Guía pedagógica y de evaluación del módulo

Aplicación de la seguridad cibernética

Núcleo de Formación Profesional

Área:
Tecnología y transporte

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

6° semestre

Editor: Colegio Nacional de Educación Profesional Técnica

Módulo: Aplicación de la seguridad cibernética.

Área: Tecnología y transporte.

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

Semestre: 6°

Horas por semestre: 90

Créditos por semestre: 9

Fecha de diseño o actualización: 20 de octubre de 2023.

Vigencia: a partir de la aprobación de la junta directiva y en tanto no se genere un documento que lo anule o actualice.

Directorio

Manuel de Jesús Espino
Dirección General

Lauro Cordero Frayre
Secretaría General

Hugo Nicolás Pérez González
Secretaría Académica

Edith Chávez Ramos
Dirección de Diseño Curricular

Aplicación de la seguridad cibernética

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

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

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

2. Generalidades pedagógicas

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

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

Los principios asociados a la concepción constructivista del aprendizaje mantienen una estrecha relación con los de la educación basada en competencias, la cual se ha concebido en el Colegio como el enfoque idóneo para orientar la formación ocupacional de los futuros profesionales técnicos-bachiller. Este enfoque constituye una de las opciones más viables para lograr la vinculación entre la educación y el sector productivo de bienes y servicios.

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

El alumno:	El docente:
❖ Mejora su capacidad para resolver problemas. ❖ Aprende a trabajar en grupo y a comunicar sus ideas. ❖ Aprende a buscar información y a procesarla. ❖ Construye su conocimiento. ❖ Adopta una posición crítica y autónoma.	❖ Organiza su formación continua a lo largo de su trayectoria profesional. ❖ Domina y estructura los saberes para facilitar experiencias de aprendizaje significativo. ❖ Planifica los procesos de enseñanza y de aprendizaje atendiendo al enfoque por competencias, y los ubica en contextos disciplinares, curriculares y sociales amplios. ❖ Lleva a la práctica procesos de enseñanza y de aprendizaje de manera efectiva, creativa e innovadora a su contexto institucional. ❖ Evalúa los procesos de enseñanza y de aprendizaje con un enfoque formativo. ❖ Construye ambientes para el aprendizaje autónomo y colaborativo.

❖ Realiza los procesos de autoevaluación y coevaluación.	❖ Contribuye a la generación de un ambiente que facilite el desarrollo sano e integral de los estudiantes. ❖ Participa en los proyectos de mejora continua de su escuela y apoya la gestión institucional.

El docente, en lugar de transmitir vertical y unidireccionalmente los conocimientos, es un mediador del aprendizaje, ya que:

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

3. Orientaciones didácticas

Para el desarrollo de las competencias del módulo se recomienda al docente:

- Realizar el encuadre del módulo, tomar acuerdos sobre la forma de trabajar y evaluar con la finalidad de cumplir con las competencias enunciadas en el módulo.
- Definir claramente las actividades y tareas a realizar.
- Fomentar la asistencia a clases.
- Fomentar un ambiente grupal de confianza y respeto para que los alumnos se sientan en libertad de exponer preguntas y/o dudas sobre los contenidos revisados en el módulo.
- Comunicar, escuchar, observar y atender las necesidades educativas y personales del alumno a fin de realimentar su formación académica y reforzar su relación para el desarrollo personal.
- Seleccionar recursos didácticos relacionados con los contenidos enunciados en el módulo.
- Fomentar la democracia y la equidad al tomar acuerdos con el grupo, organizando y dirigiendo situaciones de aprendizaje que promuevan el interés y la participación a través de lo siguiente:
    - Distribución de tareas
    - Preparación de clases con secuencia lógica
    - Proporcionar y recabar información; confiable, relevante y completa
    - Establecimiento de tiempos y formas para el desarrollo de temas y trabajos
- Promover la investigación previa y permanente, lo que permitirá al alumno participar activamente durante el desarrollo de temas y potenciará su habilidad para realizar análisis crítico de los materiales bibliográficos para construir nuevos conocimientos y aprendizajes significativos.
- Fomentar el trabajo individual, por equipo y grupal con la finalidad de promover la generación de nuevas ideas y el trabajo colaborativo.
- Utilizar experiencias personales y profesionales en el campo laboral, ejercicios, ejemplos de casos reales, etc., que le permitan al alumno relacionar aprendizajes previos con nuevos.
- Plantear casos prácticos en los que el alumno pueda poner en práctica lo aprendido en el módulo.
- Administrar la progresión de los aprendizajes, mediante el registro de avances y dificultades durante el desarrollo del programa, como un medio de guiar la realimentación.
- Considerar los tres tipos de evaluación: diagnóstica, formativa y sumativa.

4. Estrategias de aprendizaje por unidad

Unidad:	**1.** Evaluación de red, sistemas y puntos finales para la detección de vulnerabilidades en red empleando procedimientos de protección.

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

- 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 alumno:

- 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**

Unidad:	**2.** Monitoreo y protección de red empleando configuraciones y alertas para la seguridad.

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

- 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 alumno:

- 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.

- Implementar firewall basado en políticas de zona mediante la CLI.
- Recomendar requisitos de seguridad en la nube basados en un escenario de nube determinado.
- Explicar cómo utilizar las herramientas de hash.
- Explicar cómo las tecnologías de seguridad afectan el monitoreo de la seguridad.
- Utilizar diferentes tipos de logs y registros para almacenar información sobre los hosts y la red.
- Explicar el proceso de evaluación de alertas.
- **Realizar la actividad de evaluación 2.2.1 considerando la rúbrica correspondiente**

Unidad:	**3.** Administración de amenazas cibernéticas a través de la gestión de riesgos para responder a incidentes de seguridad.

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. Prácticas y actividades

En respeto a la libertad de cátedra, este apartado quedará bajo la responsabilidad de los docentes para que, de acuerdo con su experiencia, las características del grupo y el desempeño de los estudiantes, seleccione, proponga y realice aquellas que garanticen un mayor desarrollo de competencias, 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 docente implica, ante todo, una labor de investigación y promoción del autoaprendizaje para ofrecer a los educandos la información más actualizada, así como las actividades que permitan un mayor logro de los objetivos educacionales, considerando las características del grupo y del contexto en donde se desarrolla el proceso de enseñanza-aprendizaje, ya sea en el sistema presencial o en el mixto.

En este sentido, se confía en el docente como un líder que fomenta la creatividad y el emprendimiento, considerando que el aprendizaje se dará de mejor manera si el alumno relaciona la teoría con la vida diaria, con la resolución de problemas, brindando las bases científicas de la práctica, a fin de transformar el mundo concreto.

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

Derivado de lo anterior, para promover en los alumnos el “saber hacer” integrando conocimientos, habilidades y actitudes, se sugiere la planeación de actividades y prácticas que vayan de lo más simple a lo más complejo, de lo conocido a lo desconocido, en escenarios lo más reales posible, para alcanzar los logros establecidos en los Resultados de Aprendizaje y con ello, lograr la vinculación de la teoría con la práctica.

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

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

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

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

Finalmente, la evaluación **sumativa** es adoptada básicamente por una función social, ya que, mediante ella, se asume una acreditación, una promoción, un fracaso escolar, índices de deserción, etc., a través de criterios estandarizados y bien definidos. Las evidencias se

elaboran en forma individual, puesto que se está asignando, convencionalmente, un criterio o valor. Manifiesta la síntesis de los logros obtenidos por ciclo o período escolar.

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

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

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

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

De acuerdo con lo anterior, en las rúbricas se sugiere el momento para que se lleven a cabo estas 3 modalidades de evaluación: un indicador para que los alumnos practiquen la auto y la coevaluación, y una actividad de evaluación para que un docente externo al grupo evalúe el desempeño del alumno a través de la rúbrica.

Cada uno de los Resultados de Aprendizaje (RA) tiene asignada al menos una actividad de evaluación (AE), a la cual se le ha determinado una ponderación con respecto a la Unidad a la cual pertenece. Ésta a su vez, tiene una ponderación que, sumada con el resto de Unidades, conforma el 100%. Es decir, para considerar que se ha adquirido la competencia correspondiente al módulo, deberá ir acumulando dichos porcentajes a lo largo del período para estar en condiciones de acreditar el mismo. Cada una de estas ponderaciones dependerá de la relevancia que tenga dicha actividad con respecto al RA y éste a su vez, con respecto a la Unidad de Aprendizaje.

La ponderación que se asigna en cada una de las actividades queda establecida en la Tabla de ponderación, la cual está desarrollada en una hoja de cálculo que permite, tanto al alumno como al docente, ir observando y calculando los avances en términos de porcentaje, que se van alcanzando. Esta tabla de ponderación contiene los Resultados de Aprendizaje y las Unidades a las cuales pertenecen. Asimismo, indica, en la columna de actividades de evaluación, la codificación asignada a ésta desde el programa de estudios y que a su vez queda vinculada al Sistema de Evaluación Escolar SAE. Las siguientes tres columnas indican, en términos de porcentaje: la primera el peso específico asignado desde el programa de estudios para esa actividad; la segunda, peso logrado, es el nivel que el alumno alcanzó con base en las evidencias o desempeños demostrados; la tercera, peso acumulado, se refiere a la suma de los porcentajes alcanzados en las diversas actividades de evaluación y que deberá acumular a lo largo del ciclo escolar.

Otro elemento que complementa a la matriz de ponderación es la rúbrica o matriz de valoración, que establece los indicadores y criterios a considerar para evaluar, ya sea un producto, un desempeño o una actitud. Una rúbrica es, como su nombre lo indica, una matriz de doble entrada en la cual se establecen, por un lado, los indicadores o aspectos específicos que se deben tomar en cuenta como mínimo indispensable para evaluar si se ha logrado el resultado de aprendizaje esperado y, por otro, los criterios o niveles de calidad o satisfacción alcanzados. En las celdas centrales se describen los criterios que se van a utilizar para evaluar esos indicadores, explicando cuáles son las características de cada uno. Los criterios que se han establecido son: Excelente, en el cual, además de cumplir con los estándares o requisitos establecidos como necesarios en el logro del producto o desempeño, es propositivo, demuestra iniciativa y creatividad, o que va más allá de lo que se le solicita como mínimo, aportando elementos adicionales en pro del indicador; Suficiente, si cumple con los estándares o requisitos establecidos como necesarios para demostrar que se ha desempeñado adecuadamente en la actividad o elaboración del producto. Es en este nivel en el que podemos decir que se ha adquirido la competencia. Insuficiente, para cuando no cumple con los estándares o requisitos mínimos establecidos para el desempeño o producto.

Asimismo, es necesario que el docente realice la captura de la evaluación de los resultados de aprendizaje en el Sistema de Administración Escolar (SAE), considerando las fechas de corte establecidas en el calendario escolar del Sistema CONALEP, a fin de no afectar el desempeño de los alumnos y disminuir los índices de reprobación y abandono escolar.

7. Tabla de ponderación

UNIDAD	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.	**3.3.1**	**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**		
			35		
PESO TOTAL DEL MÓDULO			**100%**		

8. Matriz de valoración o rúbrica

Siglema:	**ASCI-00**	**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 de amenazas de red comunes y emergentes

INDICADORES	%	C R I T E R I O S		
		Excelente	**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, omitiendo alguno 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 estructura d encabezado de IPv4 e IPv5	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 redes, omitiendo alguno de los siguientes elementos: • Principios de seguridad de la red • Evolución de las amenazas de red • Vulnerabilidades TCP/IP

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, 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	Omite alguno de los siguientes elementos: • Información concreta y organizada • Ortografía • Imágenes alusivas al tema
	100			

Siglema:	**ASCI-00**	**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.** Realizar 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	**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 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
Protección de terminales	30	Realiza la evaluación de protección de terminales considerando los siguientes elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware	Realiza la evaluación de protección de terminales considerando los siguientes elementos: • Procedimientos de protección a los sistemas • Métodos de mitigación de malware	Realiza la evaluación de protección de terminales omitiendo alguno de los siguientes 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.	• Medidas de seguridad • Uso de herramientas de investigación	• 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: • 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 omitiendo alguno 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 • 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: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía y material manejable	No incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Material manejable Y/o contiene faltas de ortografía
	100			

Siglema:	**ASCI-00**	**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	**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 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. • Segmentación de la red • Seguridad en routers • Seguridad en dispositivos IoT Incluye ejemplo de la defensa del sistema y de la red	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. • Segmentación de la red • Seguridad en routers Seguridad en dispositivos IoT	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 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, 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. Agrega un extra en su presentación.	Incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía	No incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas Y/o contiene faltas de ortografía
	100			

Siglema:	**ASCI-00**	**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	**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, 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, omitiendo alguno 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 diseño • Uso y funcionamiento de firewalls de políticas • Configuración basada en zonas con la CLI Incluye ejemplos de las tecnologías.	Describe la aplicación de tecnologías firewall, evidenciando: • Uso para asegurar las redes • Consideraciones de diseño • Uso y funcionamiento de firewalls de políticas • Configuración basada en zonas con la CLI	Describe la aplicación de tecnologías firewall, omitiendo alguno de los siguientes elementos: • Uso para asegurar las redes • Consideraciones de 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 la aplicación de la seguridad en la nube, evidenciando: • Formas de gestionar amenazas en la nube • Dominios de la seguridad en la nube • Mitigación de amenazas a la infraestructura • Aplicaciones de seguridad • Asegurar datos en la nube • Asegurar instancias de las máquinas virtuales	Describe los dominios de ciberseguridad, omitiendo alguno 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 • Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas Incluye ejemplos de criptografía, tecnologías y protocolos.	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 • Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas	Describe la aplicación de la criptografía, tecnologías y protocolos, omitiendo alguno 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 seguridad • Monitoreo de protocolos • Datos de seguridad • Registro de terminales y redes • Proceso de evaluación de alertas
Reporte escrito Coevaluación	10	Incluye: • Título remarcado • Información solicitada • Letra legible y de buen tamaño • Sin faltas de ortografía • Colores atractivos a la vista	Incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas	No incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas

		• Imágenes y/o diagramas • Incluye datos que considera claves para recordar • Pulcritud en su trabajo. Agrega un extra en su presentación.	• Sin faltas de ortografía De material manejable	Y/o contiene faltas de ortografía
	100			

Siglema:	**ASCI-00**	**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** 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	**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: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad	Describe la gestión y cumplimiento de la ciberseguridad, omitiendo alguno de los siguientes elementos: • Documentos de política de ciberseguridad • Creación de código • Evaluación de controles de seguridad
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 pruebas • Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas Incluye ejemplos de servicios de inteligencias de amenazas.	Realiza pruebas de seguridad e inteligencia, evidenciando: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad • Herramientas de pruebas • Pruebas para evaluar seguridad • Evaluación de fuentes de inteligencia de amenazas	Realiza pruebas de seguridad e inteligencia, omitiendo alguno de los siguientes elementos: • Uso de herramientas para recopilar información • Diagnóstico de conectividad • Técnicas para pruebas de seguridad • 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: • Evaluación de vulnerabilidades de los dispositivos finales • Uso de informes CVSS • Técnicas de gestión segura • Administración de riesgos • Cálculo de riesgos • Controles de seguridad	Realiza la administración de riesgos y controles de seguridad, omitiendo alguno 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
Reporte escrito	20	Incluye: • Título remarcado • Información solicitada • 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: • Título remarcado • Información solicitada • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía	No incluye: • Título remarcado • Información solicitada • Colores llamativos • Imágenes alusivas • Y/o contiene faltas de ortografía
	100			

Siglema:	**ASCI-00**	**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	**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: • 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	Realiza el análisis digital omitiendo alguno 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
Respuesta a incidentes	40	Aplica la respuesta a incidentes, evidenciando: • Tipo de incidente • Procedimiento • Partes interesadas • Ciclo de vida • Detección y análisis • Procedimiento respuesta a incidentes • Recuperación ante desastres Incluye ejemplos de recuperación ante desastres.	Aplica la respuesta a incidentes, evidenciando: • Tipo de incidente • Procedimiento • Partes interesadas • Ciclo de vida • Detección y análisis • Procedimiento respuesta a incidentes • Recuperación ante desastres	Aplica la respuesta a incidentes, omitiendo alguno de los siguientes elementos: • Tipo de incidente • Procedimiento • Partes interesadas • 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: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas • Sin faltas de ortografía	No incluye: • Título remarcado • Información solicitada • Letra legible • Colores llamativos • Imágenes alusivas Y/o contiene faltas de ortografía
	100			