Guía pedagógica y de evaluación del módulo

Aplicación de la seguridad cibernética

Currículum Laboral

Área:
Tecnología y transporte

Carrera:
Profesional Técnico-Bachiller en Informática,
Soporte y mantenimiento de equipo de cómputo
y Telecomunicaciones

6º semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad cibernética

Área: Tecnología y transporte.

Carrera: PT-B Informática/ Soporte y mantenimiento de equipo de cómputo/ Telecomunicaciones

Semestre: Sexto

Horas por semana: 5

Fecha de diseño o actualización: 01 de julio de 2025

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

Directorio

Rodrigo Alejandro Rojas Navarrete
Dirección General

Ana María Rosas Muciño
Secretaría Académica

Patricia Alejandra Bernal Monzón
Dirección de Diseño Curricular

Desarrollo de portales de contenido y comercio

Contenido

I. Guía pedagógica

1. Descripción

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

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

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

2. Generalidades pedagógicas

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

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

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

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

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

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

3. Orientaciones didácticas

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

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

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

4. Estrategias de aprendizaje

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

- Exponer cómo los agentes de amenazas ejecutan algunos de los tipos más comunes de ataques cibernéticos.
- Describir amenazas, vulnerabilidades y ataques que ocurren en distintos dominios.
- Identificar métodos de engaño utilizados por atacantes para engañar a usuarios.
- Representar a través de diagramas los tipos de ataques a aplicaciones.
- Explicar los principios de seguridad de la red y cómo han evolucionado las amenazas de red.
- Explicar cómo las vulnerabilidades TCP/IP permiten que se ejecuten ataques a las redes.
- Utilizar las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.
- **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:

- Recomendar medidas para mitigar las amenazas.
- Resolver problemas de redes empresariales.
- Explicar cómo se emplean los dispositivos y servicios para reforzar la seguridad de las redes.
- Utilizar herramientas administrativas para configurar, monitorear y administrar los recursos del sistema.
- Implementar el monitoreo e investigación de la seguridad de la red.
- Evaluar la protección de terminales y los impactos del malware.
- **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:

- Realizar técnicas grupales al inicio y durante el desarrollo del curso para favorecer la unión, el trabajo colaborativo, mantener la motivación por el estudio y generar un clima armónico.

- Utilizar recursos audiovisuales para explicar conceptos y actividades a elaborar.
- Planificar actividades interactivas, utiliza distintos materiales y formatos para ayudar al estudiantado a la comprensión del contenido
- Exponer al estudiantado nuevas habilidades y conceptos.
- Parafrasear contenidos o definiciones demasiado técnicas de manera que la aprehensión por parte de los alumnos sea más sencilla.
- Formular preguntas que despierten el interés de los alumnos por los temas que comprende la unidad.
- Responder dudas e inquietudes de forma clara y haciendo hincapié en aquellos contenidos que puedan presentar dificultades de comprensión.
- **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:

- Explicar enfoques para la defensa de seguridad de la red.
- Practicar los diversos aspectos de la defensa de sistemas y redes.
- Configurar el control de acceso local y basado en el servidor.
- Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red.
- Explicar cómo se implementan los firewalls para proporcionar seguridad de red.
- **Realizar la actividad de evaluación 2.2.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 3.1, se recomienda al alumno:

- Crear documentos y políticas relacionados con el cumplimiento y la gobernanza de la ciberseguridad.
- Utilizar herramientas para probar la seguridad de la red.
- Evaluar las fuentes de información utilizadas para comunicar las amenazas emergentes a la seguridad de la red.
- Explicar cómo se evalúan y gestionan las vulnerabilidades de los dispositivos finales.

- Evaluar controles de seguridad de acuerdo a las características de la organización.
- Seleccionar controles de seguridad basados en los resultados de la evaluación de riesgos
- **Realizar la actividad de evaluación 3.1.1 considerando la rúbrica correspondiente**

Para el desarrollo del resultado de aprendizaje 3.2, se recomienda al alumno:

- Utilizar modelos de respuesta ante incidentes y técnicas para investigar incidentes de seguridad.
- Identificar los pasos en la cadena de eliminación cibernética.
- Realizar copias de seguridad de archivos y restaurar operaciones de red.
- Aplicar procedimientos de manejo de incidentes.
- Utilizar modelos de análisis de intrusiones.
- **Realizar la actividad de evaluación 3.2.1 considerando la rúbrica correspondiente**

5. Autonomía didáctica

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

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

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

II. Guía de evaluación

6. Descripción

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

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

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

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

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

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

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

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

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

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

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

7. Tabla de ponderación

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

Unidad de aprendizaje	Resultado de Aprendizaje	Actividad de Evaluación	% Peso Específico	% Peso Logrado	% Peso Acumulado
1. Evaluación de red, sistemas y puntos finales para la detección de vulnerabilidades en red empleando procedimientos de protección.	**1.1** Configura una red simulada de una organización empleando conceptos de ciberseguridad, medidas de mitigación y seguridad ante amenazas de red comunes y emergentes.	**1.1.1**	**15%**		
	1.2 Evalúa la seguridad del punto final y documenta una estrategia de seguridad en la red configurando medidas de seguridad en dispositivos de red y terminales para su protección.	**1.2.1**	**15%**		
% PESO PARA LA UNIDAD			**30%**		
2. Monitoreo y protección de red empleando configuraciones y alertas para la seguridad.	**2.1** Configura prácticas y procesos de defensa de la red de acuerdo con los principios y tecnologías de confidencialidad aplicados en la seguridad cibernética.	**2.1.1**	**20%**		
	2.2 Configura medidas y alertas de seguridad en la nube empleando los mecanismos tecnológicos, de monitoreo y criptografía aplicados en la seguridad cibernética.	**2.2.1**	**15%**		
% PESO PARA LA UNIDAD			**35%**		

3. Administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad.	**3.1** Evalúa vulnerabilidades y realiza la gestión de riesgos de red a través de herramientas y pruebas de seguridad a fin de establecer controles de seguridad.	**3.1.1**	**20%**		
	3.2 Utiliza modelos de respuesta ante incidentes de acuerdo con su tipo y características a fin de aplicar la ciberseguridad en la red.	**3.2.1**	**15%**		
% PESO PARA LA UNIDAD			**35%**		
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:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**1.1** Configura una red simulada de una organización empleando conceptos de ciberseguridad, medidas de mitigación y seguridad ante de amenazas de red comunes y emergentes			**Actividad de evaluación:**	**1.1.1** Realiza un diagrama describiendo la configuración de una red considerando la ciberseguridad, medidas de mitigación y seguridad ante amenazas de red comunes y emergentes		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Ataques a la ciberseguridad	**30**	Describe ataques a la ciberseguridad, considerando: • Ataques comunes • Métodos de engaño • Ataques cibernéticos • Ataques a dispositivos inalámbricos y móviles • Ataques a aplicaciones Incluye ejemplos de otros tipos de ataques a la ciberseguridad	Describe ataques a la ciberseguridad, considerando: • Ataques comunes • Métodos de engaño • Ataques cibernéticos • Ataques a dispositivos inalámbricos y móviles • Ataques a aplicaciones	Describe ataques a la ciberseguridad, considerando la mayoría de: • Ataques comunes • Métodos de engaño • Ataques cibernéticos • Ataques a dispositivos inalámbricos y móviles • Ataques a aplicaciones	Describe ataques a la ciberseguridad, omitiendo algunos de los siguientes elementos: • Ataques comunes • Métodos de engaño • Ataques cibernéticos • Ataques a dispositivos inalámbricos y móviles • Ataques a aplicaciones
Protección de redes y ataque a fundamentos	**30**	Describe la protección de redes, considerando: • Principios de seguridad de la red • Evolución de las amenazas de red • Vulnerabilidades TCP/IP Incluye ejemplo de la	Describe la protección de redes, considerando: • Principios de seguridad de la red • Evolución de las amenazas de red • Vulnerabilidades TCP/IP	Describe la protección de forma básica las redes, considerando: • Principios de seguridad de la red • Evolución de las amenazas de red • Vulnerabilidades TCP/IP	Describe la protección de redes, omitiendo alguno de los siguientes elementos: • Principios de seguridad de la red • Evolución de las amenazas de red • Vulnerabilidades TCP/IP

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		estructura d encabezado de IPv4 e IPv5			
Comunicación e infraestructura	**30**	Describe la comunicación e infraestructura de seguridad de redes, considerando: • Dispositivos inalámbricos • Amenazas WLAN • Problemas de conexión inalámbrica • Uso de dispositivos especializados • Uso de servicios de red Incluye ejemplo de una situación de seguridad de la red.	Describe la comunicación e infraestructura de seguridad de redes, considerando: • Dispositivos inalámbricos • Amenazas WLAN • Problemas de conexión inalámbrica • Uso de dispositivos especializados • Uso de servicios de red	Describe la comunicación e infraestructura de seguridad de redes de forma básica, considerando: • Dispositivos inalámbricos • Amenazas WLAN • Problemas de conexión inalámbrica • Uso de dispositivos especializados • Uso de servicios de red	Describe la comunicación e infraestructura de seguridad de redes, omitiendo alguno de los siguientes elementos: • Dispositivos inalámbricos • Amenazas WLAN • Problemas de conexión inalámbrica • Uso de dispositivos especializados • Uso de servicios de red
Diagrama **Autoevaluación**	**10**	Incluye los siguientes elementos: • Información concreta y organizada • Sin faltas de ortografía Incluye imágenes alusivas al tema. Además, incluye colores y símbolos para distinguir los elementos definidos.	Incluye los siguientes elementos: • Información concreta y organizada • Sin faltas de ortografía • Incluye imágenes alusivas al tema.	Incluye de forma parcial los siguientes elementos: • Información concreta y organizada • Sin faltas de ortografía • Incluye imágenes alusivas al tema	Omite algunos de los siguientes elementos: • Información concreta y organizada • Ortografía • Imágenes alusivas al tema.
	100				

Siglema:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**1.2** Evalúa la seguridad del punto final y documenta una estrategia de seguridad en la red configurando medidas de seguridad en dispositivos de red y terminales para su protección			**Actividad de evaluación:**	**1.2.1** Realiza un reporte escrito evaluando la seguridad del punto final considerando la estrategia de seguridad de red		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Sistema operativo	**30**	Describe el sistema operativo considerando los siguientes elementos: • Arquitectura y funcionamiento • Uso de herramientas administrativas • Procedimiento de mantenimiento seguro • Monitoreo e investigación de la seguridad de la red • Manejo de archivos de texto • Identificación de servidores • Monitoreo de archivos • Componentes básicos • Detección de malware Incluye ejemplo de una situación de seguridad en la red.	Describe el sistema operativo considerando los siguientes elementos: • Arquitectura y funcionamiento • Uso de herramientas administrativas • Procedimiento de mantenimiento seguro • Monitoreo e investigación de la seguridad de la red • Manejo de archivos de texto • Identificación de servidores • Monitoreo de archivos • Componentes básicos • Detección de malware	Describe de forma básica el sistema operativo considerando los siguientes elementos: • Arquitectura y funcionamiento • Uso de herramientas administrativas • Procedimiento de mantenimiento seguro • Monitoreo e investigación de la seguridad de la red • Manejo de archivos de texto • Identificación de servidores • Monitoreo de archivos • Componentes básicos • Detección de malware	Describe el sistema operativo omitiendo alguno de los siguientes elementos: • Arquitectura y funcionamiento • Uso de herramientas administrativas • Procedimiento de mantenimiento seguro • Monitoreo e investigación de la seguridad de la red • Manejo de archivos de texto • Identificación de servidores • Monitoreo de archivos • Componentes básicos • Detección de malware
		Realiza la evaluación de protección de terminales considerando los siguientes	Realiza la evaluación de protección de terminales considerando los	Realiza la evaluación de forma básica la protección de terminales considerando	Realiza la evaluación de protección de terminales omitiendo alguno de los

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Protección de terminales	**30**	elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware • Medidas de seguridad • Uso de herramientas de investigación • Incluye ejemplo de una situación de seguridad en la red.	siguientes elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware • Medidas de seguridad • Uso de herramientas de investigación	los siguientes elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware • Medidas de seguridad • Uso de herramientas de investigación	siguientes elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware • Medidas de seguridad • Uso de herramientas de investigación
Prácticas y procesos de ciberseguridad	**30**	Utiliza los principios, prácticas y procesos de ciberseguridad considerando: • Prácticas de confidencialidad, integridad y disponibilidad • Verificación de integridad de archivos • Contraste de los tres estados de datos • Contramedidas de ciberseguridad Incluye ejemplo de la situación de ciberseguridad.	Utiliza los principios, prácticas y procesos de ciberseguridad considerando de forma básica: • Prácticas de confidencialidad, integridad y disponibilidad • Verificación de integridad de archivos • Contraste de los tres estados de datos • Contramedidas de ciberseguridad	Utiliza los principios, prácticas y procesos de ciberseguridad considerando de forma parcial: • Prácticas de confidencialidad, integridad y disponibilidad • Verificación de integridad de archivos • Contraste de los tres estados de datos	Utiliza los principios, prácticas y procesos de ciberseguridad omitiendo algunos de los siguientes elementos: • Prácticas de confidencialidad, integridad y disponibilidad • Verificación de integridad de archivos • Contraste de los tres estados de datos • Contramedidas de ciberseguridad
Reporte	**10**	Incluye: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía	Incluye de forma básica: • Título remarcado • Información solicitada • Letra legible	Incluye de forma parcial: • Título remarcado • Información solicitada • Letra legible	No incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		• Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. Agrega un extra en su presentación.	• Colores llamativos • Imágenes alusivas • Sin faltas de ortografía y material manejable	• Colores llamativos • Imágenes alusivas • Sin faltas de ortografía y material manejable	• Material manejable • Y/o contiene faltas de ortografía
	100				

Siglema:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**2.1** Configura prácticas y procesos de defensa de la red de acuerdo con los principios y tecnologías de confidencialidad aplicados en la seguridad cibernética.			**Actividad de evaluación:**	**2.1.1** Describe a través de una presentación electrónica la configuración de prácticas y procesos de defensa de la red considerando los principios y tecnologías requeridos.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Defensa de la red	**30**	Describe la configuración de la defensa de red, considerando: • Uso de la estrategia de defensa en profundidad para protección de las redes. • Supervisión de amenazas en una organización • Políticas, reglamentos y normas de seguridad. Incluye ejemplo de la defensa de red.	Describe de forma básica la configuración de la defensa de red, considerando: • Uso de la estrategia de defensa en profundidad para protección de las redes. • Supervisión de amenazas en una organización • Políticas, reglamentos y normas de seguridad.	Describe de forma parcial la configuración de la defensa de red, considerando: • Uso de la estrategia de defensa en profundidad para protección de las redes. • Supervisión de amenazas en una organización • Políticas, reglamentos y normas de seguridad	Describe la configuración de la defensa de red, omitiendo alguno de los siguientes elementos: • Uso de la estrategia de defensa en profundidad para protección de las redes. • Supervisión de amenazas en una organización • Políticas, reglamentos y normas de seguridad.
Defensa del sistema y de la red	**30**	Describe la defensa del sistema y de la red, considerando: • Medidas de seguridad física • Medidas de seguridad para aplicaciones • Fortalecimiento de servicios y protocolos de la red.	Describe la defensa del sistema y de la red de forma básica, considerando: • Medidas de seguridad física • Medidas de seguridad para aplicaciones • Fortalecimiento	Describe la defensa del sistema y de la red de forma parcial, considerando: • Medidas de seguridad física • Medidas de seguridad para aplicaciones • Fortalecimiento	Describe la defensa del sistema y de la red, omitiendo alguno de los siguientes elementos: • Medidas de seguridad física • Medidas de seguridad para aplicaciones • Fortalecimiento de servicios y

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		• Segmentación de la red • Seguridad en routers • Seguridad en dispositivos IoT Incluye ejemplo de la defensa del sistema y de la red	de servicios y protocolos de la red. • Segmentación de la red Seguridad en routers Seguridad en dispositivos IoT	de servicios y protocolos de la red	protocolos de la red. • Segmentación de la red Seguridad en routers Seguridad en dispositivos IoT
Control de accesos	**30**	Describe la aplicación del control de acceso, considerando: • Configuración de acceso seguro en un host • Protección de datos de la red • Gestión de cuentas y estrategias de control Configuración de autenticación Incluye ejemplo del control de acceso	Describe la aplicación del control de acceso de forma basica, considerando: • Configuración de acceso seguro en un host • Protección de datos de la red • Gestión de cuentas y estrategias de control Configuración de autenticación	Describe la aplicación del control de acceso de forma parcial, considerando: • Configuración de acceso seguro en un host • Protección de datos de la red • Gestión de cuentas y estrategias de control Configuración de autenticación	Describe la aplicación del control de acceso, omitiendo alguno de los siguientes elementos: • Configuración de acceso seguro en un host • Protección de datos de la red • Gestión de cuentas y estrategias de control Configuración de autenticación
Presentación electrónica	**10**	Incluye: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo.	Incluye de forma básica lo siguiente: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar	Incluye de forma parcial lo siguiente: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar	Omite incuir la mayoría de lo siguiente: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		Agrega un extra ensu presentación.	• Pulcritud en su trabajo. Agrega un extra ensu presentación.	• Pulcritud en su trabajo	Pulcritud en su trabajo
	100				

Siglema:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**2.2** Configura medidas y alertas de seguridad en la nube empleando los mecanismos tecnológicos, de monitoreo y criptografía aplicados en la seguridad cibernética.			**Actividad de evaluación:**	**2.2.1** Demuestra la configuración de medidas y alertas de seguridad en la nube considerando los mecanismos establecidos.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Listas de control	**25**	Implementa listas de control de acceso, evidenciando: • Manejo de las listas de control estándar y extendidas de IPv4 • Uso de máscaras comodín • Configuración de listas de control de acceso • Implementación de listas de control • Mitigación de ataques • Configuración de listas IPv6 utilizando CLI Incluye ejemplos de la implementación.	Implementa listas de control de acceso, de forma básica evidenciando: • Manejo de las listas de control estándar y extendidas de IPv4 • Uso de máscaras comodín • Configuración de listas de control de acceso • Implementación de listas de control • Mitigación de ataques • Configuración de listas IPv6 utilizando CLI	Implementa listas de control de acceso, evidenciando de forma parcial: • Manejo de las listas de control estándar y extendidas de IPv4 • Uso de máscaras comodín • Configuración de listas de control de acceso • Implementación de listas de control • Mitigación de ataques Configuración de listas IPv6 utilizando CLI	Implementa listas de control de acceso, omitiendo algunos de los siguientes elementos: • Manejo de las listas de control estándar y extendidas de IPv4 • Uso de máscaras comodín • Configuración de listas de control de acceso • Implementación de listas de control • Mitigación de ataques Configuración de listas IPv6 utilizando CLI
Tecnologías firewall	**20**	Describe la aplicación de tecnologías firewall, evidenciando: • Uso para asegurar las redes • Consideraciones de	Describe la aplicación de tecnologías firewall, evidenciando de forma básica: • Uso para asegurar las redes • Consideraciones de	Describe la aplicación de tecnologías firewall, evidenciando de forma parcial: • Uso para asegurar las redes • Consideraciones de diseño	Describe la aplicación de tecnologías firewall, omitiendo alguno de los siguientes elementos: • Uso para asegurar las redes • Consideraciones de

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		diseño • Uso y funcionamiento de firewalls de políticas • Configuración basada en zonas con la CLI Incluye ejemplos de las tecnologías.	diseño • Uso y funcionamiento de firewalls de políticas • Configuración basada en zonas con la CLI	• Uso y funcionamiento de firewalls de políticas • Configuración basada en zonas con la CLI	diseño • Uso y funcionamiento de firewalls de políticas Configuración basada en zonas con la CLI
Seguridad en la nube	**20**	Describe los dominios de ciberseguridad, evidenciando: • Dominios en la tríada • Pertenencia • Áreas de ciberseguridad • Profesionales • Incluye ejemplos de dominios.	Describe los dominios de ciberseguridad, evidenciando de forma básica: • Dominios en la tríada • Pertenencia • Áreas de ciberseguridad • Profesionales • Incluye ejemplos de dominios	Describe los dominios de ciberseguridad, evidenciando de forma parcial: • Dominios en la tríada • Pertenencia • Áreas de ciberseguridad • Profesionales • Incluye ejemplos de dominios	Describe los dominios de ciberseguridad, omitiendo algunos de los siguientes elementos: • Dominios en la tríada • Pertenencia • Áreas de ciberseguridad Profesionales
Criptografía, tecnologías y protocolos	**25**	Describe la aplicación de la criptografía, tecnologías y protocolos, evidenciando: • Uso de herramientas de hash • Algoritmo cifrado de acuerdo con requisitos • Técnica para oscurecer datos • Garantías para a la integridad y autenticidad • Tecnologías de seguridad • Monitoreo de protocolos	Describe la aplicación de la criptografía, tecnologías y protocolos, evidenciando de forma básica: • Uso de herramientas de hash • Algoritmo cifrado de acuerdo con requisitos • Técnica para oscurecer datos • Garantías para a la integridad y autenticidad • Tecnologías de seguridad	Describe la aplicación de la criptografía, tecnologías y protocolos, evidenciando de forma parcial: • Uso de herramientas de hash • Algoritmo cifrado de acuerdo con requisitos • Técnica para oscurecer datos • Garantías para a la integridad y autenticidad • Tecnologías de seguridad • Monitoreo de protocolos	Describe la aplicación de la criptografía, tecnologías y protocolos, omitiendo algunos de los siguientes elementos: • Uso de herramientas de hash • Algoritmo cifrado de acuerdo con requisitos • Técnica para oscurecer datos • Garantías para a la integridad y autenticidad • Tecnologías de

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		• Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas • Incluye ejemplos de criptografía, tecnologías y protocolos.	• Monitoreo de protocolos • Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas • Incluye ejemplos de criptografía, tecnologías y protocolos.	• Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas • Incluye ejemplos de criptografía, tecnologías y protocolos.	seguridad • Monitoreo de protocolos • Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas • Incluye ejemplos de criptografía, tecnologías y protocolos
Reporte escrito **Coevaluación**	**10**	Incluye: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. Agrega un extra en su presentación	Incluye de forma básica: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. Agrega un extra en su presentación	Incluye de forma básica: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo.	Carece de la mayoría de los elementos: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Y/o contiene faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo.
	100				

Siglema:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**3.1** Evalúa vulnerabilidades y realiza la gestión de riesgos de red a través de herramientas y pruebas de seguridad a fin de establecer controles de seguridad.			**Actividad de evaluación:**	**3.1.1** Realiza un reporte escrito sobre la evaluación de vulnerabilidades y la gestión de riesgos conforme a las pruebas establecidas.		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Gestión y cumplimiento	**30**	Describe la gestión y cumplimiento de la ciberseguridad, evidenciando: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad • Incluye ejemplo aplicado de la gestión y cumplimiento.	Describe la gestión y cumplimiento de la ciberseguridad, evidenciando de forma básica: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad • Incluye ejemplo aplicado de la gestión y cumplimiento.	Describe la gestión y cumplimiento de la ciberseguridad, evidenciando de forma parcial: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad • Incluye ejemplo aplicado de la gestión y cumplimiento.	Describe la gestión y cumplimiento de la ciberseguridad, omitiendo algunos de los siguientes elementos: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad • Incluye ejemplo aplicado de la gestión y cumplimiento
Pruebas de seguridad e inteligencia	**30**	Realiza pruebas de seguridad e inteligencia, evidenciando: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad • Herramientas de	Realiza pruebas de seguridad e inteligencia, evidenciando de forma básica: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad • Herramientas de pruebas	Realiza pruebas de seguridad e inteligencia, evidenciando de forma parcial: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad • Herramientas de pruebas	Realiza pruebas de seguridad e inteligencia, omitiendo algunos de los siguientes elementos: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		pruebas • Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas Incluye ejemplos de servicios de inteligencias de amenazas.	• Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas	• Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas	• Herramientas de pruebas • Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas
Administración de riesgos y controles de seguridad	**20**	Realiza la administración de riesgos y controles de seguridad, evidenciando: • Evaluación de vulnerabilidades de los dispositivos finales • Uso de informes CVSS • Técnicas de gestión segura • Administración de riesgos • Cálculo de riesgos • Controles de seguridad • Incluye resumen de la evaluación de la vulnerabilidad y gestión de riesgos.	Realiza la administración de riesgos y controles de seguridad, evidenciando de forma básica: • Evaluación de vulnerabilidades de los dispositivos finales • Uso de informes CVSS • Técnicas de gestión segura • Administración de riesgos • Cálculo de riesgos • Controles de seguridad • Incluye resumen de la evaluación de la vulnerabilidad y gestión de riesgos.	Realiza la administración de riesgos y controles de seguridad, evidenciando de forma parcial: • Evaluación de vulnerabilidades de los dispositivos finales • Uso de informes CVSS • Técnicas de gestión segura • Administración de riesgos • Cálculo de riesgos • Controles de seguridad • Incluye resumen de la evaluación de la vulnerabilidad y gestión de riesgos.	Realiza la administración de riesgos y controles de seguridad, omitiendo algunos de los siguientes elementos: • Evaluación de vulnerabilidades de los dispositivos finales • Uso de informes CVSS • Técnicas de gestión segura • Administración de riesgos • Cálculo de riesgos • Controles de seguridad • Incluye resumen de la evaluación de la vulnerabilidad y gestión de riesgos.
Reporte escrito	**20**	• Incluye: • Título remarcado • Información solicitada • Sin faltas de ortografía • Colores atractivos a la vista	• Incluye de forma básica • Título remarcado • Información solicitada • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía	• Incluye de forma parcial • Título remarcado • Información solicitada • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía	• No omite reporte de algunos de los contenidos: • Título remarcado • Información solicitada • Colores llamativos

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		• Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra ensu presentación.	• Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra ensu presentación	• Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra ensu presentación	• Imágenes alusivas • Y/o contiene faltas de ortografía • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra ensu presentación
	100				

Siglema:	**ASCI-20**	**Nombre del módulo:**	**Aplicación de la seguridad cibernética**	**Nombre del alumno:**			
Docente evaluador:				**Grupo:**		**Fecha:**	
Resultado de aprendizaje:	**3.2** Utiliza modelos de respuesta ante incidentes de acuerdo con su tipo y características a fin de aplicar la ciberseguridad en la red.			**Actividad de evaluación:**	**3.2.1** Demuestra la aplicación del análisis digital y la respuesta a incidentes considerando los procedimientos establecidos. **HETEROEVALUACIÓN**		

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
Análisis digital	**40**	• Realiza el análisis digital evidenciando los siguientes elementos: • Procesos de análisis digitales • Cadena de eliminación cibernética • Uso de modelos de análisis de intrusiones • Manejo de incidentes • Restauración de operaciones y copias de seguridad • Incluye ejemplos de restauración de operaciones de red.	• Realiza el análisis digital evidenciando los siguientes elementos de forma básica: • Procesos de análisis digitales • Cadena de eliminación cibernética • Uso de modelos de análisis de intrusiones • Manejo de incidentes • Restauración de operaciones y copias de seguridad • Incluye ejemplos de restauración de operaciones de red.	• Realiza el análisis digital evidenciando los siguientes elementos de forma parcial: • Procesos de análisis digitales • Cadena de eliminación cibernética • Uso de modelos de análisis de intrusiones • Manejo de incidentes • Restauración de operaciones y copias de seguridad • Incluye ejemplos de restauración de operaciones de red.	• Realiza el análisis digital omitiendo algunos de los siguientes elementos: • Procesos de análisis digitales • Cadena de eliminación cibernética • Uso de modelos de análisis de intrusiones • Manejo de incidentes • Restauración de operaciones y copias de seguridad • Incluye ejemplos de restauración de operaciones de red
Respuesta a incidentes	**40**	Aplica la respuesta a incidentes, evidenciando: • Tipo de incidente • Procedimiento • Partes interesadas • Ciclo de vida • Detección y análisis • Procedimiento	• Aplica la respuesta a incidentes, evidenciando de forma básica: • Tipo de incidente • Procedimiento • Partes interesadas	• Aplica la respuesta a incidentes, evidenciando de forma parcial: • Tipo de incidente • Procedimiento • Partes interesadas	• Aplica la respuesta a incidentes, omitiendo algunos de los siguientes elementos: • Tipo de incidente • Procedimiento • Partes interesadas

INDICADORES	%	C R I T E R I O S			
		Excelente	**Bueno**	**Suficiente**	**Insuficiente**
		respuesta a incidentes • Recuperación ante desastres Incluye ejemplos de recuperación ante desastres.	• Ciclo de vida • Detección y análisis • Procedimiento respuesta a incidentes • Recuperación ante desastres	• Ciclo de vida • Detección y análisis • Procedimiento respuesta a incidentes • Recuperación ante desastres	• Ciclo de vida • Detección y análisis • Procedimiento respuesta a incidentes • Recuperación ante desastres
Reporte escrito	**20**	• Incluye: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista • Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra en su presentación.	• • Incluye de forma básica: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra en su presentación	• Incluye de forma parcial:Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra en su presentación	• Omite la mayoría de los siguientes elementos: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Y/o contiene faltas de ortografía • Sin faltas de ortografía • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. • Agrega un extra en su presentación
	100				