Realiza, de acuerdo al manual de la herramienta, y de las especificaciones en el plan de seguridad, la obtención de reportes disponibles.
- Busca en los reportes generados, las actividades detectadas de violación de la seguridad.
- Genera, con el procesador de texto, un documento profesional de los reportes obtenidos y su interpretación, y lo distribuye a los equipos restantes.
- En clase, expone sus resultados y resuelve sus dudas.
- Si la empresa entrevistada lo permite, el alumno trabaja en la configuración de herramientas de acuerdo al plan de esa empresa.

Nombre del Alumno:		**Grupo:**	

Unidad de Aprendizaje 2:	Administra herramientas de seguridad informática.

Resultado de Aprendizaje:	Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado.

Actividad núm. 5:	Monitoreo de herramientas de protección.

NOTA El docente organizará equipos de trabajo y adecua la actividad de acuerdo con los recursos con los que disponga.

Instrucciones:

Para monitorear la actividad de las herramientas de seguridad, se recomienda lo realice un equipo diferente al que lo instaló; así, el alumno practica y genera la habilidad y conocimiento para manejar las diversas herramientas.

- Realiza, de acuerdo al manual de la herramienta, y de las especificaciones en el plan de seguridad, la obtención de reportes disponibles.
- Busca en los reportes generados, las actividades detectadas de violación de la seguridad.
- Genera, con el procesador de texto, un documento con información de los reportes obtenidos y su interpretación, y lo distribuye a los equipos restantes, mediante el mecanismo de colaboración en internet.
- En clase, expone sus resultados y resuelve sus dudas.
- Dentro de las posibilidades, el alumno trabaja en la configuración de herramientas de seguridad para una empresa.

Unidad de Aprendizaje:	Administra herramientas de seguridad informática.	Número:	2
Práctica:	Interpretación de estadísticas y resultados obtenidos con las herramientas de seguridad informática	Número:	3
Propósito de la práctica:	Establecer procedimientos de monitoreo y control del modelo de seguridad para comprobar sus resultados.		
Escenario:	Laboratorio de cómputo o informática	Duración	2 horas

Materiales, Herramientas, Instrumental, Maquinaria y Equipo	**Desempeños**
• Equipo de cómputo Core Duo o superior • Conexión de internet • Sistema operativo windows xp o superior. • Software: Antivirus (mc affe, panda, BitDefender o cualquiera del que se disponga • Dispositivo de almacenamiento (USB)	• Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje **NOTA al** docente: Coordinará la realización de la práctica y organizará equipos de trabajo. **NOTA al alumno:** Realizará un respaldo de la información que generes en el centro de cómputo de tu escuela con algún dispositivo de almacenamiento. 1. Verifica que el equipo de cómputo esté conectado a la corriente eléctrica. 2. Verifica que haya corriente eléctrica en el contacto. 3. Prende el equipo de cómputo de acuerdo al manual del fabricante. 4. Verifica que el equipo de cómputo tenga instalado el sistema operativo Windows XP o superior. 5. Verifica que el equipo de cómputo tenga instalado un software antivirus. 6. Establece métricas de desempeño del antivirus, determínalo en función del número de archivos almacenados en el equipo de cómputo, la cantidad que estén infectados, considerando tipos de criterios: aceptable, medianamente aceptable, no aceptable 7. Ejecuta la revisión de virus en el equipo de cómputo en la unidad C. 8. Revisa los reportes de resultados emitidos por el software. 9. Identifica el porcentaje de archivos que se encontraron infectados a fin es establecer el correspondiente criterio de desempeño, 10. Identifica las causas de que los criterios obtenidos sean medianamente aceptable o no aceptable. 11. Establece las acciones correctivas a fin de lograr que los criterios de desempeño sean aceptables

	12. Documenta los resultados obtenidos. 13. Cierra la sesión de trabajo del software antivirus 14. Apaga apropiadamente el equipo de cómputo una vez que se haya concluido la práctica.  ADVERTENCIA DE RIESGO ELÉCTRICO

Unidad de Aprendizaje:	Administra herramientas de seguridad informática	Número:	**2**
Práctica:	Afinación de parámetros de configuración de herramientas de seguridad informática	Número:	**4**
Propósito de la práctica:	Identificar y aplicar las acciones correctivas para obtener los resultados esperados en el desempeño de las herramientas de seguridad informática.		
Escenario:	Laboratorio de cómputo o informática	Duración	3 horas

Materiales, Herramientas, Instrumental, Maquinaria y Equipo	**Desempeños**
• Equipo de cómputo Core Duo o superior • Conexión de internet • Sistema operativo windows xp o superior. • Software: Antivirus (mc affe, panda, BitDefender o cualquiera del que se disponga • Dispositivo de almacenamiento (USB) • Documento de acciones correctivas desarrollado en la práctica No. 3 “Interpretación de estadísticas y resultados obtenidos con las herramientas de seguridad informática”	• Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje **NOTA al** docente: Coordinará la realización de la práctica y organizará equipos de trabajo. **NOTA al alumno:** Realizará un respaldo de la información que generes en el centro de cómputo de tu escuela con algún dispositivo de almacenamiento. 1. Verifica que el equipo de cómputo esté conectado a la corriente eléctrica. 2. Verifica que haya corriente eléctrica en el contacto. 3. Prende el equipo de cómputo de acuerdo al manual del fabricante. 4. Verifica que el equipo de cómputo tenga instalado el sistema operativo Windows XP o superior. 5. Verifica que el equipo de cómputo tenga instalado un software antivirus. 6. Modifica los parámetros de configuración del software antivirus de acuerdo al documento desarrollado en la práctica No. 3 “Interpretación de estadísticas y resultados obtenidos con las herramientas de seguridad informática”; o en su caso instala un nuevo software antivirus que permita lograr el desempeño eficiente de esta herramienta. 7. Ejecuta la revisión de virus en el equipo de cómputo en la unidad C. 8. Revisa los reportes de resultados emitidos por el software. 9. Identifica el porcentaje de archivos que se encontraron infectados a fin es establecer el correspondiente criterio de desempeño, 10. Identifica las causas de que los criterios obtenidos sean medianamente aceptable o no aceptable.

	11. Establece las acciones correctivas que se requieran nuevamente realizar a fin de lograr que los criterios de desempeño sean aceptables 12. Documenta los resultados obtenidos. 13. Cierra la sesión de trabajo del software antivirus 14. Apaga apropiadamente el equipo de cómputo una vez que se haya concluido la práctica. .  ADVERTENCIA DE RIESGO ELÉCTRICO

II. Guía de Evaluación del Módulo
Aplicación de la seguridad informática

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 guiar 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 utilizar 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 desempeñarse en los ámbitos personal y profesional que le permitan convivir de manera armónica con el medio ambiente y la sociedad; las **disciplinares**, esenciales para que los alumnos puedan desempeñarse 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 tomar 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 alguna normalización específica de un sector o área y no en contenidos y/o potencialidades.

El **Modelo de Evaluación** se caracteriza porque es **Confiable** (que aplica 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 considerar tres finalidades de evaluación: **diagnóstica, formativa y sumativa**.

La evaluación **diagnóstica** nos permite establecer un **punto de partida** fundamentado en la detección de la situación en la que se encuentran nuestros 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 utilizarse 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 finalizar cada actividad de aprendizaje o en la integración de varias de éstas. Tiene como finalidad **informar a los alumnos de sus avances** con respecto a los aprendizajes que deben alcanzar y advertirle sobre dónde y en qué aspectos tiene debilidades o dificultades para poder regular sus procesos. Aquí se admiten errores, se identifican y se corrigen; es factible trabajar colaborativamente. Asimismo, el 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.

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

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

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

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

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, cada uno de los RA tiene asignada al menos una actividad de evaluación, a la cual 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 considerar que se ha adquirido la competencia correspondiente al módulo de que se trate, deberá **ir acumulando** dichos porcentajes a lo largo del período para estar en condiciones de acreditar 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 8 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 evaluar, 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 acumular 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 considerar para 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 tomar en cuenta como **mínimo indispensable** para evaluar si se ha logrado el resultado de aprendizaje esperado y, por otro, los criterios o **niveles de calidad o satisfacción alcanzados**. En las celdas centrales se describen los criterios que se van a utilizar para evaluar esos indicadores, explicando cuáles son las características de cada uno.

Los criterios que se han establecido son: **Excelente**, 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 medular 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 solicitar 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 recuperar los aprendizajes no logrados.

Como se plantea en los programas de estudio, en una **sesión de clase previa a finalizar la unidad**, el docente debe hacer una **sesión de recapitulación** con sus alumnos con el propósito de valorar 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, realizar actividades adicionales o repetir su desempeño nuevamente, con el fin de recuperarse de inmediato y no esperar hasta que finalice el ciclo escolar acumulando deficiencias que lo pudiesen llevar a no lograr 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 evaluar, 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 señalar que **el docente no tendrá que realizar operaciones matemáticas para el registro de los resultados de sus alumnos**, simplemente deberá marcar 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 EVALUAR			% Peso Específico	% Peso Logrado	% Peso Acumulado
			C	P	A			
1. Aplica estándares de protección de la información	**1.1**. Determina riesgos de seguridad informática con base en las características del equipo y las necesidades del usuario	**1.1.1.**	▲	▲	▲	15		
	1.2 Elabora el plan de seguridad en cómputo acorde con los riesgos determinados y estándares de protección	**1.2.1.**	▲		▲	15		
% PESO PARA LA UNIDAD						**30%**		
2. Administra herramientas de seguridad informática	**2.1** Instala y configura herramientas informáticas acordes con los estándares y buenas prácticas de seguridad en cómputo	**2.1.1.**	▲	▲	▲	40		
	2.2 Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado	**2.2.1**	▲	▲	▲	15		
	2.3 Controla parámetros de seguridad mediante verificación y actualización de acorde con nuevos requerimientos obtenidos.	**2.3.1.**		▲	▲	15		
% PESO PARA LA UNIDAD						**15%**		
PESO TOTAL DEL MÓDULO						**100%**		

9. Materiales para el Desarrollo de Actividades de Evaluación

10. Matriz de Valoración o Rúbrica

MATRIZ DE VALORACIÓN O RÚBRICA

Siglema: ASIN-02	Nombre del Módulo:	**Aplicación de la seguridad informática**		Nombre del Alumno:	
Docente evaluador:			Grupo:		Fecha:
Resultado de Aprendizaje:	**1.1.** Determina riesgos de seguridad informática con base en las características del equipo y las necesidades del usuario		Actividad de evaluación:	**1.1.1.** Elabora informe del análisis de riesgos de seguridad informática de una organización mediana o grande detectando riesgos de acuerdo con el impacto en la confidencialidad, integridad o disponibilidad de la información	

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
Matriz de riesgos	**30**	La matriz de riesgos elaborada establece categorías relacionadas con los tipos de riesgos clasificándolos en alto medio y bajo; así como las de riesgos tanto lógicos como físicos, se presenta debidamente requisitada y, además incluye un instructivo para su llenado	La matriz de riesgos elaborada establece categorías relacionadas con los tipos de riesgos clasificándolos en alto medio y bajo; así como las de riesgos tanto lógicos como físicos, y se presenta debidamente requisitada	Omite categorizar tipos de riesgos clasificándolos en alto medio y bajo; así como las de riesgos tanto lógicos como físicos, o no presenta la matriz de riesgos debidamente requisitada
Ficha técnica	**30**	La ficha técnica elaborada cumple con los siguientes requisitos: a) Especifica las características del equipo de cómputo y/o comunicaciones sobre el cual han de determinarse posibles riesgos. b) Refleja criterios de seguridad	La ficha técnica elaborada cumple con los siguientes requisitos: a) Especifica las características del equipo de cómputo y/o comunicaciones sobre el cual han de determinarse posibles riesgos. b) Refleja criterios de seguridad	La ficha técnica elaborada no cumple con cualquiera de los siguientes requisitos: a) Especifica las características del equipo de cómputo y/o comunicaciones sobre el cual han de determinarse posibles riesgos.

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
		informática aplicada al equipo de cómputo o comunicaciones caracterizado y, además incluye el manejo de íconos, viñetas o diagramas que faciliten la comprensión de la información que contiene.	informática aplicada al equipo de cómputo o comunicaciones caracterizado.	b) Refleja criterios de seguridad informática aplicada al equipo de cómputo o comunicaciones caracterizado.
Cuestionarios a usuarios	**30**	Los cuestionarios se redactan para ser contestados por usuarios o administradores y sus reactivos se dirigen a obtener información que permita analizar niveles de riesgo en la organización a través de: - Determinar la aplicación de configuraciones de seguridad en grupos y cuentas de usuario en el sistema operativo. - Verificar el cumplimiento de políticas aplicadas: de cuenta, auditoría, restricciones a usuarios o de software, firewall, antivirus y antispywar. - Uso de permisos en carpetas y documentos compartidos. - Se presentan debidamente requisitados y además cuentan con una guía de respuestas que funciona como índice de riesgos a partir de su aplicación. - Copia oculta - Archivo adjunto - Descripción de asunto	Los cuestionarios se redactan para ser contestados por usuarios o administradores y sus reactivos se dirigen a obtener información que permita analizar niveles de riesgo en la organización a través de: - Determinar la aplicación de configuraciones de seguridad en grupos y cuentas de usuario en el sistema operativo. - Verificar el cumplimiento de políticas aplicadas: de cuenta, auditoría, restricciones a usuarios o de software, firewall, antivirus y antispyware. - Uso de permisos en carpetas y documentos compartidos. - Se presentan debidamente requisitados.	Los reactivos de los cuestionarios no cumplen con cualquiera de los siguientes aspectos: 1. Encontrarse dirigidos a obtener información que permita analizar niveles de riesgo en la organización a través de: - Determinar la aplicación de configuraciones de seguridad en grupos y cuentas de usuario en el sistema operativo. - Verificar el cumplimiento de políticas aplicadas: de cuenta, auditoría, restricciones a usuarios o de software, firewall, antivirus y antispyware. - Uso de permisos en carpetas y documentos compartidos. 2. Estar dirigidos a usuarios o administradores. 3. Encontrarse debidamente requisitados.
Elementos de forma	**10**	La redacción del informe final refleja precisión y objetividad, recupera la información obtenida a partir de la matriz, la ficha técnica y los cuestionarios, no	La redacción del informe final refleja precisión y objetividad, recupera la información obtenida a partir de la matriz, la ficha técnica y los	La redacción del informe final no es precisa ni objetivo, o no hace referencia a la información obtenida a partir de la matriz, la ficha técnica y

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
		contiene faltas de ortografía o errores en las denominaciones técnicas y, además se entrega tanto de forma impresa como digital.	cuestionarios y no contiene faltas de ortografía o errores en las denominaciones técnicas.	los cuestionarios, contiene faltas de ortografía o errores en las denominaciones técnicas.
	100			

MATRIZ DE VALORACIÓN O RÚBRICA

Siglema: ASIN-02	Nombre del Módulo:	**Aplicación de la seguridad informática**	Nombre del Alumno:	
Docente evaluador:		Grupo:		Fecha:
Resultado de Aprendizaje:	**1.2.** Elabora el plan de seguridad en cómputo, acorde con los riesgos determinados y estándares de protección	Actividad de evaluación:	**1.2.1.** Elabora el plan de seguridad informática basado en estándares internacionales estableciendo mecanismos de protección a la información, así como métricas de evaluación del mismo	

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
Estándares	**20**	El plan elaborado se basa en estándares internacionales de seguridad informática entre los que se incluyen: - BS 17799 - Serie ISO 27000 - ISO 20000 y además considera modelos de seguridad informática como ITIL, Cobit o ISM3.	El plan elaborado se basa en estándares internacionales de seguridad informática entre los que se incluyen: - BS 17799 - Serie ISO 27000 - ISO 20000	El plan elaborado no considera estándares internacionales de seguridad informática entre los que se incluyen: - BS 17799 - Serie ISO 27000 - ISO 20000
Políticas	**25**	El plan elaborado define políticas relacionadas con: - Acceso físico y lógico a equipos - Creación de cuentas de usuario - Manejo de bitácoras - Protección de la red - Administración de software de seguridad - Gestión de actualizaciones, cambios almacenamiento y respaldos, y además incluye políticas de	El plan elaborado define políticas relacionadas con: - Acceso físico y lógico a equipos - Creación de cuentas de usuario - Manejo de bitácoras - Protección de la red - Administración de software de seguridad - Gestión de actualizaciones, cambios almacenamiento y respaldos,	Excluye alguna política de los siguientes criterios: - Acceso físico y lógico a equipos - Creación de cuentas de usuario - Manejo de bitácoras - Protección de la red - Administración de software de seguridad - Gestión de actualizaciones, cambios almacenamiento y respaldos

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
		capacitación al personal.		
Metas	**25**	Precisa numéricamente las metas de seguridad a alcanzar en un periodo de tiempo establecido y, además incluye un cronograma.	El plan elaborado precisa numéricamente las metas de seguridad a alcanzar en un periodo establecido.	No establecen metas o no se recurre a precisiones numéricas en el caso de establecerlas o no se precisan periodos de cumplimiento para el caso de las metas.
Evaluación de controles	**25**	El plan elaborado establece la manera de evaluar los controles implementados a través de: - Definición de los indicadores o mecanismos que corresponda - Definición de la forma de medir dichos indicadores y, además establece parámetros de seguimiento de la aplicación de controles.	El plan elaborado establece la manera de evaluar los controles implementados a través de: - Definición de los indicadores o mecanismos que corresponda - Definición de la forma de medir dichos indicadores	El plan no incluye mecanismos o métricas de evaluación.
Forma **(AUTOEVALUACIÓN)**	**5**	La redacción del plan de seguridad en cómputo refleja precisión y objetividad, se estructura incorporando como mínimo políticas, metas y evaluación de controles y no contiene faltas de ortografía o errores en las denominaciones técnicas y, además se entrega tanto de forma impresa como digital.	La redacción del plan de seguridad en cómputo refleja precisión y objetividad, se estructura incorporando como mínimo políticas, metas y evaluación de controles y no contiene faltas de ortografía o errores en las denominaciones técnicas.	La redacción del plan de seguridad en cómputo es imprecisa, poco objetiva, omite incorporar como mínimo políticas, metas y evaluación de controles, contiene faltas de ortografía o errores en las denominaciones técnicas.
	100			

MATRIZ DE VALORACIÓN O RÚBRICA

Siglema: ASIN-02	Nombre del Módulo:	**Aplicación de la seguridad informática**	Nombre del Alumno:	
Docente evaluador:		Grupo:		Fecha:
Resultado de Aprendizaje:	**2.1.** Instala y configura herramientas informáticas acordes con los estándares y buenas prácticas de seguridad en cómputo	Actividad de evaluación:	**2.1.1.** Instala y configura herramientas informáticas de manera segura y en apego al manual determinado	

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
Configuración local	**50**	La configuración local de seguridad se realiza en apego al manual elaborado, considerando como mínimo los siguientes elementos: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas - Cifrado de archivos y, además establece políticas para el manejo de antivirus y antispyware.	La configuración local de seguridad se realiza en apego al manual elaborado, considerando como mínimo los siguientes elementos: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas - Cifrado de archivos	La configuración local de seguridad no se apega al manual elaborado, o no considera como mínimo: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas - Cifrado de archivos
Configuración de red	**50**	La configuración de red de seguridad informática se realiza en apego al manual, considerando como mínimo los siguientes elementos: - Firewall perimetral - Detección de intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas y, además se expresa en una sinopsis escrita del proceso.	La configuración de red de seguridad informática se realiza en apego al manual, considerando como mínimo los siguientes elementos: - Firewall perimetral - Detección de intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas	La configuración de red de seguridad informática no se apega al manual, o no integra como mínimo cualquiera de los siguientes elementos: - Firewall perimetral - Detección de intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas
	100			

MATRIZ DE VALORACIÓN O RÚBRICA

Siglema: ASIN-02	Nombre del Módulo:	**Aplicación de la seguridad informática**	Nombre del Alumno:	
Docente evaluador:		Grupo:		Fecha:
Resultado de Aprendizaje:	**2.2.** Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado	Actividad de evaluación:	**2.2.1.** Monitorea la operación de las herramientas informáticas a fin de garantizar su funcionamiento	

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
Estado de las aplicaciones	**30**	Verifica que el estado de las aplicaciones coincida con lo establecido en el manual correspondiente y, además elabora un reporte escrito de estatus.	Verifica que el estado de las aplicaciones coincida con lo establecido en el manual correspondiente.	No establece la coincidencia entre el estado de las aplicaciones y lo establecido en el manual correspondiente.
Modificación de Configuraciones	**35**	La modificación de configuraciones se realiza conforme a los procedimientos establecidos en el manual correspondiente y, además se precisa si existen nuevos requerimientos.	La modificación de configuraciones se realiza conforme a los procedimientos establecidos en el manual correspondiente.	La modificación de configuraciones no se realiza conforme a los procedimientos establecidos en el manual correspondiente.
Respaldos	**10**	Verifica que se cuente con el respaldo de las configuraciones de las aplicaciones, y además lo reporta en un instrumento de cotejo.	Verifica que se cuente con el respaldo de las configuraciones de las aplicaciones.	Desconoce si se cuenta con el respaldo de las configuraciones de las aplicaciones.
Reporte	**25**	Elabora un reporte impreso del estado de seguridad del sistema en la fecha determinada., y además programa la ejecución automática de un reporte en forma periódica.	Presenta un reporte impreso del estado de seguridad del sistema en la fecha determinada.	No presenta un reporte impreso del estado de seguridad del sistema en la fecha determinada.
	100			

MATRIZ DE VALORACIÓN O RÚBRICA

Siglema: ASIN-02	Nombre del Módulo:	**Aplicación de la seguridad informática**		Nombre del Alumno:	
Docente evaluador:			Grupo:		Fecha:
Resultado de Aprendizaje:	**2.3** Controla parámetros de seguridad mediante verificación y actualización de acorde con nuevos requerimientos obtenidos.		Actividad de evaluación:	2.3.1	Revisa las configuraciones de equipos y redes de comunicación comprobando el cumplimiento de las políticas definidas en el plan de seguridad determinado e identificando nuevos requerimientos **(HETEROEVALUACIÓN)**

INDICADORES	**%**	**C R I T E R I O S**		
		Excelente	**Suficiente**	**Insuficiente**
Plan de revisión	**20**	Elabora un plan de revisión de software en el que se contengan como mínimo los siguientes aspectos: - Rubros a revisar - Alcances de la revisión y, además incluye en el plan, revisar el cumplimiento de las políticas de seguridad de la empresa.	Elabora un plan de revisión de software en el que se contengan como mínimo los siguientes aspectos: - Rubros a revisar - Alcances de la revisión	No cuenta con un plan de revisión de seguridad en el que se contengan como mínimo los siguientes aspectos: - Rubros a revisar - Alcances de la revisión
Balance de resultados	**20**	Elabora el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación y, además construye una matriz comparativa para expresarlo.	Elabora el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación	Omite elaborar el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación
Requerimientos	**20**	Determina los requerimientos de configuración de herramientas de seguridad, y además relaciona los riesgos asociados a dichos requerimientos.	Determina los requerimientos de configuración de herramientas de seguridad.	Desconoce la existencia de requerimientos de configuración de herramientas de seguridad

INDICADORES	%	C R I T E R I O S		
		Excelente	**Suficiente**	**Insuficiente**
Informe	**20**	Elabora los tres informes que se especifican a continuación: 1 Informe de resultados generados. 2 Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. 3 Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados, y además los presenta de manera tanto digital como impresa.	Elabora los tres informes que se especifican a continuación: 1 Informe de resultados generados. 2 Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. 3 Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados, y además los presenta de manera tanto digital como impresa.	Omite la elaboración de cualquiera de los tres informes que se especifican a continuación: 1 Informe de resultados generados. 2 Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. 3 Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados, y además los presenta de manera tanto digital como impresa.
Forma	**20**	Presenta el informe en forma impresa integrando datos de identificación: lugar, periodo, sistema auditado, características de la auditoría, resultados, responsables y firmas, y además los presenta en formato digital.	Presenta el informe en forma impresa integrando datos de identificación: lugar, periodo, sistema auditado, características de la auditoría, resultados, responsables y firmas.	No presenta el informe impreso de la auditoría con todos los datos de identificación: lugar, periodo, sistema auditado, características de la auditoría, resultados, responsables y firmas.
	100			