1. DATOS DE LA ASIGNATURA

Nombre de la Asignatura	**Seguridad Informática**
Carrera	**Ingeniería en Sistemas Computacionales**
Clave de la asignatura	**SDD-1702**
Créditos	**2-3-5**

2. PRESENTACIÓN

Caracterización de la asignatura.

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad de identificar las amenazas y vulnerabilidades que existe en la infraestructura de red de una organización, de tal forma que puede hacer un análisis de riesgos.

Además, permite identificar e integrar los mecanismos de seguridad y la infraestructura tecnológica necesaria para asegurar la disponibilidad, confidencialidad e integridad de la información en las redes de computadoras.

Permite también al alumno, aplicar mecanismos de mejora continua en los servicios de tecnologías de información y comunicaciones, encaminados a satisfacer las necesidades de los usuarios.

Proporciona al estudiante la capacidad necesaria para diseñar aplicaciones Web con los mecanismos de seguridad necesarios para su funcionalidad.

Intención didáctica.

El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el manejo de estándares, protocolos, métodos, reglas, herramientas y leyes que permitan minimizar los posibles riesgos a la infraestructura o a la información. Para esta asignatura se requiere de conocimientos sobre software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas.

Además se contempla el desarrollo de habilidades para el planteamiento de problemas, trabajo en equipo, asimismo, elementos que propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; las actividades teóricas se han descrito como actividades previas al tratamiento práctico de los temas. En las actividades prácticas sugeridas, es conveniente que el profesor sólo guie al estudiante en la construcción de su conocimiento.

En el primer tema se abordan aspectos de la seguridad informática, el valor de la información y posibles riesgos a los que está expuesto una organización.

En el segundo tema se abordan los algoritmos criptográficos desarrollados a lo largo de la historia, así como un análisis de las técnicas de cifrado de datos se programa los algoritmos utilizando un lenguaje de programación orientado a objetos.

El tema tres presenta la autentificación a nivel de red, que es utilizada para proteger la información adoptando medidas de seguridad, uso de protocolos de transmisión segura firewalls y redes privadas virtuales.

El tema cuatro plantea la seguridad en los servicios principales de internet como DNS, Web, Correo y FTTP.

Finalmente el tema cinco plantea la autentificación que debe incluirse en las aplicaciones tipo Web dentro de esquemas lógicos como directorio activo y el Ldap.

El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el desarrollo de habilidades para la experimentación, tales como: identificación, manejo e implementación de software especializado de seguridad, desarrollo de algoritmos de cifrado de datos, uso de lenguajes de programación orientados a objetos, herramientas para seguridad en redes; planteamiento de problemas; trabajo en equipo; asimismo, propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; por esta razón varias de las actividades prácticas se han descrito como actividades previas al tratamiento teórico de los temas, de manera que no sean una mera corroboración de lo visto previamente en clase, sino una oportunidad para conceptualizar a partir de lo observado.

En las actividades prácticas sugeridas, es conveniente que el profesor busque sólo guiar a sus alumnos para que ellos hagan la elección de los elementos a programar y la manera en que los tratarán. Para que aprendan a planificar, que no planifique el profesor todo por ellos, sino involucrarlos en el proceso de planeación. La lista de actividades de aprendizaje no es exhaustiva, se sugieren sobre todo las necesarias para hacer más significativo y efectivo el aprendizaje. Algunas de las actividades sugeridas pueden hacerse como actividad extra clase y comenzar el tratamiento en clase a partir de la discusión de los resultados de las observaciones, incluyendo posibles actividades en línea, en caso de poder contar con un sistema gestor de contenidos. Se busca partir de hacer los procesos de manera manual, para que el estudiante se acostumbre a reconocer el funcionamiento de los algoritmos y de las técnicas de protección y no sólo se hable de ellos en el aula. Es importante ofrecer escenarios distintos, ya sean construidos, artificiales, virtuales o naturales.

En las actividades de aprendizaje sugeridas, generalmente se propone la formalización de los conceptos a partir de experiencias concretas; se busca que el alumno tenga el primer contacto con el concepto en forma concreta y sea a través de la observación, la reflexión y la discusión que se dé la formalización; la resolución de problemas se hará después de este proceso. Esta resolución de problemas no se especifica en la descripción de actividades, por ser más familiar en el desarrollo de cualquier curso. Pero se sugiere que se diseñen problemas con datos faltantes o sobrantes de manera que el alumno se ejercite en la identificación de datos relevantes y elaboración de supuestos.

En el transcurso de las actividades programadas es muy importante que el estudiante aprenda a valorar las actividades que lleva al cabo y entienda que está construyendo su hacer futuro y en consecuencia actúe de una manera profesional; de igual manera, aprecie la importancia del conocimiento y los hábitos de trabajo; desarrolle la precisión y la curiosidad, la puntualidad, el entusiasmo y el interés, la tenacidad, la flexibilidad y la autonomía.

Es necesario que el profesor ponga atención y cuidado en estos aspectos en el desarrollo de las actividades de aprendizaje de esta asignatura.

3. COMPETENCIAS A DESARROLLAR

Competencias específicas:	**Competencias genéricas:**
Diseña mecanismos de seguridad para redes de computadoras, desarrolla algoritmos de cifrado de datos, e implementa esquemas lógicos de	**Competencias instrumentales** • Capacidad de análisis y síntesis • Capacidad de organizar y planificar • Comunicación oral y escrita

seguridad para apoyar la productividad de las organizaciones.	• Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Habilidades del manejo de la computadora. **Competencias interpersonales** • Capacidad crítica y autocrítica • Trabajo en equipo • Habilidades interpersonales. • Capacidad de comunicarse con profesionales de otras áreas. **Competencias sistémicas** • Capacidad de aplicar los conocimientos en la práctica • Habilidades de investigación • Capacidad de aprender • Capacidad de generar nuevas ideas (creatividad). • Habilidad para trabajar en forma autónoma. • Capacidad de diseñar y gestionar proyectos. • Iniciativa y espíritu emprendedor.

4. HISTORIA DEL PROGRAMA

Lugar y Fecha de Elaboración o Revisión	Participantes	Observaciones (cambios y justificación)
Instituto Tecnológico Superior de Coatzacoalcos. Instituto Tecnológico Superior de Chicontepec. Instituto Tecnológico Superior de Comalcalco. Instituto Tecnológico Superior de Teziutlán.	Academia de Ingeniería en sistemas computacionales.	Análisis y enriquecimiento de los programas por competencias generados en reuniones nacionales en el 2012.
Instituto Tecnológico Superior de Puerto Peñasco	Academia de Ingeniería en Sistemas Computacionales	Análisis y Revisión de Temario en renovación y diseño de la especialidad 2017

5. OBJETIVOS GENERALES DEL CURSO (competencia específica a desarrollar en el curso)

Diseña mecanismos de seguridad para redes de computadoras, desarrolla algoritmos de cifrado de datos, e implementa esquemas lógicos de seguridad para apoyar la productividad de las organizaciones.

6. COMPETENCIAS PREVIAS

Conocimiento de:

- Modelo de Referencia OSI.
- Configuración básica de redes.
- Desarrollo de aplicaciones web.
- Manejo de lenguajes de programación orientada a objetos.

7. TEMARIO

Unidad y Tema	Subtemas
1. Introducción a la seguridad en Redes	1.1 Definición 1.1.1Seguridad física 1.1.2Seguridad lógica 1.1.3 Niveles de seguridad 1.2 Análisis de requerimientos de seguridad 1.2.1 Amenazas 1.2.2 Vulnerabilidades 1.2.3 Riesgos 1.2.4 Tipos de ataques 1.2.4.1 Denegación del servicio 1.2.4.2 Suplantación de la identidad 1.2.5 Técnicas de Inserción 1.3Política de seguridad informática
2. Criptografía	2.1 Definición de criptografía 2.1.1 Tipos de cifrado 2.1.1.1 Cifrado por sustitución 2.1.1.2 Cifrado por transposición 2.2 Criptosistemas de Clave Secreta. 2.2.1 Generalidades sobre sistemas de clave secreta. 2.2.2 Algoritmo DES (Data Encryption Standard). 2.2.3 Modos de cifra en bloque. 2.2.4 Algoritmo IDEA (International Data Encryption Algorithm). 2.2.5 Algoritmo AES (Advanced Encryption Standard). 2.3 Criptosistemas de Cifrado en Flujo 2.3.1 Cifradores con clave continua de un solo uso. 2.3.2 Postulados de Golomb para secuencias cifrantes. 2.3.3 Estructuras generadoras de secuencias cifrantes. 2.3.4 Cifrados en flujo con registros de desplazamiento.

	2.4 Criptosistemas de Clave Pública 2.4.1 Introducción a la cifra con clave pública. 2.4.2 Protocolo de Diffie y Hellman para el intercambio de claves. 2.4.3 Cifradores de mochila de Merkle-Hellman. 2.4.4 Cifrado RSA. 2.4.5 Cifrado ElGamal
3. Autenticación	3.1 Protocolos de Autenticación 3.1.1 Claves secretas compartidas 3.1.2 Centros de distribución de claves 3.1.3 Claves públicas 3.1.4 Ejemplos de protocolos de autenticación 3.2 Firmas Digitales 3.2.1 Firmas digitales de clave simétrica 3.2.2 Firmas digitales de llave pública 3.3 Cortafuegos (firewalls) 3.3.1 Alcances y limitaciones 3.3.2 Componentes 3.3.3 Filtros de paquetes 3.3.4 Filtro de servicios
4. Seguridad en los servicios de internet	4.1 Seguridad en la Web 4.1.1 Asignación segura de nombres de dominio (DNS) 4.1.2 Capa de sockets seguros 4.1.3 HTTP Seguro 4.1.4 Seguridad en correo electrónico 4.1.5 MIME Seguro 4.1.6 PGP, GPG
5. Aplicaciones Multimedia.	5.1 Definición 5.2 Tipos de autenticación 5.3 Protocolo LDAP 5.4 Servicio Active Directory 5.5 Autenticación de aplicaciones web con LDAP 5.6 Autenticación de aplicaciones web con Active Directory 5.7 Integración de aplicaciones web con directorios ligeros de datos

8. SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

- Plantear casos de estudio para ser analizados de manera grupal.
- Realizar visitas a empresas de la región que cuenten con mecanismos de seguridad implementados en sus servidores para vincular los contenidos teóricos con la práctica.
- Solicitar la realización de investigaciones documentales como apoyo, y a partir de éstas, hacer análisis y realizar debates.
- Realizar exposiciones de los proyectos que se realicen, en donde se ilustren los inconvenientes en la configuración y la forma en que se superaron.

- Elaboración de proyectos utilizando un sistema operativo de red en donde se configuren los mecanismos de seguridad de cada unidad en redes convencionales e inalámbricas.
- Organización de conferencias y mesas de debate con especialistas en seguridad de redes que compartan su experiencia y conocimiento en la implantación de mecanismos de seguridad.

9. SUGERENCIAS DE EVALUACIÓN

La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Evaluación diagnóstica con el fin de conocer la disposición del alumno para aprender y el nivel de los conocimientos previos necesarios para el desarrollo de los nuevos aprendizajes.
- Establecer junto con los alumnos, el porcentaje de las diferentes actividades del curso. Información obtenida durante las investigaciones solicitadas, plasmadas en documentos escritos o digitales
- Participación y desempeño en el aula y laboratorio
- Participación en clase.
- Participación en los talleres.
- Dar seguimiento al desempeño en el desarrollo del temario (dominio de los conceptos, capacidad de la aplicación de los conocimientos en problemas reales y de ingeniería)
- Se recomienda utilizar varias técnicas de evaluación con un criterio específico para cada una de ellas (teórico-práctico).
- Uso de una plataforma educativa en internet la cual puede utilizarse como apoyo para crear el portafolio de evidencias del alumno (integrando: tareas, prácticas, evaluaciones, etc.)
- Presentación y calidad de los ensayos, informes de investigación y trabajos relacionados.
- Participación en las dinámicas grupales.
- Resolución de casos prácticos.
- Conclusiones y resúmenes de estudio.
- Proyecto integrador.
- Exámenes escritos.

10. UNIDADES DE APRENDIZAJE

Unidad 1: Introducción a la seguridad en redes	
Competencia Especifica a Desarrollar	**Actividades de Aprendizaje**
Conoce los conceptos básicos de seguridad, reconociendo la importancia de la misma en las redes de computadoras.	• Investiga diversas definiciones de seguridad y en una sesión plenaria construir una definición que se aplique a las redes de computadoras • Realiza un análisis de los conceptos de vulnerabilidad, amenaza y riesgo, que permita identificar cada uno en un ambiente laboral real.

Unidad 2: Criptografía	
Competencia Especifica a Desarrollar	**Actividades de Aprendizaje**
Desarrolla técnicas de cifrado, algoritmos de criptografía para resguardar la información en las organizaciones.	• Conoce las características de las técnicas de cifrado. • Desarrolla algoritmos de cifrado mediante un lenguaje de programación orientada a objetos.

Unidad 3: Autenticación.	
Competencia Especifica a Desarrollar	**Actividades de Aprendizaje**
Conoce los diferentes tipos de autenticación, comprende las firmas digitales y crea mecanismos de filtrado de paquetes.	• Realiza un análisis de los diferentes tipos de autenticación de redes que existen. • Crea una entidad certificadora. • Compara los diferentes tipos de llaves y firmas digitales. • Configura un firewall en diferentes plataformas operativas. • Implementa una red privada virtual en Windows y Linux.

Unidad 4: Seguridad en servicios de Internet	
Competencia Especifica a Desarrollar	**Actividades de Aprendizaje**
Configurara los principales servicios de Internet e implementa políticas de seguridad	• Configura un servicio de dns y lo asegura mediante políticas de seguridad. • Configura un servicio de web y lo asegura mediante políticas de seguridad.

informática para asegurarlos.	• Configura un servicio de correo electrónico y lo asegura mediante políticas de seguridad.

Unidad 5: Aplicaciones Multimedia	
Competencia Especifica a Desarrollar	**Actividades de Aprendizaje**
Crea esquemas de seguridad y los integra con aplicaciones tipo web	• Crea aplicaciones tipo web y los integra con esquemas de directorio activo.

11. FUENTES DE INFORMACIÓN

1. Academia Latino Americana de Seguridad Informática. www.microsoft.com/alsi
2. Bragg, R. Designing Security for a Microsoft Windows Server 2003 Network. Microsoft Press. Redmon, WA
3. Carballar, J. (2005) Wi-Fi Cómo Construir una Red Inalámbrica. México D.F.
4. Merike, K. Diseño de Seguridad en Redes. Prentice Hall
5. Millar, S. (2004) Seguridad en Wi Fi. McGraw-Hill. Madrid, España
6. Roldán, D. (2005) Comunicaciones Inalámbricas. Alfa Omega.
7. Stallings, W. Fundamentos de Seguridad en Redes: Aplicaciones y Estándares. Prentice Hall.
8. Sugano, A. Solución de Problemas en Redes. Anaya Multimedia-Anaya Interactiva
9. Tanenbaum, A. (2003) Redes de Computadoras. Editorial Pearson. México
10. Seguridad Unix Manuel Mediavilla Alfa omega RA-MA
11. Linux Máxima Seguridad Anónimo Prentice Hall
12. Ariel Maiorano, c2009, Criptografía: técnicas de desarrollo para profesionales. Ed Alafaomega.

12. PRACTICAS PROPUESTAS

- Instalación, configuración e implementación de un sistema operativo de red en forma segura.
- Crear una entidad certificada, llaves públicas y privadas.
- Desarrollar una arquitectura de red segura tres capas.
- Analizar y correr el algoritmo de cifrado DES en un lenguaje de programación orientado a objetos.
- Construir un algoritmo basado en RC4.
- Habilitar servicios de web, DNS, correo electrónico, gestores de bases de datos a través de canales seguros.