

1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad informática
Clave de la asignatura:	RDD 1905
SATCA ¹ :	2-3-5
Carrera:	Ingeniería en Sistemas Computacionales

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 guíe al estudiante en la construcción de su conocimiento.

¹ Sistema de Asignación y Transferencia de Créditos Académicos

En el primer tema se abordan aspectos de la seguridad informática, el valor de la información y posibles riesgos a los que esta expuesta 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 programan los algoritmos utilizando un lenguaje de programación orientado a objetos.

El tema tres presenta la autenticación 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 autenticación 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 familiares 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. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones (Cambios y justificación)
Instituto Tecnológico de la Zona Olmeca	Academia de Ingeniería en sistemas computacionales.	Reunión de la academia de Ingeniería en Sistemas Computacionales

y

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
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.

5. Competencias previas

<p>Conocimiento de:</p> <ul style="list-style-type: none"> Modelo de Referencia OSI. Configuración básica de redes. Desarrollo de aplicaciones web. Manejo de lenguajes de programación orientada a objetos.
--



6. Temario

Unidad	Temas	Subtemas
1	Introducción a la seguridad en Redes	1.1 Definición y 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
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 clavesecreta. 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

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



7. Actividades de aprendizaje de los temas

Unidad 1: Introducción a la seguridad en redes	
Competencias	Actividades de aprendizaje
<p>Competencia específica: Conoce los conceptos básicos de seguridad, reconociendo la importancia de las redes computadoras.</p>	<p>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..</p>
Unidad 2: Criptografía	
Competencias	Actividades de aprendizaje
<p>Competencia específica: Desarrolla técnicas de cifrado, algoritmos de criptografía para resguardar la información en las organizaciones.</p>	<p>Conoce las características de las técnicas de cifrado. Desarrolla algoritmos de cifrado mediante un lenguaje de programación orientada a objetos.</p>
Unidad 3: Autenticación	
Competencias	Actividades de aprendizaje
<p>Competencia específica: Conoce los diferentes tipos de autenticación, comprende las firmas digitales y mecanismos de filtrado de paquetes.</p>	<p>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.</p>

Unidad 4: Seguridad en servicios de Internet	
Competencias	Actividades de aprendizaje
Competencia específica: Configurar los principales servicios de Internet e implementar políticas de seguridad informática para asegurarlos.	Configura un servicio de dns y lo asegura mediante políticas de seguridad. Configura un servicio de web y lo asegura mediante políticas de seguridad. Configura un servicio de correo electrónico y lo asegura mediante políticas de seguridad.
Unidad 5: Autenticación de aplicaciones	
Competencias	Actividades de aprendizaje
Competencia específica: Crea esquemas de seguridad y los integra con aplicaciones tipo web	Crea aplicaciones tipo web y los integra con esquemas de directorio activo

8. Práctica(s)

- 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.
- Crear esquemas lógicos que controlen los objetivos de una organización.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las

siguientes fases:

- ✓ **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- ✓ **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- ✓ **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y específicas a desarrollar.
- ✓ **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Mapas conceptuales, reportes de prácticas, estudios de casos, exposiciones en clase, ensayos, problemarios, reportes de visitas, portafolio de evidencias y cuestionarios.

Listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación.

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 Alfaomega RA-MA
11. Linux Máxima Seguridad Anónimo Prentice Hall
12. Ariel Maiorano, c2009, Criptografía: técnicas de desarrollo para profesionales. Ed Alfaomega