Guía pedagógica y de evaluación del módulo

Aplicación de la seguridad informática

Currículum Laboral

Áreas:
Tecnología y transporte

Carrera:
Profesional Técnico-Bachiller en Informática

3º semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad informática.

Área: Tecnología y transporte.

Carrera: PT-B en Informática

Semestre: 3°

Horas por semana: 4

Fecha de diseño o actualización: 31 de mayo de 2024.

Vigencia: a partir de la aprobación de la Junta Directiva y en tanto no se genere un documento que lo actualice.

Directorio

Arturo Pontifes Martínez
Dirección General

Camilo García Ramírez
Secretaría General

Hugo Nicolás Pérez González
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Aplicación de la seguridad informática

Contenido

I. Guía pedagógica

1. Descripción

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

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

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

2. Generalidades pedagógicas

Nuestro modelo académico sustenta una base pedagógica centrada en la teoría constructivista con un enfoque humanista, la cual tiene presente la diversidad local, regional, nacional e internacional, combinada con el nuevo MCCEMS permitirá mantener una didáctica que apuesta por el desarrollo de la voluntad de aprender, hacer una conexión entre el contenido teórico y la realidad.

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

El alumnado adquiere un rol protagónico del proceso educativo, guiándolo al involucramiento y resolución de problemas económicos, políticos, sociales y del medio ambiente para la construcción de un mundo más justo, pacífico y sostenible, bajo el acompañamiento, orientación y conducción del docente, por lo que el docente bajo su experiencia buscará una combinación de estrategias didácticas que incorporen materiales y recursos que den sentido a lo que el estudiante aprende.

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

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

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

3. Orientaciones didácticas

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

- Identificar los componentes básicos de los resultados de aprendizaje para realizar el plan clase, considerando los elementos con los que se puede trabajar el contenido.
- Abordar conocimientos previos a través del diseño de una actividad, considerando la exploración de conocimientos, saberes e ideas precedentes.
- Seleccionar actividades pertinentes y acordes a los resultados de aprendizaje, procurando activar la atención del estudiantado a partir de generar ambientes de trabajo encaminados a la reflexión, el diálogo y la discusión.
- Considerar métodos y estrategias que favorezcan aprendizajes significativos.
- Plantear el objetivo de cada actividad buscando la contextualización de acuerdo con las características de la comunidad, municipio, región y estados.
- Plantear actividades dirigidas al trabajo directo con la comunidad de forma independiente como un complemento a lo revisado en clase o una extensión del tema; de ser posible tener un repositorio de información digital para alojar los materiales que el estudiantado deba consultar.
- Retroalimentar las actividades y trabajos del estudiantado con el fin de orientarlos sobre sus avances y aspectos a mejorar en sus procesos de aprendizaje.
- Promover la coevaluación, autoevaluación y heteroevaluación para favorecer la retroalimentación formativa y asertiva.
- Aplicar la transversalidad buscando proyectos que se interrelacionen de forma horizontal y vertical basado en el mapa curricular.
- Procurar que las actividades realizadas de forma independiente sean un complemento a lo revisado en clase o una extensión del tema y deberán estar dirigidas al trabajo directo con la comunidad.
- Compartir los propósitos educativos y los criterios del logro de aprendizaje con los estudiantes.
- Diseñar e implementar actividades que evidencien lo que el estudiantado está aprendiendo.
- Procurar incluir el aprendizaje práctico fuera del aula, intercambiar conocimientos con miembros de la comunidad, generar dinámicas con amigos, vecinos o familiares, ejecutar actividades comunicativas y académicas específicas, así como la aplicación progresiva de

métodos didácticos; es importante observar e identificar las habilidades y aptitudes de los estudiantes para encaminarlos, desarrollarlas mejor y apoyarles.

- Algunas estrategias para la utilización de la retroalimentación formativa son las siguientes:
    1. Clarificar y compartir los objetivos de aprendizaje y criterios de desempeño con cada estudiante al inicio de cada resultado de aprendizaje.
    2. Diseñar discusiones de clase efectivas, preguntas, actividades y tareas que hagan evidente el aprendizaje del estudiante.
    3. Proveer retroalimentación que motive el aprendizaje.
    4. Activar en la comunidad estudiantil el deseo de ser responsables de su propio proceso de aprendizaje.
    5. Fomentar la participación de las y los estudiantes como recurso de apoyo para sus pares.
- Conforme a los preceptos del MCCEMS, retomar los Recursos Socioemocionales que conforman el currículum ampliado: la Responsabilidad Social, el Cuidado Físico Corporal y el Bienestar Emocional Afectivo, constituyendo un eje articulador el cual busca que las y los estudiantes se formen como ciudadanas y ciudadanos responsables, honestos, comprometidos con el bienestar físico mental y emocional, tanto personal como social. Se pretende trabajar con mayor autonomía en el aula, la escuela, la comunidad, la solidaridad, la inclusión y la diversidad, así como el reconocimiento de la perspectiva de género y los aportes de la cultura de paz, de valorar el esfuerzo de las conductas legales y del trabajo justo y honrado, al poner en práctica acciones ciudadanas y proyectos escolares comunitarios.
- Derivado de lo anterior, durante el desarrollo del módulo se sugiere tener presente el Currículum ampliado, establecido en el Acuerdo número 09/08/23 por el que se establece y regula el Marco Curricular Común de la Educación Media Superior https://www.dof.gob.mx/nota_detalle.php?codigo=5699835&fecha=25/08/2023#gsc.tab=0

4. Estrategias de aprendizaje

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

- Investigar por equipo los conceptos principales de la seguridad informática:
  - Seguridad
  - Información
  - Informática
  - Seguridad informática
  - Principios de la seguridad informática: confidencialidad, integridad y disponibilidad.
- Diseñar un tríptico con la información anterior.
- Realizar labores de investigación en fuentes bibliográficas y sitios de Internet para identificar los principales riesgos informáticos a que está expuesto, contemplando: concepto de riesgo, tipos de riesgo, matriz de riesgo, concepto de vulnerabilidad, riesgos lógicos y riesgos físicos.
- Elaborar un cuadro sinóptico con la información obtenida.
- Elegir por equipo una empresa y recopilar la siguiente información: objetivos de resguardo de información en la empresa, organigramas, manuales de proceso y controles internos de seguridad informática.
- Complementar su investigación a través de entrevistas y cuestionarios para obtener información sobre los problemas de seguridad a los que se ha enfrentado la empresa, cuál ha sido su impacto y cómo se resolvió la problemática, políticas aplicadas, permisos en carpetas y documentos compartidos, cómo respaldan su información, qué actualizaciones de sistema operativo tienen y el reconocimiento de riesgos físicos en la organización aplicados a equipos de cómputo y comunicaciones.
- Elaborar una ficha técnica de las características del equipo de cómputo y de comunicaciones de la empresa elegida, que incluya la valoración de criterios de seguridad informática.
- Exponer ante el grupo la información obtenida de la empresa elegida.
- Elaborar la matriz de riesgos estableciendo categorías relacionadas con los tipos de riesgos clasificándolos en alto medio y bajo; así como las categorías de riesgos tanto lógicos como físicos.
- **Realizar la actividad de evaluación 1.1.1 considerando la rúbrica correspondiente**

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

- 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.
- Participar en una mesa redonda para contrastar sus investigaciones con las del resto del grupo.
- Investigar los estándares internacionales de seguridad informática y elaborar un cuadro sinóptico con la información obtenida.
- Analizar en grupos de trabajo los recursos informáticos y las características con que cuenta el laboratorio de la escuela.
- Evaluar con base en los estándares internacionales de seguridad informática el plan de seguridad informática del laboratorio de la escuela.
- Elaborar un reporte de los resultados obtenidos en el análisis.
- Contrastar en plenaria la evaluación realizada por cada equipo y llegar a acuerdos comunes sobre las necesidades de seguridad informática del laboratorio de cómputo de la escuela.
- Establecer métricas y mecanismos para la evaluación de los controles implementados, definiendo indicadores para evaluar la eficiencia de los controles implementados y el modo en que los indicadores serán medidos.
- **Realizar la actividad de evaluación 1.2.1 considerando la rúbrica correspondiente**

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

- Investigar por equipo los requerimientos y procedimientos de instalación y configuración de un software.
- Elaborar un manual de instalación y configuración de software.
- Verificar por equipo, la configuración local de seguridad, tomando en cuenta: actualizaciones automáticas para el sistema operativo y aplicaciones, manejo de cuentas, bitácoras, software y firewall local, políticas para el manejo de antispyware, cifrado de archivos y carpetas, entre otros.
- Configurar la red de seguridad informática tomando en cuenta la configuración del firewall perimetral, el sistema de detección de intrusos, los protocolos de seguridad y los permisos de archivos y carpetas compartidas.
- Analizar 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 considerando la rúbrica correspondiente.**

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

- Dar seguimiento a la actividad de la unidad anterior respecto a la operación de las herramientas informáticas configuradas en su plan y generar los reportes de su operación, después de que otro equipo de trabajo intentó romper su seguridad, tomando en cuenta el estado de las aplicaciones y su funcionamiento.
- Elaborar un reporte, de la efectividad de las herramientas y de los cambios a realizar para aumentar la eficacia del plan de seguridad.
- Modificar la configuración conforme a los procedimientos definidos en el manual.
- Respaldar los nuevos requerimientos de las configuraciones de las aplicaciones.
- **Realizar la actividad de evaluación 2.2.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 2.3, se recomienda al alumnado:

- Utilizar en el laboratorio de cómputo o informática las herramientas de auditoría para la recopilación de información y para la comparación de configuraciones, para revisar el plan de seguridad configurado en la unidad de aprendizaje anterior, determinando las modificaciones necesarias al plan y sus herramientas.
- Finalizar el proceso de configuración de las herramientas de seguridad, aplicando en el laboratorio los cambios necesarios, de acuerdo con resultados los obtenidos.
- Elaborar un reporte tomando en cuenta la operación de las aplicaciones, la comparación de métricas establecidas con los resultados obtenidos, identificación y definición de nuevos requerimientos de seguridad, medidas para solucionar los nuevos requerimientos y alternativas para optimizar los ya existentes.
- Intercambiar y analizar el reporte de otro equipo de trabajo, realizando los ajustes necesarios.
- Implementar acciones correctivas en la configuración y ejecución de herramientas de seguridad informática, tales como planes de contingencia y actualización de software y de equipo de seguridad.
- Realizar un informe que contenga los nuevos requerimientos y riesgos de seguridad identificados.
- **Realizar la actividad de evaluación 2.3.1 considerando la rúbrica correspondiente.**

5. Prácticas y Actividades

En respeto a la autonomía didáctica, este apartado quedará bajo la responsabilidad del personal docente para que, de acuerdo con su experiencia, características del grupo, la comunidad y el desempeño del estudiantado, seleccione, proponga y realice aquellas prácticas y actividades transversales que garanticen un mayor desarrollo de aprendizajes y habilidades, privilegiando las corrientes filosóficas, pedagógicas y técnicas de mayor actualidad, así como las tecnologías de la información y la comunicación, como herramientas de apoyo al proceso de enseñanza – aprendizaje.

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

De igual manera, se espera que el estudiantado asuma su responsabilidad y tome un papel activo en el proceso de desarrollo de **habilidades**, **conocimientos, actitudes y valores** que le permitirán no sólo ingresar al mundo laboral, sino participar de manera destacada en la sociedad.

II. Guía de Evaluación

6. Descripción

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

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

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

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

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

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

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

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

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

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

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

7. Tabla de ponderación

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

UNIDAD	RESULTADO DE APRENDIZAJE	ACTIVIDAD DE EVALUACIÓN	% Peso Específico	% Peso Logrado	% Peso Acumulado
1. Utiliza 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**	**20**		
% PESO PARA LA UNIDAD			**35 %**		
2. Administra herramientas de seguridad informática.	**2.1** Instala y configura herramientas informáticas acorde con los estándares y buenas prácticas de seguridad en cómputo.	**2.1.1**	**30**		
	2.2 Da seguimiento a la operación de las herramientas informáticas de acuerdo con el plan de seguridad determinado.	**2.2.1**	**20**		
	2.3 Controla parámetros de seguridad mediante verificación y actualización acorde con nuevos requerimientos obtenidos.	**2.3.1**	**15**		
% PESO PARA LA UNIDAD			**65%**		
PESO TOTAL DEL MÓDULO			**100%**		

8. Matriz de valoración o rúbrica

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

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

Siglema:	**ASIN-20**	**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 de análisis de riesgos de seguridad informática de una organización considerando los criterios de confidencialidad, integridad y disponibilidad de la información.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Matriz de riesgos	**30**	• Elabora la matriz de riesgos con las siguientes características: - Clasifica los riesgos en alto, medio y bajo - Cataloga los riesgos tanto lógicos como físicos, - La presenta debidamente requisitada - Incluye un instructivo para su llenado.	• Elabora la matriz de riesgos omitiendo una de las siguientes características: - Clasifica los riesgos en alto, medio y bajo - Cataloga los riesgos tanto lógicos como físicos, - La presenta debidamente requisitada - Incluye un instructivo para su llenado.	• Requiere apoyo para elaborar la matriz de riesgos y categorizarlos en alto, medio y bajo, lógicos y físicos. • Omite el instructivo de llenado.	• Omite la entrega de la matriz de riesgos.
Ficha técnica	**30**	• La ficha técnica elaborada cumple con los siguientes requisitos: - Especifica las características del equipo de cómputo y/o comunicaciones sobre el cual han de determinarse posibles riesgos. - Refleja criterios de seguridad informática	• La ficha técnica elaborada omite uno de lossiguientes requisitos: - Especifica las características del equipo de cómputo y/o comunicaciones sobre el cual han de determinarse posibles riesgos. - Refleja criterios de seguridad informática	• Requiere apoyo para la elaboración de la ficha técnica.	• Omite la elaboración de la ficha técnica.

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
		aplicada al equipo de cómputo o comunicaciones caracterizado. - Incluye el manejo de íconos, viñetas o diagramas que faciliten la comprensión de la información que contiene.	aplicada al equipo de cómputo o comunicaciones caracterizado. - Incluye el manejo de íconos, viñetas o diagramas que faciliten la comprensión de la información que contiene.		
Cuestionarios a usuarios	**30**	• Redacta los cuestionarios 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, ransomware y control DDOS.	• Redacta los cuestionarios para ser contestados por usuarios o administradores y sus reactivos se dirigen a obtener información que permita analizar niveles de riesgo en la organización, omitiendo alguno de los siguientes aspectos: - 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, ransomware y	• Redacta los cuestionarios para ser contestados por usuarios o administradores y sus reactivos se dirigen a obtener información que permita analizar niveles de riesgo en la organización, omitiendo dos de los siguientes aspectos: - 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, ransomware y	• Omite la elaboración de cuestionarios para ser contestados por usuarios o administradores, que permitan analizar niveles de riesgo en una organización.

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		- Uso de permisos en carpetas y documentos compartidos. - Se presentan debidamente requisitados • Elabora una guía de respuestas que funciona como índice de riesgos a partir de su aplicación. - Copia oculta - Archivo adjunto - Descripción de asunto.	control DDOS. - Uso de permisos en carpetas y documentos compartidos. - Se presentan debidamente requisitados • Omite la elaboración de una guía de respuestas que funciona como índice de riesgos a partir de su aplicación.	control DDOS. - Uso de permisos en carpetas y documentos compartidos. - Se presentan debidamente requisitados	
Elementos de forma	**10**	• Redacta minuciosamente el informe final con calidad, precisión y objetividad. • Recupera la información fundamental, obtenida a partir de la matriz, la ficha técnica y los cuestionarios. • Utiliza correctamente la ortografía en la redacción y en las denominaciones técnicas. • Entrega el informe en tiempo y forma, tanto en formato impreso como digital.	• Redacta el informe con precisión y objetividad. • Recupera la información clave, obtenida a partir de la matriz, la ficha técnica y los cuestionarios. • Comete algunos errores ortográficos en la redacción y en las denominaciones técnicas. • Entrega el informe en tiempo y forma, de manera digital o impresa.	• Redacta el informe con precisión. • Recupera la información básica obtenida a partir de la matriz, la ficha técnica y los cuestionarios. • Muestra desconocimiento del uso de reglas ortográficas para la redacción del informe y el manejo de las denominaciones técnicas. • Entrega el informe fuera de tiempo de manera digital o impresa.	• Redacta el informe de manera poco precisa. • Omite la información obtenida a partir de la matriz, la ficha técnica y los cuestionarios. • Contiene faltas de ortografía y errores en las denominaciones técnicas. • Omite la entrega del informe.
	100				

Siglema:	**ASIN-20**	**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 de la información y métricas de evaluación.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Estándares	**20**	• Elabora el plan basándose en los estándares internacionales de seguridad informática entre los que se incluyen: - BS 17799 - Serie ISO 27000 - ISO/IEC 27032: Directrices para la ciberseguridad. - ISO/IEC 27033: Seguridad de las redes. - ISO/IEC 27034: Seguridad de las aplicaciones. - ISO/IEC 27035: Gestión de incidentes de seguridad de TI. - ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros. - ISO 20000 • Incluye los modelos de seguridad informática como ITIL, Cobit e ISM3.	• Elabora el plan basándose en los estándares internacionales de seguridad informática omitiendo uno de los siguientes: - BS 17799 - Serie ISO 27000 - ISO/IEC 27032: Directrices para la ciberseguridad. - ISO/IEC 27033: Seguridad de las redes. - ISO/IEC 27034: Seguridad de las aplicaciones. - ISO/IEC 27035: Gestión de incidentes de seguridad de TI. - ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros. - ISO 20000 • Considera uno de los siguientes modelos de	• Elabora el plan basándose en los estándares internacionales de seguridad, omitiendo dos de los siguientes: - BS 17799 - Serie ISO 27000 - ISO/IEC 27032: Directrices para la ciberseguridad. - ISO/IEC 27033: Seguridad de las redes. - ISO/IEC 27034: Seguridad de las aplicaciones. - ISO/IEC 27035: Gestión de incidentes de seguridad de TI. - ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros. - ISO 20000 • Omite los modelos de seguridad informática como ITIL, Cobit e ISM3.	• Elabora el plan basándose en los estándares internacionales de seguridad, considerando únicamente uno o dos de los siguientes: - BS 17799 - Serie ISO 27000 - ISO/IEC 27032: Directrices para la ciberseguridad. - ISO/IEC 27033: Seguridad de las redes. - ISO/IEC 27034: Seguridad de las aplicaciones. - ISO/IEC 27035: Gestión de incidentes de seguridad de TI. - ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros. - ISO 20000

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
			seguridad informática como ITIL, Cobit o ISM3.		
Políticas	**25**	• Elabora el plan definiendo 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 • Incluye políticas de capacitación al personal.	• Elabora el plan omitiendo una de las siguientes políticas: - 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 • Omite la inclusión de políticas de capacitación al personal.	• Elabora el plan omitiendo dos de las siguientes políticas: - 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	• Requiere ayuda para elaborar el plan e identificar las siguientes políticas: - 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.
metas	**25**	• Precisa jerárquica y numéricamente las metas de seguridad por alcanzar en un periodo de tiempo establecido. • Elabora detalladamente un cronograma considerando la totalidad de las actividades por realizar.	• Precisa numéricamente las metas de seguridad por alcanzar en un periodo de tiempo establecido. • Elabora un cronograma considerando las actividades más importantes por realizar.	• Precisa algunas metas de seguridad por alcanzar, sin definir tiempos. • Elabora un cronograma de algunas actividades por realizar.	• Excluye el establecimiento de metas. • Omite la elaboración de un cronograma para organizar las actividades.
Evaluación de controles	**25**	• Establece en el plan, la manera de evaluar los controles implementados a través de: - Definición de los indicadores o mecanismos que corresponda	• Establece en el plan, la manera de evaluar los controles implementados omitiendo uno de los siguientes aspectos: - Definición de los indicadores o mecanismos que	• Establece en el plan, la manera de evaluar los controles implementados omitiendo dos de los siguientes aspectos: - Definición de los indicadores o mecanismos que	• Omite en el plan mecanismos o métricas de evaluación.

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		- Definición de la forma de medir dichos indicadores. - Establece parámetros de seguimiento de la aplicación de controles.	corresponda - Definición de la forma de medir dichos indicadores. - Establece parámetros de seguimiento de la aplicación de controles.	corresponda - Definición de la forma de medir dichos indicadores. Establece parámetros de seguimiento de la aplicación de controles.	
Forma **Autoevaluación**	**5**	• Redacta el plan de seguridad en cómputo con precisión y objetividad. • Incorpora detalladamente políticas, metas y evaluación de controles. • Redacta con buena de ortografía y sin errores en las denominaciones técnicas • Entrega el documento en tiempo y forma, tanto de forma en formato impreso como digital.	• Redacta el plan de seguridad en cómputo con precisión. • Incorpora políticas, metas y evaluación de controles • Redacta con algunos errores ortográficos o faltas en las denominaciones técnicas • Entrega el documento a tiempo, en formato impreso o digital.	• Redacta el plan de seguridad en cómputo • Incorpora algunas políticas, metas o evaluación de controles. • Redacta con errores ortográficos y faltas en las denominaciones técnicas • Entrega el documento fuera de tiempo, en formato impreso o digital.	• Redacta el plan de seguridad en cómputo de manera imprecisa y poco objetiva. • Excluye la incorporación de políticas, metas y evaluación de controles. • Está redactado con faltas de ortografía y errores en las denominaciones técnicas. • Omite la entrega del documento a tiempo. • Entrega el documento hecho a mano de manera física.
	100				

Siglema:	**ASIN-20**	**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 acorde 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	**Bueno**	**Suficiente**	**Insuficiente**
Configuración local	**45**	• Realiza la configuración local de seguridad en apego al manual elaborado, considerando los siguientes elementos: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas - Cifrado de archivos - Establece políticas para el manejo de antivirus y antispyware.	• Realiza la configuración local de seguridad en apego al manual elaborado, omitiendo uno de los siguientes elementos: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas - Cifrado de archivos - Establece políticas para el manejo de antivirus y antispyware.	• Realiza la configuración local de seguridad en apego al manual elaborado, omitiendo dos de los siguientes elementos: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas. - Cifrado de archivos. - Establece políticas para el manejo de antivirus y antispyware.	• Realiza la configuración local de seguridad, omitiendo lo establecido en el manual. • Considera uno o dos de los siguientes elementos en la configuración: - Actualizaciones automáticas - Manejo de cuentas, bitácoras y software - Firewall local - Permisos de archivos y carpetas compartidas. - Cifrado de archivos. - Establece políticas para el manejo de antivirus y antispyware.
Configuración de red	**45**	• Configura la red de seguridad informática en apego al manual, considerando los siguientes elementos: - Firewall perimetral - Detección de	• Configura la red de seguridad informática en apego al manual, omitiendo uno de los siguientes elementos: - Firewall perimetral - Detección de	• Configura la red de seguridad informática en apego al manual, omitiendo dos de los siguientes elementos: - Firewall perimetral - Detección de	• Configura la red de seguridad informática con procedimientos ajenos al manual. • Incluye uno de los siguientes elementos: - Firewall perimetral

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas • Elabora detalladamente un diagrama de flujo para describir el proceso.	intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas • Elabora un diagrama de flujo para describir el proceso.	intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas • Describe el proceso en un organizador gráfico diferente a un diagrama de flujo.	- Detección de intrusos - IPSEC / http sobre ssl - Permisos de aplicaciones compartidas. • Omite la descripción del proceso.
Configuración y seguridad conforme a manual **Coevaluación**	**10**	• Realiza sistemáticamente la configuración de seguridad conforme a las especificaciones del manual.	• Realiza la configuración de seguridad conforme a las especificaciones básicas del manual.	• Realiza la configuración de seguridad conforme a las especificaciones mínimas del manual.	• Omite la consulta del manual para realizar la configuración de seguridad.
	100				

Siglema:	**ASIN-20**	**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	**Bueno**	**Suficiente**	**Insuficiente**
Estado de las aplicaciones	**30**	• Verifica sistemáticamente que el estado de las aplicaciones coincida con lo establecido en el manual correspondiente. • Elabora detalladamente un reporte escrito de estatus.	• Verifica que el estado de las aplicaciones coincida con lo establecido en el manual correspondiente. • Elabora un reporte escrito de estatus.	• Verifica que el estado de algunas aplicaciones coincida con lo establecido en el manual correspondiente. • Omite la elaboración del reporte escrito.	• Omite la verificación de la coincidencia entre el estado de las aplicaciones y lo establecido en el manual correspondiente.
Modificación de configuraciones	**35**	• Identifica y realiza sistemáticamente la modificación de configuraciones conforme a los procedimientos establecidos en el manual correspondiente. • Precisa si existen nuevos requerimientos.	• Realiza sistemáticamente la modificación de configuraciones conforme a los procedimientos establecidos en el manual correspondiente. • Identifica si existen nuevos requerimientos.	• Realiza la modificación de configuraciones conforme a los procedimientos establecidos en el manual correspondiente. • Requiere apoyo para identificar si existen nuevos requerimientos.	• Modifica las configuraciones excluyendo los procedimientos establecidos en el manual. • Omite la identificación de nuevos requerimientos.
Respaldos	**10**	• Verifica detalladamente que cuenta con el respaldo de las configuraciones de las aplicaciones. • Elabora un reporte detallado y escrito en un cuadro sinóptico.	• Verifica que cuenta con el respaldo de las configuraciones de las aplicaciones. • Elabora un reporte por escrito en un cuadro sinóptico.	• Identifica el respaldo de las configuraciones de las aplicaciones. • Elabora un reporte por escrito en un formato diferente a un cuadro sinóptico.	• Desconoce si se cuenta con el respaldo de las configuraciones de las aplicaciones. • Omite la elaboración del reporte.
Reporte	**25**	• Elabora detalladamente un reporte impreso del estado de seguridad del sistema, en la fecha determinada.	• Elabora un reporte impreso del estado de seguridad del sistema, en la fecha determinada.	• Requiere ayuda para realizar el reporte del estado del sistema de seguridad.	• Omite la elaboración del reporte impreso del estado de seguridad del sistema en la fecha determinada.

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
		• Programa la ejecución automática de un reporte en forma periódica.	• Programa con errores la ejecución automática de un reporte en forma periódica.	• Necesita apoyo para programar la ejecución automática de un reporte en forma periódica.	• Desconoce cómo programar la ejecución de un reporte en forma periódica.
	100				

Siglema:	**ASIN-20**	**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 evaluando el cumplimiento de las políticas del plan de seguridad, así como determinarnuevos requerimientos. **(HETEROEVALUACIÓN)**		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Plan de revisión	**20**	• Elabora un plan de revisión detallada de software en el que se contengan los siguientes aspectos: - Rubros por revisar. - Alcances de la revisión. - Herramientas de auditoria para la recopilación de la información. - Herramientas de auditoría para la comparación de configuraciones. - Estado de las aplicaciones. - Funcionamiento de las aplicaciones. - Medidas para solucionar nuevos requerimientos. - Alternativas para optimizar lo existente. • Incluye en el plan, la revisión minuciosa del cumplimiento de las	• Elabora un plan de revisión de software en el que se omiten dos de los siguientes aspectos: - Rubros por revisar. - Alcances de la revisión. - Herramientas de auditoria para la recopilación de la información. - Herramientas de auditoría para la comparación de configuraciones. - Estado de las aplicaciones. - Funcionamiento de las aplicaciones. - Medidas para solucionar nuevos requerimientos. - Alternativas para optimizar lo existente. • Incluye en el plan, la revisión del cumplimiento de algunas de las políticas	• Elabora un plan de revisión de software en el que se omiten más de dos de los siguientes aspectos: - Rubros por revisar. - Alcances de la revisión. - Herramientas de auditoria para la recopilación de la información. - Herramientas de auditoría para la comparación de configuraciones. - Estado de las aplicaciones. - Funcionamiento de las aplicaciones. - Medidas para solucionar nuevos requerimientos. - Alternativas para optimizar lo existente. • Omite en el plan la revisión del cumplimiento de las políticas de	• Omite la elaboración de un plan de revisión de software.

INDICADORES	%	C R I T E R I O S			
		Excelente	Bueno	Suficiente	Insuficiente
		políticas de seguridad de la empresa.	de seguridad de la empresa.	seguridad de la empresa	
Balance de resultados	**20**	• Elabora sistemáticamente el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. • Construye una matriz comparativa para expresar jerárquicamente los resultados.	• Elabora el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. • Construye una matriz comparativa para expresar los resultados.	• Elabora con errores el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. • Requiere apoyo para elaborar una matriz comparativa para expresar los resultados.	• Omite elaborar el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. • Desconoce el procedimiento para elaborar una matriz comparativa para expresar los resultados.
Requerimientos	**20**	• Determina correctamente los requerimientos de configuración de herramientas de seguridad. • Relaciona sistemáticamente los riesgos asociados a dichos requerimientos.	• Determina con algunos errores los requerimientos de configuración de herramientas de seguridad. • Relaciona los riesgos asociados a dichos requerimientos.	• Requiere apoyo para determinar los requerimientos de configuración de herramientas de seguridad. • Necesita ayuda para relacionar los riesgos asociados a dichos requerimientos.	• Desconoce la existencia de los requerimientos de configuración de las herramientas de seguridad y cómo relacionar los riesgos a dichos requerimientos.
Informe	**20**	• Elabora y entrega de manera impresa y digital los tres informes que se especifican a continuación: - Informe de resultados generados. - Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación. - Informe que contenga	• Elabora y entrega de manera impresa y digital dos de los tres informes que se especifican a continuación: - Informe de resultados generados. - Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación.	Elabora y entrega de manera impresa y/o digital uno de los tres informes que se especifican a continuación: - Informe de resultados generados. - Informe que contenga el balance de resultados obtenidos en la configuración de las herramientas de seguridad aplicadas a los equipos y redes de comunicación.	• Omite la elaboración y entrega de los informes requeridos.

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		los nuevos requerimientos y/o riesgos de seguridad identificados.	- Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados.	- Informe que contenga los nuevos requerimientos y/o riesgos de seguridad identificados	
Forma	**20**	• Presenta el informe en formato digital e impreso con las siguientes características: - Datos de identificación. - Lugar - Periodo. - Sistema auditado. - Características de la auditoría. - Resultados. - Responsables. - Firmas.	• Presenta el informe en formato digital e impreso omitiendo una de las siguientes características: - Datos de identificación. - Lugar. - Periodo. - Sistema auditado. - Características de la auditoría. - Resultados. - Responsables. - Firmas.	• Presenta el informe en formato digital o impreso omitiendo dos o más de las siguientes características: - Datos de identificación. - Lugar. - Periodo. - Sistema auditado. - Características de la auditoría. - Resultados. - Responsables. - Firmas.	• Presenta el informe impreso o digital de la auditoría en un formato diferente al requerido por el docente. • Omite la mayoría de la información requerida.
	100				