PROGRAMA DE ESTUDIOS DE LA UNIDAD DE APRENDIZAJE: SEGURIDAD WEB Y APLICACIONES

CLAVE: 5FP-FM409 CRÉDITOS: 3.37

RAMA DEL CONOCIMIENTO:

* Ingeniería y Ciencias Físico Matemáticas [X]
* Ciencias Sociales y Administrativas [ ]
* Ciencias Médico Biológicas [ ]

ÁREA DE FORMACIÓN CURRICULAR:

Institucional [ ]
Científica, Humanística y Tecnológica Básica [ ]
Profesional [X]

TIPO DE ESPACIO: Aula [X] Taller [ ] Laboratorio [ ]
Otros ambientes de aprendizaje [ ]

MODALIDAD: Escolar [X] No escolarizada [X] Mixta [X]

VIGENCIA A PARTIR DE: AGOSTO 2010

CARRERA: TÉCNICO EN PROGRAMACIÓN

NIVEL: 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [X] 6 [ ]

SEMESTRE: QUINTO

UNIDADES ACADÉMICAS DONDE SE IMPARTE:

Todas: [ ] CECyT: 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ] 6 [ ] 7 [ ] 8 [ ] 9 [X]
10 [ ] 11 [ ] 12 [ ] 13 [ ] 14 [ ] 15 [ ] CET1 [ ]

TIEMPOS ASIGNADOS:

GLOBAL: 54 HRS/18 SEMANAS / SEMESTRE

AULA: 3 HRS / SEMANA TOTAL: 54 HRS / SEMESTRE

TALLER: -- HRS / SEMANA TOTAL: -- HRS / SEMESTRE

LABORATORIO: -- HRS / SEMANA TOTAL: -- HRS / SEMESTRE

OTROS AMBIENTES DE APRENDIZAJE: -- HRS / SEMANA
TOTAL: -- HRS / SEMESTRE

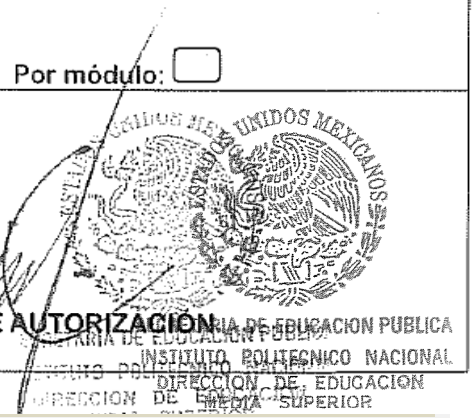
ORGANIZACIÓN:

Por asignatura: [X] Por área: [ ] Por módulo: [ ]

PROCESO DE DISEÑO Y AUTORIZACIÓN

	día	mes	año
ELABORADO POR: REP. ACAD. NMS IPN FECHA DE ELABORACIÓN:	07	08	09
REVISADO POR: DEMS FECHA DE REVISIÓN:	24	08	09
APROBADO POR: CTCE-NMS FECHA DE APROBACIÓN:	07	09	09
AUTORIZADO POR: CPA-CGC FECHA DE AUTORIZACIÓN:	09	09	09

FIRMA Y SELLO DE AUTORIZACIÓN



Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

FUNDAMENTACIÓN

La Unidad de Aprendizaje de Seguridad Web y Aplicaciones pertenece al área de formación Profesional del Bachillerato Tecnológico de la Carrera de Técnico en Programación, Nivel Medio Superior del Instituto Politécnico Nacional. Se ubica en el Quinto nivel y semestre del plan de estudios, se imparte de manera obligatoria en la rama del conocimiento Ingeniería y Ciencias Físico Matemáticas.
Seguridad Web y Aplicaciones es una unidad de aprendizaje integrada por tres unidades didácticas y tiene como propósito principal preparar al estudiante para que desarrolle competencias en el Desarrollo de Software, a través de la utilización de Servicios de Seguridad que permitan la implementación de diferentes mecanismos de Seguridad que proporcionen la protección contra ataques o amenazas que afecten el funcionamiento del sistema.

Por ello las competencias disciplinares, general y particulares del curso implican como principales objetos de conocimiento; aplicar seguridad a los sistemas de información web y aplicaciones, empleando servicios y mecanismos de seguridad establecidos por las tecnologías de la información, con base en estándares de la industria del software, contextualizar los concepto de seguridad en sistemas web y aplicaciones, emplear y examinar algoritmos criptográficos y protocolos fundamentales en aplicaciones de seguridad en redes, emplear herramientas de seguridad en la protección de sistemas de la información. Se parte del enfoque constructivista en el que, el maestro es el facilitador del aprendizaje y el Estudiante participa de manera activa en la adquisición de un aprendizaje significativo, a partir de ejercitar los procedimientos establecidos en este Programa de Estudios.

El enfoque disciplinar tiene una orientación para la programación.

Las principales relaciones con otras unidades de aprendizaje se reflejan en la aplicación de las competencias adquiridas en el desarrollo del proyecto de software que se lleva a cabo en la unidad de aprendizaje de Laboratorio de Proyectos de Tecnologías de la Información III ubicada en el quinto semestre de la carrera y es sucesora de las unidades de aprendizaje de Programación y Servicios Web ubicada en el cuarto semestre de la carrera, a fin de proporcionar una formación integral.

En este sentido, el enfoque didáctico de la unidad incorpora como principales métodos constructivistas el Aprendizaje Basado en Problemas, Aprendizaje Orientado a Proyectos, Método de Casos y Aprendizaje Colaborativo; los cuales deben estar apoyados por una diversidad de materiales multimedia tomando en cuenta los diferentes estilos de aprendizaje de los estudiantes.

La metodología de trabajo de este programa de estudios se basa en estándares de aprendizaje planteados en las competencias. Cada competencia se desagrega en resultados de aprendizaje (RAP) que se abordan a través de actividades sustantivas y tienen como propósito indicar una generalidad para desarrollar las secuencias didácticas que atenderán cada RAP. Las evidencias con las que se evaluará formativamente cada RAP, se definen mediante un desempeño integrado, en el que los estudiantes mostrarán su saber hacer de manera reflexiva, utilizando el conocimiento que va adquiriendo durante el proceso didáctico para luego transferir ese aprendizaje a situaciones similares y diferentes.

El papel del profesor tendrá una intervención mediadora entre los contenidos disciplinarios, las características del contexto y los instrumentos o herramientas que provee al estudiante para facilitar un aprendizaje significativo, estratégico, autónomo y colaborativo a través de haceres reflexivos, críticos y creativos.

Para llevar a cabo de forma adecuada las actividades se requiere de un Profesor Titular que cumpla con el perfil descrito en el apartado de Perfil Docente.

La evaluación de los aprendizajes comprenderá tres momentos: al inicio para diagnosticar los conocimientos previos que permitan establecer conexiones significativas con la propuesta de aprendizaje. Durante el proceso de aprendizaje para cumplir con una función formativa que realimente tanto al estudiante

como al profesor y una final que propicie la acreditación del aprendizaje con fines de promoción a los siguientes niveles o certificación de competencias.

También es posible aplicar una evaluación por competencias para certificar la Unidad de Aprendizaje previo a su inicio.

Los productos y desempeños que desarrolle el estudiante durante el desarrollo del semestre serán integradas en un portafolio de evidencias de aprendizaje y las actividades que se trabaje en equipo se registrarán en un portafolio colaborativo. Los portafolios de evidencias contendrán las evaluaciones correspondientes de los cuestionarios, ejercicios, programas, de cada unidad en forma digital, para facilitar su manejo.

Las rúbricas serán los elementos a integrar para la evaluación del aprendizaje que se utilizarán para cada unidad; las cuales contendrán categorías (conocimientos, habilidades y actitudes) que se desarrollan en cada escenario propuesto, por lo que dentro de los criterios de acreditación en los planes de evaluación por unidad, se presentan las condiciones satisfactorias a considerar dentro de la construcción de las rúbricas, no siendo únicas o discriminantes, por lo que se deben enriquecer con base en las herramientas de aprendizaje propuestas para cada unidad que se describen en las actividades tanto de aprendizaje como de enseñanza.

Estas se integran al portafolio de evidencias mediante un registro por parte del docente para conocer las habilidades, conocimientos y actitudes adquiridas por el estudiante, así como sus deficiencias.

Además de cumplir con las rúbricas como evidencias de aprendizaje, el estudiante deberá realizar un proyecto vinculado a los fines de los sectores sociales que atiende la carrera que incorpore las competencias adquiridas en ésta, aplicándolas en el contexto de la unidad de aprendizaje Laboratorio de Proyectos de Tecnologías de la Información III, desarrollándolo colaborativamente. La evaluación se realizará tomando los aspectos formativos y sumativos.

Este programa de estudios tiene una naturaleza normativa al establecer los estándares para la certificación de competencias, por lo tanto la planeación didáctica de las secuencias, estrategias de aprendizaje y enseñanza se desarrollarán con base en los elementos que incorpora este documento.

Las competencias genéricas que se incorporan a esta unidad de aprendizaje corresponden con el Marco Común del Sistema Nacional de Bachillerato y se establecen en la siguiente matriz.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

MATRÍZ DE VINCULACIÓN DE COMPETENCIAS GENÉRICAS Y DISCIPLINARES

Competencias genéricas / Competencias Genéricas y Disciplinares Particulares	1. Se conoce y valora a sí mismo y aborda problemas y retos teniendo en cuenta los objetivos que persigue	2. Es sensible al arte y participa en la apreciación e interpretación de sus expresiones en distintos géneros.	3. Elige y practica estilos de vida saludables.	4. Escucha, interpreta y emite mensajes pertinentes en distintos contextos mediante la utilización de medios, códigos y herramientas apropiados.	5. Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos.	6. Sustenta una postura personal sobre temas de interés y relevancia general, considerando otros puntos de vista de manera crítica y reflexiva.	7. Aprende por iniciativa e interés propio a lo largo de la vida.	8. Participa y colabora de manera efectiva en equipos diversos.	9. Participa con una conciencia cívica y ética en la vida de su comunidad, región, México y el mundo.	10. Mantiene una actitud respetuosa hacia la interculturalidad y la diversidad de creencias, valores, ideas y prácticas sociales.	11. Contribuye al desarrollo sustentable de manera crítica, con acciones responsables.
RESULTADOS DE APRENDIZAJE											
Competencia Particular 1 — 1.1				X	X			X	X		
Competencia Particular 1 — 1.2				X	X			X			
Competencia Particular 2 — 2.1				X	X	X	X	X			
Competencia Particular 2 — 2.2				X	X	X	X	X			
Competencia Particular 3 — 3.1				X	X			X			
Competencia Particular 3 — 3.2				X	X			X			
Competencia Particular 3 — 3.3				X	X			X			
Competencia Particular 3 — 3.4				X	X			X			
Competencia Particular 3 — 3.5				X	X			X			
Competencia Particular 4 — 4.1				X	X			X			
Competencia Particular 4 — 4.2				X	X	X	X	X			
Competencia Particular 4 — 4.3				X	X			X			

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

RED DE COMPETENCIAS (GENERAL Y PARTICULARES)

Competencia General

Aplica Seguridad a los sistemas de información web y aplicaciones, empleando servicios y mecanismos de seguridad establecidos por las tecnologías de la información, con base en estándares de la industria del software.

Competencia particular 1

Contextualiza los conceptos que caracterizan a la seguridad en sistemas web y aplicaciones.

- **RAP 1.1** Describe los elementos que se relacionan con la seguridad en las tecnologías de la información.
- **RAP 1.2** Contextualiza el concepto de servicio de seguridad con base en estándares establecidos.

Competencia particular 2

Emplea algoritmos criptográficos y protocolos fundamentales en aplicaciones de seguridad en redes.

- **RAP 2.1** Aplica técnicas de cifrado simétrico a través de lenguajes de programación
- **RAP 2.2** Emplea autentificación y criptografía de clave pública para implementar seguridad.

Competencia particular 3

Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e internet..

- **RAP 3.1** Describe las especificaciones de autentificación en la seguridad de redes.
- **RAP 3.2** Describe la seguridad usada en las aplicaciones de correo electrónico a partir de estándares.
- **RAP 3.3** Esquematiza el modelo de seguridad IP.
- **RAP 3.4** Contextualiza el modelo de seguridad Web a través de estándares.
- **RAP 3.5** Describe el sistema de seguridad basado en la gestión de redes.

Competencia particular 4

Emplea herramientas de seguridad en la protección de sistemas de la información.

- **RAP 4.1** Describe enfoques de prevención y detección de intrusos en las tecnologías de la información.
- **RAP 4.2** Aplica mecanismos de seguridad contra las amenazas de software dañino.
- **RAP 4.3** Describe el sistema de seguridad basado en el uso de cortafuegos.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PERFIL DEL DOCENTE

El profesor que imparta la unidad de aprendizaje de seguridad web y aplicaciones habrá de presentar el examen de oposición para mostrar las habilidades que posee en el manejo del conocimiento disciplinar, así como su disposición, autoridad y tolerancia en el manejo de grupos de aprendizaje. Por lo tanto debe contar con las competencias que se indican en las condiciones interiores del trabajo.

Competencias Generales

1. Organiza su formación continua a lo largo de su trayectoria profesional.
2. Domina y estructura los saberes para facilitar experiencias de aprendizajes significativos.
3. Planifica los procesos de enseñanza y de aprendizaje atendiendo al enfoque por competencias y los ubica en los contextos disciplinares, curriculares y sociales amplios.
4. Lleva a la práctica procesos de enseñanza y de aprendizaje de manera efectiva, creativa e innovadora a su contexto institucional.
5. Evalúa los procesos de enseñanza y aprendizaje con un enfoque formativo.
6. Construye ambientes para aprendizaje autónomo y colaborativo.
7. Contribuye a la generación de un ambiente que facilite el desarrollo sano e integral de los estudiantes.
8. Participa en los proyectos de mejora continua de su escuela y apoya la gestión institucional.

Perfil Profesional:

1. Tener título profesional en rama afín a las Tecnologías de la Información, de preferencia con experiencia docente y profesional.
2. Manejo de herramientas de desarrollo de software actuales.
3. Conocimientos en administración de proyectos de software.
4. Manejo de lenguajes de programación actuales.
5. Utilización de las Tecnologías de la Información.
6. Manejo de plataformas de software.
7. Elaboración de planes estratégicos para el desarrollo de software.
8. Conocimiento y aplicación de lenguajes de modelado de software.
9. Manejo de plataformas tecnológicas de aprendizaje.
10. Posee conocimientos sobre el análisis y diseño de sistemas de información y seguridad.
11. Manejo de herramientas multimedia.
12. Aplicación de la normatividad para el desarrollo de sus actividades.
13. Personal íntegra, responsable, honesta, propositiva, tolerante, puntual, respetuosa, dispuesta a la capacitación y actualización necesarias para la labor docente, con facilidad de palabra y comunicación, con vocación docente y compromiso social.
15. Manejo de Lenguajes de programación

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

ESTRUCTURA DIDÁCTICA

UNIDAD DIDÁCTICA No. 1: FUNDAMENTOS Y PROCEDIMIENTOS DE SEGURIDAD						
COMPETENCIA PARTICULAR: Contextualiza los conceptos que caracterizan a la seguridad en sistemas web y aplicaciones.						
RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 1.1: Describe los elementos que se relacionan con la seguridad en las tecnologías de la información.						
			TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas			
CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		**AMBIENTE DE APRENDIZAJE**	**EVIDENCIA DE APRENDIZAJE**	**CRITERIOS DE EVALUACIÓN FORMATIVA**	**MATERIALES Y RECURSOS DIDACTICOS**
	DE APRENDIZAJE	**DE ENSEÑANZA**				
CONCEPTUALES Amenazas y Ataques Ataques pasivos Ataques activos. **PROCEDIMENTALES** Habilidad para describir el funcionamiento la seguridad en las tecnologías de la información. **ACTITUDINALES** Se expresa y comunica Piensa crítica y reflexivamente. Trabaja en forma colaborativa.	Identifica los elementos de la seguridad en las tecnologías de la información. Organiza la información nueva respecto a la Seguridad en las tecnologías de la información. Describe el funcionamiento y las características de la seguridad en las tecnologías de la información por medio de ejemplos.	Presenta información de las características de la seguridad en las tecnologías de la información Supervisa la discusión de ideas y conceptos de seguridad en las tecnologías de la información. Presenta escenarios con ejemplos de utilización de seguridad en las tecnologías de la información. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de seguridad en las tecnologías de la información y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de la seguridad en las tecnologías de la información son identificadas e infiere conclusiones a partir de ellas. La información de la seguridad en las tecnologías de la información es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 1: FUNDAMENTOS Y PROCEDIMIENTOS DE SEGURIDAD

COMPETENCIA PARTICULAR: Contextualiza los conceptos que caracterizan a la seguridad en sistemas web y aplicaciones.

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 1.2: Contextualiza el concepto de servicio de seguridad con base en estándares establecidos.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Seguridad Servicios de Seguridad Mecanismos de Seguridad Estándares de Seguridad **PROCEDIMENTALES** Habilidad para identificar y organizar conceptos de los servicios de seguridad en las tecnologías de la información. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica los conceptos de los servicios de seguridad en las tecnologías de la información con base en estándares. Organiza la información nueva respecto a los servicios de seguridad en las tecnologías de la información. Describe el funcionamiento y las características de los servicios de seguridad en las tecnologías de la información.	Presenta información de los servicios de seguridad en las tecnologías de la información. Supervisa la discusión de ideas y conceptos de los servicios de seguridad en las tecnologías de la información. Presenta escenarios con ejemplos de los servicios de seguridad en las tecnologías de la información. Facilita la elaboración de modelos a partir de información obtenida. Promueve la participación en la exposición de ideas y conceptos	Dentro del Aula.	Esquematiza los servicios de seguridad en las tecnologías de la información.	Las ideas clave de los servicios de seguridad en las tecnologías de la información son Identificadas e infiere conclusiones a partir de ellas. La información de los servicios de seguridad en las tecnologías de la información es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás de manera reflexiva. El esquema de los servicios de seguridad en las tecnologías de la información es realizado.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 2: CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA

COMPETENCIA PARTICULAR: Emplea algoritmos criptográficos y protocolos fundamentales en aplicaciones de seguridad en redes.

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 2.1: Aplica técnicas de cifrado simétrico a través de lenguajes de programación

TIEMPO ESTIMADO PARA OBTENER EL RAP: 12 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Cifrado Simétrico Principios de cifrado simétrico Algoritmos de cifrado simétrico Modos de operación del cifrado por bloques Distribución de claves **PROCEDIMENTALES** Habilidad para programar los elementos fundamentales del cifrado simétrico. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Aprende de forma autónoma Trabaja en forma colaborativa	Analiza e identifica los principales elementos del cifrado simétrico en un escenario planteado. Investiga acerca de las características del cifrado simétrico y los modos de operación del cifrado por bloques. Soluciona escenario utilizando cifrado simétrico.	Presenta el escenario que involucra cifrado simétrico. Facilita la formación de los conceptos relacionados al cifrado simétrico. Orienta la investigación del cifrado simétrico y aplicaciones del mismo. Supervisa la solución del escenario por medio de programación.	Dentro del Aula.	Soluciona el escenario y define los elementos del cifrado simétrico, características y programa ejemplos del mismo.	Las ideas y conceptos del cifrado simétrico son expresadas mediante representaciones lingüísticas, o gráficas. El cifrado simétrico se realiza utilizando las tecnologías de la información para procesar e interpretar información. Estructura ideas y argumentos de manera clara, coherente y sintética. Define metas y da seguimiento a sus procesos de construcción de conocimiento. Propone maneras de solucionar un problema en equipo, definiendo un curso de acción con pasos específicos.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de texto. Software de modelado. Entorno de Programación.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 2: CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA

COMPETENCIA PARTICULAR: Emplea algoritmos criptográficos y protocolos fundamentales en aplicaciones de seguridad en redes.

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 2.2: Emplea autentificación y criptografía de clave pública para implementar seguridad.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 12 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Criptografía de clave pública y autentificación. Autentificación mediante cifrado. Funciones Hash. Principios de criptografía de clave pública. Algoritmos de criptografía de clave pública. Firmas Digitales. Gestión de Claves. **PROCEDIMENTALES** Habilidad para aplicar autentificación y criptografía de clave pública. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Aprende de forma autónoma Trabaja en forma colaborativa	Analiza e identifica los principales elementos de la autentificación y criptografía de clave pública en un escenario planteado. Investiga acerca de la autentificación y criptografía de clave pública. Soluciona escenario utilizando autentificación y criptografía de clave pública	Presenta el escenario que involucra autentificación y criptografía de clave pública. Facilita la formación de los conceptos relacionados a la autentificación y criptografía de clave pública. Orienta la investigación de la autentificación y criptografía de clave pública; así como aplicaciones de las mismas. Supervisa la solución del escenario por medio de programación.	Dentro del Aula . .	Soluciona el escenario y define los elementos de la autentificación y criptografía de clave pública, características y programa ejemplos de los mismos.	Las ideas y de la autentificación y criptografía de clave pública son expresadas mediante representaciones lingüísticas, o gráficas. La autentificación y criptografía de clave pública se realiza utilizando las tecnologías de la información para procesar e interpretar información. Estructura ideas y argumentos de manera clara, coherente y sintética. Define metas y da seguimiento a sus procesos de construcción de conocimiento. Propone maneras de solucionar un problema en equipo, definiendo un curso de acción con pasos específicos.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de texto. Software de modelado. Entorno de Programación.

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 3: SEGURIDAD EN REDES

COMPETENCIA PARTICULAR: Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet.

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 3.1: Describe las especificaciones de autentificación en la seguridad de redes.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Aplicaciones de autentificación Kerberos Certificados **PROCEDIMENTALES** Habilidad para identificar y organizar conceptos de autentificación en la seguridad de redes. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Aprende de forma autónoma Trabaja en forma colaborativa	Identifica los elementos de autentificación en la seguridad de redes. Organiza la información nueva respecto a la autentificación en la seguridad de redes. Describe el funcionamiento y las características de la autentificación en la seguridad de redes por medio de ejemplos.	Presenta información de las características de la autentificación en la seguridad de redes. Supervisa la discusión de ideas y conceptos de autentificación en la seguridad de redes. Presenta escenarios con ejemplos de utilización de autentificación en la seguridad de redes. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de la autentificación en la seguridad de redes y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de la autentificación en la seguridad de redes son identificadas e infiere conclusiones a partir de ellas. La información de la autentificación en la seguridad de redes es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 3: SEGURIDAD EN REDES

COMPETENCIA PARTICULAR: Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 3.2: Describe la seguridad usada en las aplicaciones de correo electrónico a partir de estándares.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Seguridad en el correo electrónico Claves criptográficas y archivos de claves. Gestión de clave pública. S/MIME **PROCEDIMENTALES** Habilidad para organizar conceptos y describir la seguridad en aplicaciones de correo electrónico **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica los elementos de seguridad en aplicaciones de correo electrónico a partir de estándares. Organiza la información nueva respecto a la seguridad en aplicaciones de correo electrónico. Describe el funcionamiento y las características de seguridad en aplicaciones de correo electrónico por medio de ejemplos.	Presenta información de las características de seguridad en aplicaciones de correo electrónico Supervisa la discusión de ideas y conceptos de seguridad en aplicaciones de correo electrónico. Presenta escenarios con ejemplos de utilización de seguridad en aplicaciones de correo electrónico Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de seguridad en aplicaciones de correo electrónico y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de seguridad en aplicaciones de correo electrónico son identificadas e infiere conclusiones a partir de ellas. La información seguridad en aplicaciones de correo electrónico es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 3: SEGURIDAD EN REDES

COMPETENCIA PARTICULAR: Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 3.3: Esquematiza el modelo de seguridad IP.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Seguridad IP Aplicaciones de autentificación Arquitectura de seguridad IP Gestión de claves **PROCEDIMENTALES** Habilidad para organizar conceptos y describir el funcionamiento del modelo de seguridad IP. **ACTITUDINALES** Se expresa y comunica. Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica las características de la modelo de seguridad IP. Organiza la información nueva respecto al modelo de seguridad IP. Describe el funcionamiento y las características del modelo de seguridad IP por medio de ejemplos.	Presenta información del modelo de seguridad IP. Supervisa la discusión de ideas y conceptos del modelo de seguridad IP. Presenta escenarios con ejemplos de utilización del modelo de seguridad IP. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula	Define conceptos del modelo de seguridad IP y clasifica información por características y elabora ejemplos.	Las ideas clave del modelo de seguridad IP. son identificadas e infiere conclusiones a partir de ellas. La información del modelo de seguridad IP es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás de manera reflexiva.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de texto.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 3: SEGURIDAD EN REDES

COMPETENCIA PARTICULAR: Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 3.4: Contextualiza el modelo de seguridad Web a través de estándares.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Seguridad de la web Amenazas de seguridad web SSL (Secure Socket Layer) y TLS (Transport Layer Security) SEL (Secure Electronic Transaction) **PROCEDIMENTALES** Habilidad para identificar y organizar conceptos del modelo de seguridad Web con base en estándares. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica los conceptos del modelo de seguridad Web con base en estándares. Organiza la información nueva respecto al modelo de seguridad Web con base en estándares. Describe el funcionamiento y las características del modelo de seguridad Web con base en estándares.	Presenta información del modelo de seguridad Web con base en estándares. . Supervisa la discusión de ideas y conceptos del modelo de seguridad Web con base en estándares. Presenta escenarios con ejemplos del modelo de seguridad Web con base en estándares. Facilita la elaboración de modelos a partir de información obtenida. Promueve la participación en la exposición de ideas y conceptos	Dentro del Aula.	Esquematiza el modelo de seguridad Web con base en estándares.	Las ideas clave del modelo de seguridad Web con base en estándares son Identificadas e infiere conclusiones a partir de ellas. La información de modelo de seguridad Web con base en estándares. es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás de manera reflexiva. El esquema de los servicios de seguridad en las tecnologías de la información es realizado.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 3: SEGURIDAD EN REDES

COMPETENCIA PARTICULAR: Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 3.5: Describe el sistema de seguridad basado en la gestión de redes.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Seguridad en la gestión de redes SNMP **PROCEDIMENTALES** Habilidad para identificar y organizar conceptos de seguridad con base en la gestión de redes. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica los elementos de la seguridad con base en la gestión de redes. Organiza la información nueva respecto a la Seguridad con base en la gestión de redes. Describe el funcionamiento y las características de la seguridad con base en la gestión de redes por medio de ejemplos.	Presenta información de las características de la seguridad con base en la gestión de redes. Supervisa la discusión de ideas y conceptos de seguridad con base en la gestión de redes. Presenta escenarios con ejemplos de utilización de seguridad con base en la gestión de redes. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de seguridad con base en la gestión de redes y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de la seguridad con base en la gestión de redes.son identificadas e infiere conclusiones a partir de ellas. La información de la seguridad con base en la gestión de redes.es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 4: SEGURIDAD EN SISTEMAS

COMPETENCIA PARTICULAR: Emplea herramientas de seguridad en la protección de sistemas de la información.

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 4.1: Describe enfoques de prevención y detección de intrusos en las tecnologías de la información.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Intrusos Detección de intrusos Gestión de contraseñas **PROCEDIMENTALES** Habilidad para identificar y organizar conceptos de prevención y detección de intrusos en las tecnologías de la información. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa	Identifica los elementos de prevención y detección de intrusos en las tecnologías de la información. Organiza la información nueva respecto a la prevención y detección de intrusos en las tecnologías de la información Describe el funcionamiento y las características de la prevención y detección de intrusos en las tecnologías de la información por medio de ejemplos.	Presenta información de las características de la prevención y detección de intrusos en las tecnologías de la información. Supervisa la discusión de ideas y conceptos de prevención y detección de intrusos en las tecnologías de la información. Presenta escenarios con ejemplos de utilización de prevención y detección de intrusos en las tecnologías de la información. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de prevención y detección de intrusos en las tecnologías de la información y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de prevención y detección de intrusos en las tecnologías de la información son identificadas e infiere conclusiones a partir de ellas. La información de prevención y detección de intrusos en las tecnologías de la información es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 4: SEGURIDAD EN SISTEMAS

COMPETENCIA PARTICULAR: Emplea herramientas de seguridad en la protección de sistemas de la información

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 4.2: Aplica mecanismos de seguridad contra las amenazas de software dañino.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Software dañino Virus Antivirus **PROCEDIMENTALES** Habilidad para modelar seguridad contra amenazas de software dañino. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Aprende de forma autónoma Trabaja en forma colaborativa	Investiga las características de seguridad contra las amenazas de software dañino. Analiza el funcionamiento de los mecanismos de seguridad contra las amenazas de software dañino. Aplica mecanismos de seguridad contra las amenazas de software dañino. Organiza la información nueva respecto a mecanismos de seguridad contra las amenazas de software dañino.	Orienta la investigación del estudiante con respecto a mecanismos de seguridad contra las amenazas de software dañino y sus características. Facilita la formación de los conceptos relacionados a mecanismos de seguridad contra las amenazas de software dañino. Facilita la elaboración de modelos a partir de información obtenida. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula	Modela seguridad con mecanismos contra las amenazas de software dañino utilizados en Internet, ejemplificando los mismos. .	- Las ideas y conceptos de mecanismos de seguridad contra las amenazas de software dañino se expresan mediante representaciones lingüísticas, o gráficas. - Sigue instrucciones y procedimientos de manera reflexiva, comprendiendo como cada uno de sus pasos contribuye al alcance de un objetivo. - Define metas y da seguimiento a sus procesos de construcción de conocimiento. - La solución al problema de modelado de seguridad con mecanismos contra las amenazas de software dañino es propuesta en equipo, definiendo un curso de acción con pasos específicos.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de texto.

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

UNIDAD DIDÁCTICA No. 4: SEGURIDAD EN SISTEMAS

COMPETENCIA PARTICULAR: Emplea herramientas de seguridad en la protección de sistemas de la información

RESULTADO DE APRENDIZAJE PROPUESTO (RAP) No. 4.3: Describe el sistema de seguridad basado en el uso de cortafuegos.

TIEMPO ESTIMADO PARA OBTENER EL RAP: 3 Horas

CONTENIDOS DE APRENDIZAJE	ACTIVIDADES SUSTANTIVAS		AMBIENTE DE APRENDIZAJE	EVIDENCIA DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN FORMATIVA	MATERIALES Y RECURSOS DIDACTICOS
	DE APRENDIZAJE	DE ENSEÑANZA				
CONCEPTUALES Cortafuegos Diseño de cortafuegos Sistemas de confianza **PROCEDIMENTALES** Habilidad para organizar conceptos y describir la seguridad basado en el uso de cortafuegos. **ACTITUDINALES** Se expresa y comunica Piensa critica y reflexivamente Trabaja en forma colaborativa.	Identifica los elementos de la seguridad basado en el uso de cortafuegos. Organiza la información nueva respecto a la Seguridad basado en el uso de cortafuegos Describe el funcionamiento y las características de la seguridad basado en el uso de cortafuegos por medio de ejemplos.	Presenta información de las características de la seguridad basado en el uso de cortafuegos Supervisa la discusión de ideas y conceptos de seguridad basado en el uso de cortafuegos. Presenta escenarios con ejemplos de utilización de seguridad basado en el uso de cortafuegos. Promueve la participación en la exposición de ideas y conceptos.	Dentro del Aula.	Define los elementos de seguridad basado en el uso de cortafuegos y los clasifica de acuerdo a características y elabora ejemplos de los mismos.	Las ideas clave de seguridad basada en el uso de cortafuegos son identificadas e infiere conclusiones a partir de ellas. La información de seguridad basada en el uso de cortafuegos es ordenada de acuerdo a categorías, jerarquías y relaciones. Aporta puntos de vista y considera reflexivamente el de los demás.	Tecnologías de la información y comunicación. Materiales didácticos multimedia. Material de apoyo hipertextual. Software de procesamiento de Texto. Software de modelado

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PLAN DE EVALUACIÓN SUMATIVA DEL CURSO

No. DE UNIDAD DIDÁCTICA	EVIDENCIA INTEGRADORA DE LA COMPETENCIA PARTICULAR (DESEMPEÑO, CONOCIMIENTO, PRODUCTO)	CRITERIOS DE EVALUACIÓN	PORCENTAJE DE ACREDITACIÓN
1	Elabora descripción del funcionamiento y características de seguridad en las tecnologías de la información, contextualizando con ejemplos.	Las características y conceptos corresponden a la seguridad en las tecnologías de la información, identificando fundamentos y contextualizando por medio de ejemplos.	10%
2	Presenta solución de escenarios propuestos, empleando algoritmos criptográficos y protocolos en aplicaciones de seguridad en redes.	Utiliza algoritmos criptográficos, autentificación, criptografía de clave pública y aplica técnicas de cifrado simétrico por medio de programas para proveer seguridad en redes.	50%
3	Esquematiza modelo para proporcionar seguridad a redes e Internet.	Las características y conceptos corresponden a la seguridad en las redes, identificando fundamentos y contextualizando por medio de ejemplos	20%
4	Aplica herramientas de seguridad contra las amenazas de software dañino	Utiliza herramientas y mecanismos para proporcionar seguridad contra ataques de software dañino que atente contra las tecnologías de la información.	20%

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

EVIDENCIA INTEGRADORA DE LA COMPETENCIA GENERAL O UNIDAD DE APRENDIZAJE (DESEMPEÑO, CONOCIMIENTO, PRODUCTO)	CRITERIOS DE EVALUACIÓN
Desarrolla modelo de seguridad utilizando fundamentos y mecanismos establecidos por los servicios de seguridad de aplicaciones y redes, aplicando algoritmos de criptografía e implementando a través de programas.	Descripción de fundamentos de seguridad en las tecnologías de la información y prevención de ataques a través de servicios y mecanismos de seguridad. Diseño de seguridad implementando algoritmos de cifrado simétrico, autentificación y clave publica Elaboración de proyecto integrador, justificando implementación de seguridad a través de la utilización de servicios web.
	100%

Carrera: TÉCNICO EN PROGRAMACIÓN Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

REFERENCIAS DOCUMENTALES

No.	TÍTULO DEL DOCUMENTO	TIPO			DATOS DEL DOCUMENTO		CLASIFICACIÓN	
		Libro	Antología	Otro (especifique)	AUTOR (ES)	EDITORIAL Y AÑO	BASICO	CONSULTA
1	Fundamentos de Seguridad en Redes. Aplicaciones y Estándares	X			William Stallings	Pearson Prentice Hall 2004	X	
2	Seguridad en Redes Telemáticas	X			Justo Cariacedo Gallardo	McGrawHill 2004	X	
3	Sistemas Distribuidos Conceptos y Diseño	X			Coulouris George Dollimore Jean Kindberg	Pearson Addison Wesley 2001		X
4	Sistemas Distribuidos Principios y Paradigmas	X			Tanenbaum Andrew S. Van Steen Maarten	Pearson Prentice Hall 2008		X
5	Ingeniería del Software	X			Sommerville Ian	Pearson Addison Wesley 2005		X
6	Ingeniería del Software	X			Pressman Roger S.	McGrawHill 2005		X

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PÁGINAS ELECTRÓNICAS

UNIDAD (ES) DEL PROGRAMA	Autor, Título y Dirección Electrónica	DATOS DE LA PÁGINA CONTENIDO PRINCIPAL				CLASIFICACIÓN	
		Texto	Simuladores	Imágenes	Otro	Básico	Consulta
1,2	S/A , Seguridad Informática, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica , 29/Octubre/2009	**X**				**X**	
1	S/A , Seguridad Informática ¿Qué, porqué y para qué?, http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm , 29/Octubre/2009				**X**		**X**
1,2	Máximo Merlat , Seguridad Informática, http://www.monografias.com/trabajos/hackers/hackers.shtml , 29/Octubre/2009	**X**				**X**	**X**
2	S/A , Criptografía, http://es.wikipedia.org/wiki/Criptograf%C3%ADa , 29/Octubre/2009				**X**	**X**	**X**
2	S/A, Encriptación, http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion , 29/Octubre/2009				**X**		**X**
3,4	S/A, Programación, http://www.programación.com , 29/Octubre/2009				**X**		**X**

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PROGRAMA SINTÉTICO

COMPETENCIA GENERAL (DE LA UNIDAD DE APRENDIZAJE) :
Desarrolla Sistemas Distribuidos empleando modelos establecidos en la interconexión de redes y las tecnologías de la información, con base en protocolos y estándares de la industria del software.

COMPETENCIA PARTICULAR (DE CADA UNIDAD DIDACTICA)	RAP	CONTENIDOS
1. Contextualiza los conceptos que caracterizan a la seguridad en sistemas web y aplicaciones.	1.1 Describe los elementos que se relacionan con la seguridad en las tecnologías de la información. 1.2 Contextualiza el concepto de servicio de seguridad con base en estándares establecidos.	**CONCEPTUALES** - Amenazas y Ataques - Ataques pasivos - Ataques activos - Seguridad - Servicios de Seguridad - Mecanismos de Seguridad - Estándares de Seguridad **PROCEDIMENTALES** - Habilidad para describir el funcionamiento la seguridad en las tecnologías de la información. - Habilidad para identificar y organizar conceptos de los servicios de seguridad en las tecnologías de la información.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PROGRAMA SINTÉTICO

COMPETENCIA PARTICULAR (DE CADA UNIDAD DIDACTICA)	RAP	CONTENIDOS
2. Emplea algoritmos criptográficos y protocolos fundamentales en aplicaciones de seguridad en redes.	2.1. Aplica técnicas de cifrado simétrico a través de lenguajes de programación 2.2 Emplea autentificación y criptografía de clave pública para implementar seguridad.	**CONCEPTUALES** - Cifrado Simétrico - Principios de cifrado simétrico - Algoritmos de cifrado simétrico - Modos de operación del cifrado por bloques - Distribución de claves - Criptografía de clave pública y autentificación - Autentificación mediante cifrado - Funciones Hash - Principios de criptografía de clave pública - Algoritmos de criptografía de clave pública - Firmas Digitales - Gestión de Claves **PROCEDIMENTALES** - Habilidad para programar los elementos fundamentales del cifrado simétrico. - Habilidad para aplicar autentificación y criptografía de clave pública.

PROGRAMA SINTÉTICO

COMPETENCIA PARTICULAR (DE CADA UNIDAD DIDACTICA)	RAP	CONTENIDOS
3. Examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes e Internet	3.1 Describe las especificaciones de autentificación en la seguridad de redes. 3.2 Describe la seguridad usada en las aplicaciones de correo electrónico a partir de estándares. 3.3 Esquematiza el modelo de seguridad IP. 3.4 Contextualiza el modelo de seguridad Web a través de estándares. 3.5 Describe el sistema de seguridad basado en la gestión de redes.	**CONCEPTUALES** - Aplicaciones de autentificación - Kerberos - Certificados - Seguridad en el correo electrónico - Claves criptográficas y archivos de claves - Gestión de clave pública - S/MIME - Seguridad IP - Aplicaciones de autentificación - Arquitectura de seguridad IP - Gestión de claves - Seguridad de la web - Amenazas de seguridad web - SSL (Secure Socket Layer) y TLS (Transport Layer Security) - SEL (Secure Electronic Transaction) - Seguridad en la gestión de redes . SNMP **PROCEDIMENTALES** - Habilidad para identificar y organizar conceptos de autentificación en la seguridad de redes. - Habilidad para organizar conceptos y describir la seguridad en aplicaciones de correo electrónico. - Habilidad para organizar conceptos y describir el funcionamiento del modelo de seguridad IP. - Habilidad para identificar y organizar conceptos del modelo de seguridad Web con base en estándares. - Habilidad para identificar y organizar conceptos de seguridad con base en la gestión de redes.

Carrera: TÉCNICO EN PROGRAMACIÓN

Unidad de Aprendizaje: SEGURIDAD WEB Y APLICACIONES

PROGRAMA SINTÉTICO

COMPETENCIA PARTICULAR (DE CADA UNIDAD DIDACTICA)	RAP	CONTENIDOS
4. Emplea herramientas de seguridad en la protección de sistemas de la información. .	4.1 Describe enfoques de prevención y detección de intrusos en las tecnologías de la información. 4.2 Aplica mecanismos de seguridad contra las amenazas de software dañino. 4.3 Describe el sistema de seguridad basado en el uso de cortafuegos.	**CONCEPTUALES** - Intrusos - Detección de intrusos - Gestión de contraseñas - Software dañino - Virus - Antivirus - Cortafuegos - Diseño de cortafuegos - Sistemas de confianza **PROCEDIMENTALES** - Habilidad para identificar y organizar conceptos de prevención y detección de intrusos en las tecnologías de la información.. - Habilidad para modelar seguridad contra amenazas de software dañino. - Habilidad para organizar conceptos y describir la seguridad basado en el uso de cortafuegos.