Programa de Estudios de la Unidad de Aprendizaje: CIBERSEGURIDAD

Clave:	6FP-FM1312	Créditos:	3.37

Ramas de Conocimiento

Ingeniería y Ciencias Físico Matemáticas	X	Ciencias Sociales Administrativas		Ciencias Médico Biológicas	

Área de Formación Curricular

Institucional		Científica, Humanística y Tecnológica Básica		Profesional	X

Tipo de Espacio

Aula	X	Taller		Laboratorio	X	Otros ambientes de Aprendizaje	

Modalidad

Escolarizada	X	No Escolarizada		Mixta	

Vigencia a Partir:	ENERO 2025

Proceso de Diseño y Autorización:			Día	Mes	Año
Elaborado por:	REP. ACAD. NMS	Fecha de Elaboración:	05	09	2024
Revisado por:	DEMS	Fecha de Revisión:	25	11	2024
Aprobado por:	CTCE-NMS	Fecha de Aprobación:	09	12	2024
Autorizado por:	CPA-CGC	Fecha de Autorización:	13	12	2024

Programa Académico:	TÉCNICO EN PROGRAMACIÓN

Nivel:	1°	2°	3°	4°	5°	6°

Unidades Académicas donde se Imparte:

TODAS LAS U.A.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	CET1

Tiempos Asignados:

Global:	54	Hrs/18 semanas/Semestre		
Aula:	1	Hrs/Semana	Total: 18	Hrs/Semestre
Taller:	-	Hrs/Semana	Total: -	Hrs/Semestre
Laboratorio:	2	Hrs/Semana	Total: 36	Hrs/Semestre
Otros ambientes de aprendizaje:	-	Hrs/Semana	Total: -	Hrs/Semestre

Organización

Por Unidad de Aprendizaje:	X	Por Área:		Por Módulo:	

Firma y Sello de Autorización

PODER EJECUTIVO FEDERAL · ESTADOS UNIDOS MEXICANOS · MÉXICO CDMX

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

M. EN E.N.A. MARÍA ISABEL ROJAS RUIZ
Directora de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

FUNDAMENTACIÓN

La unidad de aprendizaje **Ciberseguridad** pertenece al área de formación profesional del Bachillerato Tecnológico Bivalente del Nivel Medio Superior del Instituto Politécnico Nacional, se ubica en el sexto nivel del Plan de Estudios del Programa Académico Técnico en Programación y se imparte en la modalidad escolarizada, de manera obligatoria en la rama del conocimiento de Ingeniería y Ciencias Físico-Matemáticas.

La presente Unidad de Aprendizaje introduce al estudiante en el mundo de la ciberseguridad, partiendo de una comprensión de la misma como una dimensión científica, técnica, tecnológica, social, responsable y metodológica, al igual que proporciona las herramientas conceptuales, procedimentales y actitudinales necesarias para identificar, analizar, diseñar, optimizar e innovar soluciones a problemas de seguridad en sistemas, aplicaciones o proyectos, de manera efectiva, con pensamiento crítico- analítico, razonamiento abstracto, creatividad, iniciativa, y diversas habilidades cognitivas, así como principios y dimensiones del desarrollo humano, sostenible y con perspectiva de género.

Ciberseguridad es una unidad de aprendizaje que se enfoca en el desarrollo de habilidades técnicas, cognitivas y socioemocionales inherentes al estudio, análisis, aplicación y resolución de problemas en ciberseguridad, por ello se emplearán metodologías didácticas activas como: el Aprendizaje Basado en Problemas y el Aprendizaje Basado en Retos, como apoyo al desarrollo de competencias de un entorno actualizado, trabajo colaborativo, trabajo en equipo, reto al cambio, autodirección, resolución de problemas cercanos a la realidad, autogestión del aprendizaje y resiliencia. Además, de emplear herramientas tecnológicas que fomentarán la colaboración e interacción presenciales y en línea en forma síncrona o asíncrona, que corresponden a la educación actual.

El rol del docente será de mediador entre el estudiante y los contenidos didácticos a abordar, puesto que se centrará en la creación, organización, supervisión y mediación de los espacios de trabajo, incluidas las aulas virtuales, los ciberespacios, sin dejar de atender las necesidades técnicas, de conocimientos, apoyo logístico y metodológico en los procesos de aprendizaje individual y grupal, con el objetivo de generar ambientes que favorezcan la educación técnica, inclusiva, flexible, sustentable y con perspectiva de género.

El estudiante desarrollará un trabajo autónomo en diferentes ambientes de aprendizaje, organizará el trabajo de manera independiente y articulará saberes de diversos campos del conocimiento, que le posibilitarán construir y expresar su propio conocimiento en beneficio de la sociedad; también adquirirá habilidades tanto tecnológicas como personales que promoverán la comunicación asertiva, la creatividad, la negociación, la gestión del tiempo, la motivación, el liderazgo y la responsabilidad social vinculada a la protección del medio ambiente, la erradicación de toda manifestación de violencia de género, la inclusión y la accesibilidad.

La evaluación se efectuará en el marco de la evaluación auténtica, por esto, comprenderá tres momentos: diagnóstica, formativa y sumativa. La evaluación diagnóstica se llevará a cabo mediante una charla informal sobre conocimientos previos con evaluación y retroalimentación durante el mismo momento, con la finalidad de que el docente efectúe los ajustes didácticos pertinentes y de ser necesario, nivele y ajuste los conocimientos previos adquiridos en otras unidades de aprendizaje para que establezca conexiones significativas con las unidades didácticas de la unidad de aprendizaje. Un segundo momento de la evaluación hace referencia a la evaluación formativa, que se desarrollará a lo largo del proceso de enseñanza-aprendizaje mediante las secuencias didácticas y actividades de aprendizaje formativas que estimulen el aprendizaje activo y significativo del estudiante. Este momento se enriquecerá con diversos tipos de evaluación, como la autoevaluación, la coevaluación y heteroevaluación, puesto que coadyuvarán a dar seguimiento al desarrollo de los saberes y habilidades en contexto. Cabe señalar que estas clases de evaluación serán reforzadas a través de la retroalimentación efectiva y constante.

En el tercer momento de la evaluación, con fines de acreditación, se diseñarán escenarios con problemas comunes que permitan recuperar el nivel de logro y conducir al estudiante a la meta cognición en la unidad de aprendizaje **Ciberseguridad**, mediante evidencias de conocimiento, comprensión y diseño de algoritmos, escritura de programas en algún lenguaje de programación, compilación de los programas escritos, entre otras evidencias de aprendizaje, cuyos criterios, aspectos e indicadores serán conocidos por los estudiantes en forma previa. Las evidencias de evaluación formativa e integradora mostrarán el saber hacer de manera reflexiva de los estudiantes, utilizando el conocimiento que van adquiriendo durante el proceso didáctico para luego transferir y aplicar este aprendizaje en contextos escolares, sociales y laborales.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: **Técnico en Programación**

Unidad de Aprendizaje: **Ciberseguridad**

En base a la flexibilidad curricular y en el reconocimiento de aprendizajes múltiples, también podrá aplicarse una evaluación general para verificar que los conocimientos adquiridos por el estudiante demuestren que domina los saberes, objetivos y alcances de la **Ciberseguridad**, al finalizar el periodo ordinario. De esa forma, el programa de estudios de esta unidad de aprendizaje establece estándares para el desarrollo de conocimientos, habilidades socioemocionales, actitudes y valores.

La dinámica de trabajo en la unidad de aprendizaje será de forma individual y en algunas actividades en equipos. Por esta situación se debe contar con un docente titular y un docente auxiliar ya que los productos y actividades que desarrolle el estudiante durante el periodo semestral serán integradas en un portafolio de evidencias de aprendizaje y las actividades que se trabaje de forma individual se registrarán en un portafolio colaborativo. La importancia de contar con este docente tiene el objetivo de reforzar el aprendizaje significativo de cada estudiante, así como de atender y cumplir con las normas de seguridad e higiene que aseguren la integridad física del estudiante, el correcto empleo de los equipos de cómputo en los laboratorios del Programa Académico de Técnico en Programación.

PODER EJECUTIVO FEDERAL
ESTADOS UNIDOS MEXICANOS
MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

DESCRIPCIÓN DE LA UNIDAD DE APRENDIZAJE

Unidad de Aprendizaje: Ciberseguridad		
Propósito de la Unidad de Aprendizaje Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad 1: Introducción a la Ciberseguridad		
Unidad de competencia	Aprendizajes esperados	Contenidos de aprendizaje
Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.	Identifica las principales amenazas de los hackers con base en el análisis de los conceptos de ciberseguridad, datos personales e identidad en línea para la implementación de medidas de seguridad que protejan los datos de los usuarios.	**Conceptual:** • **Ciberseguridad** ○ ¿Qué es la Ciberseguridad? ○ Proteger los Datos Personales ○ La identidad en línea ○ ¿Dónde se encuentran los datos? ○ Dispositivos inteligentes • **Hackers y Hacking ético** ○ ¿Quiénes son? ○ ¿Qué quieren? ○ Robo de identidad ○ ¿Quién más quiere mis datos? ○ Hacking ético **Procedimental:** • Recupera los conceptos básicos de ciberseguridad, datos personales e identidad en línea para concebir de mejor forma las amenazas y proteger los datos sensibles. • Recupera los conceptos básicos de hackeo, hacking ético dentro de la ciberseguridad para proteger a los sistemas informáticos de los hackers. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva

INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

		• Se comunica de manera asertiva

	Distingue las principales amenazas a la seguridad de la información en una organización, incluyendo tipos de ciberataques, malware y vectores de ataque, para asegurar el adecuado manejo y resguardo de los datos en las organizaciones.	**Conceptual:**
		• **Datos de la organización**
		  ○ Tipos de datos de la organización
		  ○ El modelo de John McCumber (El Cubo de McCumber)
		  ○ Violaciones de seguridad de datos
		  ○ Casos reales a las Violaciones de seguridad de datos
		• **Ciberatacantes**
		  ○ Tipos de atacantes
		  ○ Amenazas internas y externas
		  ○ Tipos de malware
		  ○ Síntomas del malware
		• **Métodos de infiltración**
		  ○ Ingeniería social
		  ○ Denegación de servicio
		  ○ DoS distribuido
		  ○ Ataque Botnet
		  ○ Ataques Man-in-the-Middle (MitM) y (MitMo) (hombre en el medio y móvil)
		  ○ Ataque por envenenamiento SEO
		  ○ Descifrado de contraseñas de Wi-Fi
		  ○ Ataques de contraseña
		  ○ Tiempos de craqueo
		  ○ Amenazas persistentes avanzadas
		Procedimental:
		• Identifica las vulnerabilidades en casos reales de violaciones a la seguridad asociadas a cada tipo de dato en una organización
		• Identifica las técnicas y métodos de infiltración a los sistemas informáticos para protegerlos de los ataques más comúnmente utilizados.
		Actitudinal:
		• Trabaja de manera colaborativa
		• Hace uso de pensamiento analítico
		• Desarrolla responsabilidad social
		• Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas.
		• Toma de decisiones

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

		• Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva
Unidad 2: Protección de Datos y Organizaciones		
Unidad de competencia	Aprendizajes esperados	Contenidos de aprendizaje

Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.	Implementa estrategias de seguridad para redes inalámbricas domésticas y empresariales, incluyendo el cifrado de datos, la protección de la privacidad y medidas de prevención contra el acceso no autorizado.	**Conceptual:**
		• **Proteja sus dispositivos y su red**
		  ○ Protegiendo los dispositivos informáticos
		  ○ Seguridad de la red inalámbrica en casa y oficina
		  ○ Riesgos del Wi-Fi público
		  ○ Seguridad por contraseña
		  ○ Guías para las contraseñas
		  ○ Verificación de contraseña
		• **Cifrado de datos**
		  ○ ¿Qué es la cifrado?
		  ○ ¿Cómo se cifran sus datos?
		  ○ ¿Cómo se eliminan sus datos de forma permanente?
		  ○ ¿A quién le pertenecen sus datos?
		  ○ Términos del servicio
		  ○ Política de uso de datos
		  ○ Configuración de privacidad
		• **Protección de la privacidad en línea**
		  ○ Autenticación en Dos Factores
		  ○ Autorización abierta
		  ○ Social Media Sharing (Compartir en medios o redes sociales)
		  ○ Privacidad de correo electrónico y navegadores web
		Procedimental:
		• Hace uso de técnicas de seguridad para contraseñas, para la protección de los dispositivos de la red de casa y oficina, garantizando la seguridad en los mismos.
		• Utiliza métodos como la autenticación de doble factor y el cifrado de los datos de la red para garantizar la seguridad de los sistemas informáticos.
		Actitudinal:
		• Trabaja de manera colaborativa

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

		• Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

	Selecciona los dispositivos de ciberseguridad más adecuados, como cortafuegos y sistemas de detección en tiempo real, para mitigar las amenazas y proteger los sistemas informáticos de las organizaciones.	**Conceptual:**
		• **Dispositivos de Ciberseguridad para las organizaciones**
		  ○ Dispositivos de seguridad
		  ○ Cortafuegos (firewalls)
		  ○ Análisis de puertos
		  ○ Sistemas de detección y prevención de intrusiones
		  ○ Detección en tiempo real
		  ○ Protección contra software malicioso
		  ○ Mejores prácticas de seguridad
		• **Enfoque de comportamiento de la ciberseguridad para las organizaciones**
		  ○ Seguridad basada en el comportamiento
		  ○ NetFlow
		  ○ Pruebas de Penetración
		  ○ Reducción del impacto
		Procedimental:
		• Integra seguridad en los diferentes tipos de redes para evitar la intrusión a sistemas y personas no autorizadas.
		• Selecciona diversos dispositivos de seguridad para proteger y analizar los diversos ataques de ciberseguridad que se encuentran expuestas las diferentes organizaciones.
		Actitudinal:
		• Trabaja de manera colaborativa
		• Hace uso de pensamiento analítico
		• Desarrolla responsabilidad social
		• Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

		• Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva
Unidad 3: Educación profesional, Marco Legal y Normativo		
Unidad de competencia	Aprendizajes esperados	Contenidos de aprendizaje
Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.	Evalúa los riesgos de ciberseguridad para tomar decisiones informadas sobre la inversión en seguridad y la implementación de políticas y procedimientos que garanticen la confidencialidad, integridad y disponibilidad de la información, a través de la gestión de riesgos.	**Conceptual:** • **Gestión de riesgos en ciberseguridad** ○ Plan de Gestión de Riesgos ○ Objetivos de la Gestión de Riesgos ○ Identificación, Apreciación y Tratamiento de riesgos **Procedimental:** • Evalúa los riesgos dentro de una organización para reducir o minimizar las inseguridades potenciales. • Evalúa los riesgos para reducir o prevenir resultados desfavorables. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva
	Compara las diferentes carreras y certificaciones profesionales que existen en materia de ciberseguridad conociendo el marco legal y normativo en México.	• **Conceptual:** • **Educación profesional en ciberseguridad** ○ Carreras y certificaciones ○ Trayectorias profesionales en ciberseguridad ○ Educación y ciberseguridad en México • **Marco Legal y Normativo** ○ Cuestiones legales y éticas en Ciberseguridad

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

		○ Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados ○ Normas internacionales ○ Normas nacionales • **Procedimental:** • Recupera el tipo de educación y las trayectorias profesionales para poder ingresar al mundo de la ciberseguridad teniendo una educación formal. • Recupera leyes, normas y cuestiones éticas en el marco de la ciberseguridad para poder aplicar la legislación y normatividad vigente. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

MATRIZ DE VINCULACIÓN

	Unidad de Competencia 1		Unidad de Competencia 2		Unidad de Competencia 3	
COMPETENCIAS PARA EL SIGLO XXI HABILIDADES BLANDAS Y SOCIOEMOCIONALES	**AE 1**	**AE 2**	**AE 1**	**AE 2**	**AE 1**	**AE 2**
Trabajo colaborativo	X	X	X	X	X	X
Pensamiento analítico	X	X	X	X	X	X
Responsabilidad social	X	X	X	X	X	X
Pensamiento crítico	X	X	X	X	X	X
Toma de decisiones	X	X	X	X	X	X
Adaptabilidad	X	X	X	X	X	X
Resolución de problemas	X	X	X	X	X	X
Comunicación asertiva	X	X	X	X	X	X

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

PERFIL DOCENTE

El docente que imparta la Unidad de Aprendizaje de Ciberseguridad contará con las habilidades en el manejo de los saberes disciplinares y profesionales, así como su disposición, autoridad y tolerancia en el manejo de grupos de aprendizaje. Por lo tanto, debe poseer las habilidades que favorezcan el desarrollo de las competencias disciplinares y las habilidades blandas con nuevas tecnologías.

Habilidades docentes en el desarrollo del Talento

En el campo de su especialización:

- Habilidades y conocimientos profesionales que se requiere para la impartición de la Unidad de Aprendizaje.
- Emplea habilidades digitales actualizadas para el desarrollo de la Unidad de Aprendizaje.

En el campo pedagógico:

- Fomentar procesos de enseñanza que le permitan interpretar y resolver las necesidades de aprendizaje de los estudiantes, tomando en cuenta sus capacidades, habilidades, vocación e intereses.
- Desarrollar procesos de enseñanza-aprendizaje, utilizando métodos basados en las estrategias didácticas, aprovechando espacios educativos distintos a las aulas, para mejorar la calidad y pertinencia de la enseñanza.

En el campo de la investigación:

- Fortalecer el trabajo académico a partir del aprovechamiento de los resultados y productos de los proyectos de investigación

Perfil Profesional

- Licenciado o Ingeniero en Sistemas de Ciberseguridad o Analista de Ciberseguridad o Analista de Incidentes e Intrusiones o Analista de delitos cibernéticos o Gerente de Ciberseguridad o Auditor de TI o Arquitecto de ciberseguridad o Licenciado o Ingeniero Comunicaciones y Electrónica o en Computación o Informática o Maestría en Ciencias Computacionales o en Sistemas Informáticos o en Educación o a fin, preferentemente con experiencia de seis meses o más, en el área docente.

- Experiencia deseable preferentemente de seis meses o más, en el sector público o privado aplicando los conocimientos de la unidad de aprendizaje

Se requiere de **un docente titular y un docente auxiliar que** oriente y realimente a los estudiantes, debido a la naturaleza de las actividades de enseñanza-aprendizaje y de las actividades y ejercicios en el cifrado de datos, protección de la privacidad en línea, dispositivos de Ciberseguridad para las organizaciones, Enfoque de comportamiento de la ciberseguridad para las organizaciones, Gestión de riesgos en ciberseguridad, Educación profesional en ciberseguridad, Marco Legal y Normativo, revisando que se encuentren los elementos mínimos necesarios, para que cada estudiante alcance un aprendizaje significativo. Con cada ejercicio, actividad y práctica que se desarrolle en el aula, aula virtual y en el laboratorio de esta unidad de aprendizaje el estudiante irá adquiriendo las competencias disciplinares y profesionales, así como las habilidades blandas necesarias para el logro de los objetivos.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

ESTRUCTURA DIDÁCTICA

Unidad Didáctica 1:	Introducción a la Ciberseguridad	**Nivel:**	6to Nivel
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 1:	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.		
Aprendizaje Esperado No 1:	Identifica las principales amenazas de los hackers con base en el análisis de los conceptos de ciberseguridad, datos personales e identidad en línea para la implementación de medidas de seguridad que protejan los datos de los usuarios.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	9 horas

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
Conceptual: ✓ **Ciberseguridad** • ¿Qué es la Ciberseguridad? • Proteger los Datos Personales • La identidad en línea • ¿Dónde se encuentran los datos? • Dispositivos inteligentes ✓ **Hackers y Hacking ético** • ¿Quiénes son? • ¿Qué quieren? • Robo de identidad • ¿Quién más quiere mis datos? • Hacking ético	• Recupera los conceptos básicos de ciberseguridad, datos personales e identidad en línea para concebir de mejor forma las amenazas y proteger los datos sensibles de las personas. • Recupera los conceptos básicos de hackeo, hacking ético dentro de la ciberseguridad para proteger a los sistemas informáticos de los hackers.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Método **STEM** (Science, Technology, Engineering and Mathematics)

Apertura:

- El docente, hace una exploración de conocimientos generales, con una lluvia de ideas sobre los conceptos básicos de ciberseguridad para generar a partir de las respuestas una introducción a la ciberseguridad.

Desarrollo:

- El docente hace una presentación electrónica los conceptos básicos de ciberseguridad, datos personales e identidad en línea, hackeo, hackers, y el hacking ético.
- Los estudiantes buscan, discriminan y sintetizan información para construir su conceptualización de los elementos referentes a la ciberseguridad, el docente retroalimenta las aportaciones de los estudiantes.

EJECUTIVO FEDERAL PODERES UNIDOS MEXICANOS ESTADOS UNIDOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

- El docente presenta en tiempo real como se pueden proteger los datos personales, las diferencias entre la identidad fuera de línea y en línea, así como ejemplos de cómo los datos o información que se sube a las aplicaciones viven en servidores de diferentes partes del mundo.
- Los estudiantes utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a los conceptos básicos de ciberseguridad hackers y el hackeo ético.
- El docente utiliza el pc para presentar algunos videotutoriales sobre aspectos relevantes del hackeo malintencionado y ético.

Cierre:

- Los estudiantes responden mediante una ronda de preguntas sobre los conceptos básicos de ciberseguridad, como proteger los datos personales, el hackeo, los hackers, y el hacking ético, así como anexan una breve reflexión sobre la importancia de la protección de los datos personales e identidad en línea que se tiene en la vida cotidiana, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	• Reporte de investigación sobre los conceptos básicos de ciberseguridad y como proteger los datos personales e identidad en línea. • Cuadro comparativo de los tipos de hackers	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Reporte de investigación y cuadro comparativo sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte y cuadro comparativo en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • El Reporte de investigación incluye los elementos fundamentales de ciberseguridad y como proteger los datos personales e identidad en línea. • Cuadro comparativo sobre las diferencias entre los tipos de hackers. • El cuadro comparativo incluye al menos 3 diferencias entre los tipos de hackers. • El cuadro comparativo muestra claramente las diferencias entre los tipos de hackers. • El cuadro comparativo establece la relación entre las preguntas planteadas sobre los tipos de hackers.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Unidad Didáctica 1:	Introducción a la Ciberseguridad	**Nivel:**	**6to Nivel**
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 1:	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.		
Aprendizaje Esperado No 2:	Distingue las principales amenazas a la seguridad de la información en una organización, incluyendo tipos de ciberataques, malware y vectores de ataque, para asegurar el adecuado manejo y resguardo de los datos en las organizaciones.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	**9 horas**

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
✓ **Datos de la organización** • Tipos de datos de la organización • El modelo de John McCumber (El Cubo de McCumber) • Violaciones de seguridad de datos • Casos reales a las Violaciones de seguridad de datos ✓ **Ciberatacantes** • Tipos de atacantes • Amenazas internas y externas • Tipos de malware • Síntomas del malware ✓ **Métodos de infiltración** • Ingeniería social • Denegación de servicio • DoS distribuido • Ataque Botnet • Ataques Man-in-the-Middle (MitM) y (MitMo) (hombre en el medio y móvil) • Ataque por envenenamiento SEO • Descifrado de contraseñas de Wi-Fi • Ataques de contraseña • Tiempos de craqueo • Amenazas persistentes avanzadas	• Identifica las vulnerabilidades en casos reales de violaciones a la seguridad asociadas a cada tipo de dato en una organización. • Identifica las técnicas y métodos de infiltración a los sistemas informáticos para protegerlos de los ataques más comúnmente utilizados.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aula Invertida

Apertura:

- El docente, hace una exploración de conocimientos generales, con una lluvia de ideas sobre los tipos de datos que existen dentro de una organización, el modelo de John McCumber mejor conocido como el cubo de McCumber, las amenazas internas, las externas, así como los tipos de malware y de atacantes para generar a partir de las respuestas una introducción

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

a los tipos de datos que se encuentran en una organización y a los tipos de Ciberatacantes. Posteriormente se realiza la exploración de los conocimientos generales mediante un formulario aplicado a los estudiantes en alguna plataforma o aula virtual sobre los métodos de infiltración que los estudiantes conocen o no, esto con el objetivo de generar a partir de esos conocimientos previos una introducción a los métodos de infiltración conocidos actualmente.

- El docente proporciona material didáctico correspondiente a los temas a tratar previo a la clase. Da indicaciones de las acciones y actividades a realizar. Los estudiantes realizan las acciones y actividades previas a la clase, a fin de que puedan comprender el tema previo a la misma.

Desarrollo:

- Durante las clases el docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera contextualizada los tipos de datos que existen dentro de una organización, el modelo de John McCumber, las amenazas internas, las externas, así como los tipos de malware y de atacantes. El estudiante aclara dudas y contextualiza la información. El docente retroalimenta las aportaciones y motiva a los estudiantes.
- El docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera contextualizada los métodos de infiltración a los sistemas informáticos. El estudiante aclara dudas y contextualiza la información. El docente retroalimenta las aportaciones y motiva a los estudiantes.
- Los estudiantes utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a las infiltraciones. El docente presenta en tiempo real mediante videos ejemplos de infiltraciones a organizaciones y sistemas que se han suscitado en los últimos años.

Cierre:

- Los estudiantes responden mediante una ronda de preguntas sobre los tipos de datos que existen dentro de una organización, el modelo de John McCumber, las amenazas internas, las externas, los tipos de malware y los métodos de infiltración que se han suscitado en los últimos años, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

Ambiente de Aprendizaje:
Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	• Reporte de investigación sobre el modelo de John McCumber. • Cuadro comparativo para denotar las diferencias entre los métodos de infiltración.	**Instrumento de Evaluación:** Lista de cotejo **Criterios de Forma (estilo):** • Entrega de Reporte de investigación y cuadro comparativo sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte y cuadro comparativo en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • El Reporte de investigación incluye los elementos fundamentales del cubo de John McCumber. • Cuadro comparativo sobre métodos de infiltración, donde identifica al menos 3 métodos de infiltración. • Se muestra diferencias entre métodos de infiltración. • Establece la relación entre los métodos de infiltración.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Unidad Didáctica 2:	Protección de Datos y Organizaciones	**Nivel:**	6to Nivel
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 2:	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.		
Aprendizaje Esperado No 1:	Implementa estrategias de seguridad para redes inalámbricas domésticas y empresariales, incluyendo el cifrado de datos, la protección de la privacidad y medidas de prevención contra el acceso no autorizado.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	9 horas

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
✓ **Proteja sus dispositivos y su red** • Protegiendo los dispositivos informáticos • Seguridad de la red inalámbrica en casa y oficina • Riesgos del Wi-Fi público • Seguridad por contraseña • Guías para las contraseñas • Verificación de contraseña ✓ **Cifrado de datos** • ¿Qué es la cifrado? • ¿Cómo se cifran sus datos? • ¿Cómo se eliminan sus datos de forma permanente? • ¿A quién le pertenecen sus datos? • Términos del servicio • Política de uso de datos • Configuración de privacidad ✓ **Protección de la privacidad en línea** • Autenticación en Dos Factores • Autorización abierta • Social Media Sharing (Compartir en medios o redes sociales) • Privacidad de correo electrónico y navegadores web.	• Hace uso de técnicas de seguridad para contraseñas, para la protección de los dispositivos de la red de casa y oficina, garantizando la seguridad en los mismos. • Utiliza métodos como la autenticación de doble factor y el cifrado de los datos de la red para garantizar la seguridad de los sistemas informáticos	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Método STEAM

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Apertura: Activación del Conocimiento
El docente:
- Realiza una encuesta Inicial, donde hace uso de herramientas interactivas para evaluar percepciones sobre seguridad digital.
- Inicia una lluvia de Ideas, por medio de una discusión guiada sobre la importancia de la seguridad digital.
- Presenta la dinámica sobre protección de dispositivos y cifrado de datos.

Desarrollo: Construcción del Conocimiento
El estudiante:
- Realiza la configuración de seguridad de redes simuladas.
- Demuestra el cifrado de datos.
- Desarrolla la habilitación de autenticación de dos factores en cuentas.
- Analiza de políticas de privacidad en plataformas populares.
- Interactúa en plataforma virtual sobre privacidad en línea.

Cierre: Síntesis y Reflexión
- El docente aplica una actividad rápida (quiz) para medir la comprensión de los temas, por parte de los estudiantes.
- El estudiante participa en una discusión sobre la aplicación de conceptos en la vida diaria.
- El estudiante crea un plan para mejorar la seguridad de dispositivos.
- El estudiante expone los planes y obtiene retroalimentación del docente.

Ambiente de Aprendizaje:
Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	**Plan Integral de Seguridad Digital**	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega Plan Integral de Seguridad Digital en archivo electrónico, sin faltas de ortografía y en un documento pdf en laboratorio o plataforma virtual. • Entrega de actividades en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Incluye capturas de pantalla del proceso, justificación técnica y una reflexión final sobre la aplicación de las medidas de seguridad. • Denota una comprensión completa de los conceptos de ciberseguridad y protección de datos. • identifica de manera precisa y exhaustiva los riesgos específicos a los que están expuestos los dispositivos • Las medidas propuestas están alineadas con la gravedad de los riesgos identificados

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Unidad Didáctica 2:	Protección de Datos y Organizaciones	**Nivel:**	**6to Nivel**
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 2:	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.		
Aprendizaje Esperado No 2:	Selecciona los dispositivos de ciberseguridad más adecuados, como cortafuegos y sistemas de detección en tiempo real, para mitigar las amenazas y proteger los sistemas informáticos de las organizaciones.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	**9 horas**

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
✓ **Dispositivos de Ciberseguridad para las organizaciones** • Dispositivos de seguridad • Cortafuegos (firewalls) • Análisis de puertos • Sistemas de detección y prevención de intrusiones • Detección en tiempo real • Protección contra software malicioso • Mejores prácticas de seguridad ✓ **Enfoque de comportamiento de la ciberseguridad para las organizaciones** • Seguridad basada en el comportamiento • NetFlow • Pruebas de Penetración • Reducción del impacto	Integra seguridad en los diferentes tipos de redes para evitar la intrusión a sistemas y personas no autorizadas. Selecciona diversos dispositivos de seguridad para proteger y analizar los diversos ataques de ciberseguridad que se encuentran expuestas las diferentes organizaciones.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aula invertida.

Apertura:

- El docente inicia la clase con una lluvia de ideas sobre los dispositivos de seguridad que conocen los estudiantes, como cortafuegos, antivirus y sistemas de detección de intrusiones. Se analiza cómo estos dispositivos son esenciales para proteger a las organizaciones de amenazas externas y se introducen los conceptos clave relacionados con los dispositivos de ciberseguridad.
- Actividad inicial: Los estudiantes comparten sus experiencias o conocimiento sobre la importancia de los cortafuegos y dispositivos de seguridad en la protección de redes empresariales.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Desarrollo:

- El docente realiza una exposición sobre los dispositivos de seguridad utilizados en las organizaciones, como cortafuegos, sistemas de análisis de puertos y sistemas de detección y prevención de intrusiones (IDS/IPS). Se explican conceptos como la detección en tiempo real y las herramientas de protección contra software malicioso.

Actividad durante la sesión:

- Configura un cortafuegos (firewall), estableciendo reglas de seguridad y control de acceso en una red simulada y realizar un análisis de puertos usando herramientas como Nmap para identificar puertos abiertos y vulnerabilidades en una red simulada.

Cierre:

- Al final de la sesión, los estudiantes participan en una discusión grupal donde responden a preguntas sobre la importancia de los dispositivos de seguridad y las mejores prácticas en la protección de redes. También reflexionan sobre el enfoque basado en el comportamiento y su efectividad para identificar amenazas.

Ambiente de Aprendizaje:
Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • **Equipo de Cómputo (PC o Lap Top)** • **Conexión a internet** • **Video proyector** • **Aulas Virtuales** **Recursos Didácticos:** • **Libros digitales o impresos relacionados al tema.** • **Infografías y Videos relacionados al tema.** • **Presentaciones electrónicas relacionadas al tema.** • **Formularios interactivos relacionados al tema.** • **Páginas, sitios web y aplicaciones móviles relacionadas al tema.**	**Reporte de Seguridad Integral para Organizaciones**	**Instrumento de Evaluación: Rúbrica** **Criterios de Forma (estilo):** • Entrega de Reporte de Seguridad Integral para Organizaciones, sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Realiza un reporte de Seguridad Integral para Organizaciones, incluyendo la configuración de un cortafuegos con reglas de seguridad, el análisis de puertos utilizando herramientas como Nmap, la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS). • Incluye en el Reporte de Seguridad Integral para Organizaciones la reflexión sobre la seguridad basada en el comportamiento mediante el análisis de NetFlow y pruebas de penetración.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Unidad Didáctica 3:	Educación profesional, Marco Legal y Normativo	**Nivel:**	**6to Nivel**
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 3:	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.		
Aprendizaje Esperado No 1:	Evalúa los riesgos de ciberseguridad para tomar decisiones informadas sobre la inversión en seguridad y la implementación de políticas y procedimientos que garanticen la confidencialidad, integridad y disponibilidad de la información, a través de la gestión de riesgos.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	**9 horas**

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
• **Gestión de riesgos en ciberseguridad** ✓ Plan de Gestión de Riesgos ✓ Objetivos de la Gestión de Riesgos ✓ Identificación, Apreciación y Tratamiento de riesgos	• Evalúa los riesgos dentro de una organización para reducir o minimizar las inseguridades potenciales. • Evalúa los riesgos para reducir o prevenir resultados desfavorables.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Método STEM

Apertura:

El docente:

- Hace una exploración de conocimientos generales, con una lluvia de ideas sobre la planeación de riesgos y generar con ello, a partir de las respuestas, el plan de gestión de riesgos.

Desarrollo:

El docente:

- Hace una presentación en canva o similar sobre la planeación de gestión de riesgos, los estudiantes buscan, discriminan y sintetizan información para construir su conceptualización sobre los objetivos, la identificación, apreciación y tratamiento de los riesgos, el docente retroalimenta las aportaciones de los estudiantes.
- Con la ayuda de actividades interactivas presenta en tiempo real como se realiza un plan de gestión de riesgos con todos sus elementos, así como ejemplos de diversos planes de gestión de diferentes empresas del sector público y privado.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

El estudiante:

- Se reúnen en equipo utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a la planeación de la gestión de riesgos. El docente utiliza el pc para presentar algunos videotutoriales sobre aspectos relevantes de la planeación de gestión de riesgos.

Cierre:

- Los estudiantes responden mediante una ronda de preguntas sobre la planeación de gestión de riesgos, así como anexan una breve reflexión sobre la importancia de contar con esta planeación, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	**Reflexión sobre la importancia de contar con una planeación de gestión de riesgos en ciberseguridad**	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de plan estratégico archivo electrónico, sin faltas de ortografía y en un documento pdf en laboratorio o plataforma virtual. • Entrega de actividades en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Demuestra una comprensión clara de lo que significa la gestión de riesgos en ciberseguridad • Reconoce la importancia estratégica de la gestión de riesgos para la protección de los activos de información de una organización. • Describe las posibles consecuencias negativas de no contar con una planeación de gestión de riesgos. • Relaciona la gestión de riesgos con otros conceptos clave de ciberseguridad, como vulnerabilidades, amenazas y controles de seguridad.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Unidad Didáctica 3:	Educación profesional, Marco Legal y Normativo	**Nivel:**	**6to Nivel**
Propósito General:	Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.		
Unidad de Competencia No 3:	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.		
Aprendizaje Esperado No 2:	Compara las diferentes carreras y certificaciones profesionales que existen en materia de ciberseguridad para tomar una decisión y dedicar su proyecto de vida a la ciberseguridad, conociendo el marco legal y normativo en México.	**Tiempo estimado para obtener el Aprendizaje Esperado:**	**9 horas**

Contenidos de Aprendizaje

Conceptuales	Procedimentales	Actitudinales
• **Educación profesional en ciberseguridad** ✓ Carreras y certificaciones ✓ Trayectorias profesionales en ciberseguridad ✓ Educación y ciberseguridad en México • **Marco Legal y Normativo** ✓ Cuestiones legales y éticas en Ciberseguridad ✓ Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados ✓ Normas internacionales ✓ Normas nacionales	• Recupera el tipo de educación y las trayectorias profesionales para poder ingresar al mundo de la ciberseguridad teniendo una educación formal. • Recupera leyes, normas y cuestiones éticas en el marco de la ciberseguridad para poder aplicar la legislación y normatividad vigente.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aula Invertida

Apertura:

El docente:

- Hace una exploración de conocimientos generales, con una lluvia de ideas sobre las Carreras y certificaciones que existen actualmente en México, para generar a partir de las respuestas un cuadro comparativo sobre a qué se dedica cada una de los diferentes perfiles en ciberseguridad.
- Proporciona material didáctico correspondiente a la Educación y ciberseguridad en México previo a la clase. Da indicaciones de las actividades a realizar. Los estudiantes realizan las actividades previas a la clase, a fin de que puedan comprender el tema.

Desarrollo:

- Durante las clases el docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera contextualizada el Marco Legal y Normativo que existe en la actualidad.
- El estudiante aclara dudas y contextualiza la información. El docente retroalimenta las aportaciones y motiva a los estudiantes.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

- El docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera explícita las Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados, las Normas internacionales y las Normas nacionales en materia de ciberseguridad. El docente retroalimenta las aportaciones y motiva a los estudiantes.
- Los estudiantes utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a las Normas internacionales y nacionales en materia de ciberseguridad. El docente presenta el Marco Legal y Normativo.

Cierre:

- Los estudiantes responden mediante una ronda de preguntas sobre las Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados, las Normas internacionales y las Normas nacionales, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Instrumento y Criterios de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	• Reporte de investigación sobre los tipos de educación y trayectorias profesionales en ciberseguridad. • Reporte de investigación sobre las leyes, normas y cuestiones éticas en el marco de la ciberseguridad.	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Reporte de investigación sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Elabora un reporte de investigación incluyendo los tipos de educación y trayectorias profesionales en ciberseguridad. • Incluye el Reporte de investigación las leyes, normas y cuestiones éticas en el marco de la ciberseguridad. • Incluye gráficas, análisis por mes y por semestre para profesionales en ciberseguridad.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

PRÁCTICAS

Nombre de la Práctica:	Pruebas de penetración o Hacking ético	**N° de la Práctica:**	1	**Tiempo:**	6 horas
Unidad de Competencia 1:	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.				
Aprendizajes Esperados Relacionados con la Práctica:	Identifica las principales amenazas de los hackers con base en el análisis de los conceptos de ciberseguridad, datos personales e identidad en línea para la implementación de medidas de seguridad que protejan los datos de los usuarios.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
✓ **Hackers y Hacking ético** • ¿Quiénes son? • ¿Qué quieren? • Robo de identidad • ¿Quién más quiere mis datos? • Hacking ético	Recupera los conceptos básicos de hackeo, hacking ético dentro de la ciberseguridad para proteger a los sistemas informáticos de los hackers.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Método **STEM** (Science, Technology, Engineering and Mathematics)

- **Apertura:** El docente, hace una exploración de conocimientos generales, con una lluvia de ideas sobre la planeación de riesgos y generar con ello, a partir de las respuestas, el plan de gestión de riesgos.
- **Desarrollo:** El docente hace una presentación en canva o similar sobre la planeación de gestión de riesgos, los estudiantes buscan, discriminan y sintetizan información para construir su conceptualización sobre los objetivos, la identificación, apreciación y tratamiento de los riesgos, el docente retroalimenta las aportaciones de los estudiantes.
- El docente con la ayuda de actividades interactivas presenta en tiempo real como se realiza un plan de gestión de riesgos con todos sus elementos, así como ejemplos de diversos planes de gestión de diferentes empresas del sector público y privado.
- Los estudiantes se reúnen en equipo utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a la planeación de la gestión de riesgos. El docente utiliza el pc para presentar algunos videotutoriales sobre aspectos relevantes de la planeación de gestión de riesgos.
- **Cierre:** Los estudiantes responden mediante una ronda de preguntas sobre la planeación de gestión de riesgos, así como anexan una breve reflexión sobre la importancia de contar con esta planeación, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	Reporte de investigación sobre el hacking ético.	**Instrumento de Evaluación: Rubrica** **Criterios de Forma (estilo):** • Entrega de Reporte de investigación sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • El Reporte de investigación incluye que es el hacking ético, ¿para qué sirve?, ¿es bueno es malo? • El Reporte de investigación incluye una conclusión personal.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Nombre de la Práctica:	Brechas de seguridad	**N° de la Práctica:**	**2**	**Tiempo:**	**6 horas**
Unidad de Competencia 1:	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.				
Aprendizaje Esperado 2 Relacionados con la Práctica:	Distingue las principales amenazas a la seguridad de la información en una organización, incluyendo tipos de ciberataques, malware y vectores de ataque, para asegurar el adecuado manejo y resguardo de los datos en las organizaciones.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
Ciberatacantes • Tipos de atacantes • Amenazas internas y externas • Tipos de malware • Síntomas del malware **Métodos de infiltración** • Ingeniería social • Denegación de servicio • DoS distribuido • Ataque Botnet • Ataques Man-in-the-Middle (MitM) y (MitMo) (hombre en el medio y móvil) • Ataque por envenenamiento SEO • Descifrado de contraseñas de Wi-Fi • Ataques de contraseña • Tiempos de craqueo • Amenazas persistentes avanzadas	• Identifica las técnicas y métodos de infiltración a los sistemas informáticos para protegerlos de los ataques más comúnmente utilizados.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva .

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aprendizaje basado en el Pensamiento

- **Apertura:** El docente, hace una exploración de conocimientos generales, con una lluvia de ideas sobre las Carreras y certificaciones que existen actualmente en México, para generar a partir de las respuestas un cuadro comparativo sobre a qué se dedica cada una de los diferentes perfiles en ciberseguridad.
- El docente proporciona material didáctico correspondiente a la Educación y ciberseguridad en México previo a la clase. Da indicaciones de las actividades a realizar. Los estudiantes realizan las actividades previas a la clase, a fin de que puedan comprender el tema.
- **Desarrollo:** Durante las clases el docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera contextualizada el Marco Legal y Normativo que existe en la actualidad. El estudiante aclara dudas y contextualiza la información. El docente retroalimenta las aportaciones y motiva a los estudiantes.

  El docente corrobora lo aprendido y realiza acciones para explicar a los estudiantes y poner el conocimiento en práctica y de manera explícita las Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados, las Normas internacionales y las Normas nacionales en materia de ciberseguridad. El docente retroalimenta las aportaciones y motiva a los estudiantes.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Los estudiantes utilizan el pc como herramienta para consultar diferente información, videotutoriales y aplicaciones referentes a las Normas internacionales y nacionales en materia de ciberseguridad. El docente presenta el Marco Legal y Normativo.

- **Cierre:** Los estudiantes responden mediante una ronda de preguntas sobre las Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados, las Normas internacionales y las Normas nacionales, el docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa

Ambiente de Aprendizaje:
Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	Cuadro comparativo ataques a organizaciones	Instrumento de Evaluación: Lista de cotejo Criterios de Forma (estilo): • Entrega de cuadro comparativo sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega de la actividad en tiempo y forma solicitados. Criterios de Fondo (parte técnica): • Desarrolla un cuadro comparativo, incluyendo: • 3 ejemplos de organizaciones. • Responde los siguientes cuestionamientos, Fecha del incidente, Organización afectada, ¿Qué se llevó?, ¿Qué tipo de ataque se utilizó?, ¿Qué acciones se pueden tomar para evitar que la infracción vuelva a ocurrir en el futuro? y fuente(s) consultada(s). • El cuadro comparativo establece la relación entre las preguntas anteriormente planteadas.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Nombre de la Práctica:	**Configuración en Medidas de Ciberseguridad**	**N° de la Práctica:**	**3**	**Tiempo:**	**6 horas**
Unidad de Competencia:	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.				
Aprendizajes Esperados Relacionados con la Práctica:	Implementa estrategias de seguridad para redes inalámbricas domésticas y empresariales, incluyendo el cifrado de datos, la protección de la privacidad y medidas de prevención contra el acceso no autorizado.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
✓ **Proteja sus dispositivos y su red** • Protegiendo los dispositivos informáticos • Seguridad de la red inalámbrica en casa y oficina • Riesgos del Wi-Fi público • Seguridad por contraseña • Guías para las contraseñas • Verificación de contraseña	• Hace uso de técnicas de seguridad para contraseñas, para la protección de los dispositivos de la red de casa y oficina, garantizando la seguridad en los mismos.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aprendizaje basado en problemas / Aprendizaje colaborativo

El docente:

- Expone un ejemplo práctico sobre la implementación de medidas de seguridad en redes inalámbricas domésticas y empresariales, destacando la importancia del cifrado de datos, protección de la privacidad y seguridad por contraseña.
- Proporciona una demostración de cómo configurar la seguridad de una red Wi-Fi doméstica y empresarial, incluyendo el uso de autenticación en dos factores y herramientas de cifrado.
- Presenta un caso de estudio sobre los riesgos del uso de Wi-Fi público y plantea preguntas para discutir las mejores prácticas de seguridad, como la protección de contraseñas y la verificación de datos.
- Da instrucciones para el uso de herramientas de cifrado y autenticación, guiando a los estudiantes en la configuración de una red segura y la implementación de políticas de privacidad.

El estudiante:

- Los estudiantes analizan la situación de una red doméstica o empresarial y aplican los conceptos aprendidos sobre seguridad de contraseñas, cifrado de datos y protección de la privacidad en línea.
- Realizan pruebas de seguridad en redes Wi-Fi utilizando herramientas de cifrado y autenticación en dos factores, y crean una configuración de seguridad para proteger sus datos y dispositivos.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

- Trabajan en equipo para identificar posibles vulnerabilidades en un escenario dado y proponen soluciones innovadoras para fortalecer la seguridad de la red.
- Presentan sus soluciones y discuten en grupo las estrategias de protección más efectivas, validando sus decisiones a través de retroalimentación colaborativa.

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	Informe de Configuración de Seguridad de Red Wi-Fi	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Informe de Configuración de Seguridad de Red Wi-Fi sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del informe en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • El Informe de Configuración de Seguridad de Red Wi-Fi incluye medidas de seguridad adecuadas y demuestra comprensión de conceptos clave. • El Informe de Configuración de Seguridad de Red Wi-Fi incluye una conclusión personal sobre el tema revisado.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Nombre de la Práctica:	**Implementación de seguridad en redes informáticas**	**N° de la Práctica:**	**4**	**Tiempo:**	**6 horas**
Unidad de Competencia:	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.				
Aprendizajes Esperados Relacionados con la Práctica:	Selecciona los dispositivos de ciberseguridad más adecuados, como cortafuegos y sistemas de detección en tiempo real, para mitigar las amenazas y proteger los sistemas informáticos de las organizaciones.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
✓ **Dispositivos de Ciberseguridad para las organizaciones** • Dispositivos de seguridad • Cortafuegos (firewalls) • Análisis de puertos • Sistemas de detección y prevención de intrusiones • Detección en tiempo real • Protección contra software malicioso • Mejores prácticas de seguridad	Integra seguridad en los diferentes tipos de redes para evitar la intrusión a sistemas y personas no autorizadas.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aprendizaje basado en problemas / Aprendizaje colaborativo

El docente:

- Explica la importancia de proteger los dispositivos informáticos y redes mediante medidas de seguridad, como contraseñas fuertes y verificación en dos pasos.
- Facilita ejemplos prácticos sobre el cifrado de datos y la eliminación segura de información, aclarando conceptos como políticas de uso y configuración de privacidad.
- Proporciona un enfoque sobre cómo la protección de la privacidad en línea puede lograrse mediante herramientas de autenticación, como la autenticación en dos factores.
- Da instrucciones detalladas sobre el uso de herramientas de protección de datos, guías para contraseñas y cómo configurar opciones de privacidad en redes sociales, correos electrónicos y navegadores.

El estudiante:

- Analiza la seguridad de sus dispositivos y redes, aplicando medidas de protección como contraseñas seguras y la configuración de autenticación en dos factores.
- Realiza prácticas de cifrado y eliminación segura de datos, explorando cómo proteger su información personal en plataformas y redes sociales.
- Trabaja en equipo para identificar posibles vulnerabilidades y propone soluciones de seguridad basadas en las herramientas aprendidas, como la autenticación en dos factores y políticas de privacidad.
- Presenta sus soluciones y discute en grupo, reflexionando sobre la seguridad en línea y validando las mejores prácticas para proteger la privacidad en redes sociales, correos electrónicos y navegadores.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	Reporte sobre Amenazas Cibernéticas y Soluciones.	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Reporte sobre Amenazas Cibernéticas y Soluciones sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Desarrolla el reporte sobre Amenazas Cibernéticas y Soluciones incluyendo contraseñas seguras, autenticación en dos factores y cifrado de datos para proteger la información personal y los dispositivos. • incluye en el reporte sobre Amenazas Cibernéticas y Soluciones, una conclusión personal sobre el tema revisado.

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Nombre de la Práctica:	**Planeación de gestión de riesgos**	**N° de la Práctica:**	**5**	**Tiempo:**	**6 horas**
Unidad de Competencia:	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.				
Aprendizajes Esperados Relacionados con la Práctica:	Evalúa los riesgos de ciberseguridad para tomar decisiones informadas sobre la inversión en seguridad y la implementación de políticas y procedimientos que garanticen la confidencialidad, integridad y disponibilidad de la información, a través de la gestión de riesgos.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
• **Gestión de riesgos en ciberseguridad** ✓ Plan de Gestión de Riesgos ✓ Objetivos de la Gestión de Riesgos ✓ Identificación, Apreciación y Tratamiento de riesgos	• Evalúa los riesgos dentro de una organización para reducir o minimizar las inseguridades potenciales. • Evalúa los riesgos para reducir o prevenir resultados desfavorables.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Método STEM

- **Apertura:** El docente, muestra varias planeaciones de gestión de riesgos de diversas organizaciones para el análisis.
- **Desarrollo:** El docente hace uso de los equipos ya formados en las unidades de aprendizaje de proyecto integrador, dirección de proyectos, laboratorio de software IV o alguna otra en donde se hayan creado equipos para solicitar de manera grupal el documento de planeación de gestión de riesgos de su misma empresa o equipo trabajado para el proyecto aula, los estudiantes trabajan de manera colaborativa así como, buscan, discriminan y sintetizan información para construir el documento de Planeación de gestión de Riesgos, el docente retroalimenta el trabajo colaborativo de cada uno de los equipos.
- **Cierre:** Los estudiantes terminan y entregan el reporte de la planeación de gestión de riesgos en el aula virtual o directamente al docente en el laboratorio de programación. El docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje.

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	**Plan de gestión de Riesgos**	**Instrumento de Evaluación:** • Lista de cotejo **Criterios de Forma (estilo):** • Entrega de plan estratégico archivo electrónico, sin faltas de ortografía y en un documento pdf en laboratorio o plataforma virtual. • Entrega de actividades en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Incluye una carátula, desarrollo y conclusiones. • Identificación de los riesgos relevantes y potencialmente significativos • Desarrollo de la probabilidad y el impacto de cada riesgo • Propuestas de medidas concretas para mitigar, transferir, aceptar o evitar cada riesgo • Establecimiento de un proceso para monitorear los riesgos a lo largo del tiempo

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Nombre de la Práctica:	**Remuneración económica para profesionales en ciberseguridad**	**N° de la Práctica:**	**6**	**Tiempo:**	**6 horas**
Unidad de Competencia:	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.				
Aprendizajes Esperados Relacionados con la Práctica:	Compara las diferentes carreras y certificaciones profesionales que existen en materia de ciberseguridad para tomar una decisión y dedicar su proyecto de vida a la ciberseguridad, conociendo el marco legal y normativo en México.				

Contenidos de Aprendizaje Relacionados con la Práctica

Conceptuales	Procedimentales	Actitudinales
• **Educación profesional en ciberseguridad** ✓ Carreras y certificaciones ✓ Trayectorias profesionales en ciberseguridad ✓ Educación y ciberseguridad en México	• Recupera el tipo de educación y las trayectorias profesionales para poder ingresar al mundo de la ciberseguridad teniendo una educación formal.	• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

Estrategia Didáctica y Ambiente de Aprendizaje

Estrategia Didáctica: Aula Invertida

- **Apertura:** El docente, proporciona material didáctico, link e información de fuentes confiables en donde se observe la remuneración económica del pago a las personas profesionales en ciberseguridad. Da indicaciones de las actividades a realizar en un entorno fuera del laboratorio de programación. Los estudiantes realizan las actividades previas a la clase.
- **Desarrollo:** Durante las clases el docente corrobora lo aprendido mediante una lluvia de ideas, realiza debates y acciones para entrar en un entorno de análisis de la remuneración de los profesionales en ciberseguridad, realiza un cuadro comparativo con la remuneración de forma anual y semestral. El estudiante aclara dudas y contextualiza la información. El docente retroalimenta las aportaciones y motiva a los estudiantes.
- **Cierre:** Los estudiantes realizan el reporte del análisis realizado entre ellos y el docente responden mediante una ronda de preguntas sobre las remuneraciones más altas, bajas e intermedias y las actividades desarrolladas entre los profesionales de ciberseguridad. El docente responde a las preguntas o dudas que el estudiante llegará a tener para facilitar su aprendizaje, así como se les solicita que realicen de manera individual la evidencia de aprendizaje formativa.

Ambiente de Aprendizaje:

Es un ambiente de aprendizaje presencial en los laboratorios de programación, pero además el docente creará un aula virtual en alguna plataforma tecnológica. Para poder tener comunicación con los estudiantes de manera asíncrona y con ello complementar la comunicación y resolver dudas.

PODER EJECUTIVO FEDERAL
ESTADOS UNIDOS MEXICANOS
MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

Herramientas Tecnológicas y Recursos Didácticos	Evidencia de Aprendizaje para la Evaluación Formativa	Criterios e Instrumentos de Evaluación
Herramientas Tecnológicas: • Equipo de Cómputo (PC o Lap Top) • Conexión a internet • Video proyector • Aulas Virtuales **Recursos Didácticos:** • Libros digitales o impresos relacionados al tema. • Infografías y Videos relacionados al tema. • Presentaciones electrónicas relacionadas al tema. • Formularios interactivos relacionados al tema. • Páginas, sitios web y aplicaciones móviles relacionadas al tema.	Informe de remuneración económica para profesionales en ciberseguridad	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Informe de Remuneración económica para profesionales en ciberseguridad sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del informe en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Desarrolla el informe de Remuneración económica para profesionales en ciberseguridad incluye gráficas, análisis por mes y por semestre para profesionales en ciberseguridad. • incluye en el Informe de Remuneración económica para profesionales en ciberseguridad incluye una conclusión personal sobre el tema revisado.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

PLAN DE EVALUACIÓN SUMATIVA

N°	Unidad de Competencia	Evidencia Integradora	Criterios e Instrumento de Evaluación	Porcentaje de Acreditación
1	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.	Portafolio de evidencias: • Reporte de investigación sobre los conceptos básicos de ciberseguridad y como proteger los datos personales e identidad en línea. • Cuadro comparativo de los tipos de hackers. • Reporte de investigación sobre el modelo de John McCumber. • Cuadro comparativo para denotar las diferencias entre los métodos de infiltración.	**Instrumento de Evaluación: Lista de cotejo** **Criterios de Forma (estilo):** • Entrega de Reporte de investigación y cuadro comparativo sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte y cuadro comparativo en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • El Reporte de investigación incluye los elementos fundamentales de ciberseguridad y como proteger los datos personales e identidad en línea. • Cuadro comparativo sobre las diferencias entre los tipos de hackers. • El cuadro comparativo incluye al menos 3 diferencias entre los tipos de hackers. • El cuadro comparativo muestra claramente las diferencias entre los tipos de hackers. • El cuadro comparativo establece la relación entre las preguntas planteadas sobre los tipos de hackers. • El Reporte de investigación incluye los elementos fundamentales del cubo de John McCumber. • Cuadro comparativo sobre métodos de infiltración, donde identifica al menos 3 métodos de infiltración • Se muestra diferencias entre métodos de infiltración.	**40%**

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

			• Establece la relación entre los métodos de infiltración.	
2	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.	Portafolio de evidencias: • Plan Integral de Seguridad Digital • Reporte de Seguridad Integral para Organizaciones	**Instrumento de Evaluación: Lista de cotejo / Rubrica** **Criterios de Forma (estilo):** • Entrega Plan Integral de Seguridad Digital en archivo electrónico, sin faltas de ortografía y en un documento pdf en laboratorio o plataforma virtual. • Entrega de Reporte de Seguridad Integral para Organizaciones, sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega de actividades en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Incluye capturas de pantalla del proceso, justificación técnica y una reflexión final sobre la aplicación de las medidas de seguridad. • Denota una comprensión completa de los conceptos de ciberseguridad y protección de datos. • El Reporte de Seguridad Integral para Organizaciones, incluye la configuración de un cortafuegos con reglas de seguridad, el análisis de puertos utilizando herramientas como Nmap, la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS). • El Reporte de Seguridad Integral para Organizaciones incluye la reflexión sobre la seguridad basada en el comportamiento mediante el análisis de NetFlow y pruebas de penetración.	**40%**
	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y	Portafolio de evidencias:	**Instrumento de Evaluación: Lista de cotejo**	**20%**

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

3	normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.	• Planeación de gestión de riesgos • Reporte de investigación sobre los tipos de educación y trayectorias profesionales en ciberseguridad. • Reporte de investigación sobre las leyes, normas y cuestiones éticas en el marco de la ciberseguridad.	**Criterios de Forma (estilo):** • Entrega de plan estratégico en archivo electrónico sin faltas de ortografía y en un documento pdf en laboratorio o plataforma virtual. • Entrega de Reporte de investigación sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega del reporte en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Incluye una carátula, desarrollo y conclusiones. • Identifica todos los riesgos relevantes y potencialmente significativos • Desarrollo la probabilidad y el impacto de cada riesgo • Propuesto medidas concretas para mitigar, transferir, aceptar o evitar cada riesgo • Estableció un proceso para monitorear los riesgos a lo largo del tiempo • El Reporte de investigación incluye los tipos de educación y trayectorias profesionales en ciberseguridad. • Reporte de investigación incluye las leyes, normas y cuestiones éticas en el marco de la ciberseguridad.	

Propósito de la Unidad de Aprendizaje	Evidencia Integradora	Criterios e Instrumento de Evaluación	Porcentaje de Acreditación
Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.	Manual para la defensa en Ciberseguridad aplicable a organizaciones públicas y/o privadas.	**Instrumento de Evaluación:** Lista de cotejo / Rubrica **Criterios de Forma (estilo):** • Entrega de Manual para la defensa en Ciberseguridad en archivo electrónico, sin faltas de ortografía y en un	100%

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

		documento pdf en laboratorio o plataforma virtual. • Entrega de Manual para la defensa en Ciberseguridad, sin faltas de ortografía, en un archivo pdf en aula o plataforma virtual. • Entrega de actividades en tiempo y forma solicitados. **Criterios de Fondo (parte técnica):** • Incluye capturas de pantalla del proceso, justificación técnica y una reflexión final sobre la aplicación de las medidas de seguridad. • Denota una comprensión completa de los conceptos de ciberseguridad y protección de datos. • Desarrolla la configuración de un cortafuegos con reglas de seguridad, el análisis de puertos utilizando herramientas como Nmap, la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS). • Desarrolla una reflexión sobre la seguridad basada en el comportamiento mediante el análisis de NetFlow y pruebas de penetración.	

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

PROGRAMA SINTÉTICO

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE			
Diseña medidas de ciberseguridad a sistemas informáticos para la protección de amenazas y ataques digitales que comprometan su operación, su identidad y sus datos en red, contra el uso indebido y no autorizado de una forma analítica, creativa e innovadora.			
N°	**UNIDAD DE COMPETENCIA**	**APRENDIZAJES ESPERADOS**	**CONTENIDOS DE APRENDIZAJE/SABERES**

1	Analiza los principios fundamentales de ciberseguridad, en la protección de información personal y la identidad digital, considerando los riesgos asociados a los diferentes tipos de malware y ataques cibernéticos, mediante un pensamiento crítico.	1.-Identifica las principales amenazas de los hackers con base en el análisis de los conceptos de ciberseguridad, datos personales e identidad en línea para la implementación de medidas de seguridad que protejan los datos de los usuarios.	**Conceptual:**
			• **Ciberseguridad**
			  ○ ¿Qué es la Ciberseguridad?
			  ○ Proteger los Datos Personales
			  ○ La identidad en línea
			  ○ ¿Dónde se encuentran los datos?
			  ○ Dispositivos inteligentes
			• **Hackers y Hacking ético**
			  ○ ¿Quiénes son?
			  ○ ¿Qué quieren?
			  ○ Robo de identidad
			  ○ ¿Quién más quiere mis datos?
			  ○ Hacking ético
			Procedimental:
			• Recupera los conceptos básicos de ciberseguridad, datos personales e identidad en línea para concebir de mejor forma las amenazas y proteger los datos sensibles de las personas.
			• Recupera los conceptos básicos de hackeo, hacking ético dentro de la ciberseguridad para proteger a los sistemas informáticos de los hackers.
			Actitudinal:
			• Trabaja de manera colaborativa
			• Hace uso de pensamiento analítico
			• Desarrolla responsabilidad social
			• Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas.
			• Toma de decisiones

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

			• Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

		2.-Distingue las principales amenazas a la seguridad de la información en una organización, incluyendo tipos de ciberataques, malware y vectores de ataque, para asegurar el adecuado manejo y resguardo de los datos en las organizaciones.	**Conceptual:**
			• **Datos de la organización**
			  ○ Tipos de datos de la organización
			  ○ El modelo de John McCumber (El Cubo de McCumber)
			  ○ Violaciones de seguridad de datos
			  ○ Casos reales a las Violaciones de seguridad de datos
			• **Ciberatacantes**
			  ○ Tipos de atacantes
			  ○ Amenazas internas y externas
			  ○ Tipos de malware
			  ○ Síntomas del malware
			• **Métodos de infiltración**
			  ○ Ingeniería social
			  ○ Denegación de servicio
			  ○ DoS distribuido
			  ○ Ataque Botnet
			  ○ Ataques Man-in-the-Middle (MitM) y (MitMo) (hombre en el medio y móvil)
			  ○ Ataque por envenenamiento SEO
			  ○ Descifrado de contraseñas de Wi-Fi
			  ○ Ataques de contraseña
			  ○ Tiempos de craqueo
			  ○ Amenazas persistentes avanzadas
			Procedimental:
			• Identifica las vulnerabilidades en casos reales de violaciones a la seguridad asociadas a cada tipo de dato en una organización

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

			• Identifica las técnicas y métodos de infiltración a los sistemas informáticos para protegerlos de los ataques más comúnmente utilizados. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva
2	Evalúa la seguridad de las redes inalámbricas domésticas y empresariales mediante el cifrado de datos y la implementación de dispositivos de seguridad para evitar el acceso no autorizado y la suplantación de identidad.	1.-Implementa estrategias de seguridad para redes inalámbricas domésticas y empresariales, incluyendo el cifrado de datos, la protección de la privacidad y medidas de prevención contra el acceso no autorizado.	**Conceptual:** • **Proteja sus dispositivos y su red** ○ Protegiendo los dispositivos informáticos ○ Seguridad de la red inalámbrica en casa y oficina ○ Riesgos del Wi-Fi público ○ Seguridad por contraseña ○ Guías para las contraseñas ○ Verificación de contraseña • **Cifrado de datos** ○ ¿Qué es la cifrado? ○ ¿Cómo se cifran sus datos? ○ ¿Cómo se eliminan sus datos de forma permanente? ○ ¿A quién le pertenecen sus datos? ○ Términos del servicio ○ Política de uso de datos ○ Configuración de privacidad • **Protección de la privacidad en línea** ○ Autenticación en Dos Factores ○ Autorización abierta

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

			○ Social Media Sharing (Compartir en medios o redes sociales) ○ Privacidad de correo electrónico y navegadores web **Procedimental:** • Hace uso de técnicas de seguridad para contraseñas, para la protección de los dispositivos de la red de casa y oficina, garantizando la seguridad en los mismos. • Utiliza métodos como la autenticación de doble factor y el cifrado de los datos de la red para garantizar la seguridad de los sistemas informáticos. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva
			Conceptual: • **Dispositivos de Ciberseguridad para las organizaciones** ○ Dispositivos de seguridad ○ Cortafuegos (firewalls) ○ Análisis de puertos ○ Sistemas de detección y prevención de intrusiones ○ Detección en tiempo real ○ Protección contra software malicioso ○ Mejores prácticas de seguridad

EJECUTIVO FEDERAL PODER UNIDOS MEXICANOS ESTADOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

		2.- Selecciona los dispositivos de ciberseguridad más adecuados, como cortafuegos y sistemas de detección en tiempo real, para mitigar las amenazas y proteger los sistemas informáticos de las organizaciones.	• **Enfoque de comportamiento de la ciberseguridad para las organizaciones**
			  ○ Seguridad basada en el comportamiento
			  ○ NetFlow
			  ○ Pruebas de Penetración
			  ○ Reducción del impacto
			
			Procedimental:
			• Integra seguridad en los diferentes tipos de redes para evitar la intrusión a sistemas y personas no autorizadas.
			• Selecciona diversos dispositivos de seguridad para proteger y analizar los diversos ataques de ciberseguridad que se encuentran expuestas las diferentes organizaciones.
			Actitudinal:
			• Trabaja de manera colaborativa
			• Hace uso de pensamiento analítico
			• Desarrolla responsabilidad social
			• Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas.
			• Toma de decisiones
			• Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático.
			• Muestra capacidad de resolver problemas de manera efectiva
			• Se comunica de manera asertiva

3	Estructura la gestión de riesgos en las organizaciones en apego a el marco legal y normativo en México para anticiparse a las inseguridades potenciales en ciberseguridad.	1.- Evalúa los riesgos de ciberseguridad para tomar decisiones informadas sobre la inversión en seguridad y la implementación de políticas y procedimientos que garanticen la confidencialidad, integridad y disponibilidad de la información, a través de la gestión de riesgos.	**Conceptual:**
			• **Gestión de riesgos en ciberseguridad**
			  ○ Plan de Gestión de Riesgos
			  ○ Objetivos de la Gestión de Riesgos
			  ○ Identificación, Apreciación y Tratamiento de riesgos
			Procedimental:
			• Evalúa los riesgos dentro de una organización para reducir o minimizar las inseguridades potenciales.

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL Dirección de Educación Media Superior

			• Evalúa los riesgos para reducir o prevenir resultados desfavorables. **Actitudinal:** • Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

		2.- Compara las diferentes carreras y certificaciones profesionales que existen en materia de ciberseguridad para tomar una decisión y dedicar su proyecto de vida a la ciberseguridad, conociendo el marco legal y normativo en México.	• **Conceptual:**
			• **Educación profesional en ciberseguridad**
			  ○ Carreras y certificaciones
			  ○ Trayectorias profesionales en ciberseguridad
			  ○ Educación y ciberseguridad en México
			• **Marco Legal y Normativo**
			  ○ Cuestiones legales y éticas en Ciberseguridad
			  ○ Leyes Federales de Protección de Datos Personales en Posesión de Particulares y de Sujetos Obligados
			  ○ Normas internacionales
			  ○ Normas nacionales
			• **Procedimental:**
			• Recupera el tipo de educación y las trayectorias profesionales para poder ingresar al mundo de la ciberseguridad teniendo una educación formal.
			• Recupera leyes, normas y cuestiones éticas en el marco de la ciberseguridad para poder aplicar la legislación y normatividad vigente.
			Actitudinal:

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: **Técnico en Programación**

Unidad de Aprendizaje: **Ciberseguridad**

			• Trabaja de manera colaborativa • Hace uso de pensamiento analítico • Desarrolla responsabilidad social • Hace uso de pensamiento crítico y analítico para la resolución de diversos problemas. • Toma de decisiones • Se adapta a los cambios tecnológicos, entendiendo de manera responsable el uso de la seguridad de los datos en un sistema informático. • Muestra capacidad de resolver problemas de manera efectiva • Se comunica de manera asertiva

INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior

Programa Académico: Técnico en Programación

Unidad de Aprendizaje: Ciberseguridad

BIBLIOGRAFÍA BÁSICA Y COMPLEMENTARIA

Número y Nombre de la Unidad Didáctica	FORMATO APA	CLASIFICACIÓN	
		Básico	Consulta
Unidad didáctica 1: Introducción a la Ciberseguridad	Rocío Aldeco Pérez, Gina Gallegos García, & LilMaría Rodríguez Henríquez. (2020). Introducción a la ciberseguridad y sus aplicaciones en México (1.a ed.).	X	
	GUÍA DE CIBERSEGURIDAD para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación		X
Unidad didáctica 2: Protección de Datos y Organizaciones	Rocío Aldeco Pérez, Gina Gallegos García, & LilMaría Rodríguez Henríquez. (2020). Introducción a la ciberseguridad y sus aplicaciones en México (1.a ed.).	X	
	GUÍA DE CIBERSEGURIDAD para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación		X
Unidad didáctica 3: Educación profesional, Marco Legal y Normativo	Rocío Aldeco Pérez, Gina Gallegos García, & LilMaría Rodríguez Henríquez. (2020). Introducción a la ciberseguridad y sus aplicaciones en México (1.a ed.).	X	
	GUÍA DE CIBERSEGURIDAD para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación		X

PODER EJECUTIVO FEDERAL ESTADOS UNIDOS MEXICANOS MÉXICO CDMX
INSTITUTO POLITÉCNICO NACIONAL
Dirección de
Educación Media Superior