1.- Datos de la asignatura

Nombre de la asignatura:	Seguridad en Tecnologías de la Información y Comunicaciones
Clave de la asignatura:	2-2-4
(Créditos) SATCA	TRC-1705
Carrera:	Ingeniería en Sistemas Computacionales.

2.- Presentación

La asignatura seguridad en tecnologías de la información aporta al perfil del egresado los conceptos más importantes, una fundamentación metodológica y de las herramientas tecnológicas para que el estudiante tenga elementos para establecer un sistema de seguridad que contemple aspectos de evaluación, prevención, detección, reacción y recuperación para proteger de manera sistémica los activos que tienen valor para las organizaciones.
El alumno conocerá y desarrollará, políticas, puntos de control, evaluaciones de seguridad y monitoreo de los distintos elementos que conforman la arquitectura de la seguridad para las organizaciones.

Se organiza el temario en cinco unidades agrupadas en contenidos conceptuales y aspectos prácticos relacionados con el diseño de sistemas seguros los cuales le permitirán al estudiante solucionar problemas de implementación modelos de transporte y almacenamiento de datos altamente confidenciales dentro de una organización.

La primera unidad aborda la fundamentación teórica sobre la cultura de la seguridad en la sociedad y en las organizaciones así como también se analiza los peligros presentes en las redes sociales.

La segunda unidad analiza la propuesta de seguridad por parte de la organización ISO y su correcta implementación.

La unidad número tres aborda los temas de criptografía simétrica y asimétrica y propone una serie de prácticas demostrativas.

La cuarta unidad propone la implementación de usa serie de escenarios experimentales con diversas tecnologías de protección en redes WAN-IP.

La quinta unidad aborda el estudio e implementación de sistemas seguros en instalaciones de centros de datos dentro de las organizaciones.

Intención didáctica
El docente debe ser conocedor de la disciplina que está bajo su responsabilidad, conocer su origen y desarrollo histórico para considerar este conocimiento al abordar los temas.
Desarrollar la capacidad para coordinar y trabajar en equipo; orientar el trabajo del estudiante y potenciar en él la autonomía, el trabajo cooperativo y la toma de decisiones.
Mostrar flexibilidad en el seguimiento del proceso formativo y propiciar la interacción entre los estudiantes. Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.

- Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes.

Ejemplo: buscar, identificar y seleccionar información de fuentes diversas, como las bases de datos: EBSCO, GALE-CENGAGE, THOMSON-REUTERS e IEEEXPLORE, entre otras.

- Fomentar actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración de y entre los estudiantes. Ejemplo: Realizar y documentar las prácticas elaboradas dentro y fuera de clase.
- Observar y analizar fenómenos y problemáticas propias del campo de aplicación. Ejemplos: Atender requerimientos de una propuesta tecnológica sugerida.
- Relacionar los contenidos de esta asignatura con las demás del plan de estudios, a las que ésta da soporte, para desarrollar una visión interdisciplinaria en el estudiante. Ejemplos: identificar y sugerir características específicas de hardware en aplicaciones de sistemas de redes, plataformas operativas, etc.
- Propiciar el desarrollo de capacidades intelectuales relacionadas con la lectura, la escritura y la expresión oral. Ejemplos: trabajar las actividades prácticas a través de guías escritas, redactar informes de las prácticas y exponer los resultados y conclusiones obtenidas frente al grupo.
- Facilitar el contacto directo con materiales, herramientas e instrumentos, al llevar a cabo actividades prácticas, para contribuir a la formación de las competencias para el trabajo experimental, como identificación, manejo de componentes y trabajo en equipo.
- Propiciar el desarrollo de actividades intelectuales de inducción-deducción y análisis-síntesis, que encaminen hacia la investigación.
- Desarrollar actividades de aprendizaje que propicien la aplicación de los conceptos, modelos y metodologías que se van aprendiendo en el desarrollo de la asignatura.
- Proponer problemas que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución.
- Cuando los temas lo requieran, utilizar medios audiovisuales para una mejor comprensión del estudiante.
- Estimular el uso de simuladores de software para una mejor comprensión de los temas.

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 Acapulco. Mayo 2016.	Dr. Eduardo de la Cruz Gámez. Ing. Oscar Arzeta Armenta. M.T.I. Jorge Carranza Gómez. M.A. Eduardo Peralta Martiñon.	Se realizó una evaluación de la pertinencia de la materia a la vista de las líneas de investigación del departamento académico; Se revisó nueva bibliografía para actualizar el temario de la misma.

4.- competencias a desarrollar

Competencias específicas:	Competencias genéricas
• Elegir herramientas de seguridad para la evaluación y monitoreo de redes de computadoras. • Reportar de manera efectiva los resultados del sistema de seguridad. • Conocer los pasos principales para la administración de seguridad de tecnologías de información.	**1.- Competencias instrumentales:** • Capacidades cognitivas. • Capacidad metodológica para manipular el ambiente. • Destrezas tecnológicas relacionadas con el uso y manejo de equipo de cómputo, así como de búsqueda y manejo de información. • Destrezas lingüística tales como la comunicación oral y escrita. **2.- Competencias interpersonales** • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Capacidad de trabajar en equipo • Interdisciplinario. • Capacidad de comunicarse con profesionales de otras áreas. • Habilidad para trabajar en un ambiente laboral. • Compromiso ético. **3.- Competencias sistémicas:** • Identificar los requisitos de seguridad de las organizaciones. • Aplicar diferentes herramientas para

	prevenir, monitorear, y evaluar la tecnología de información de la organización.

5. Competencias previas

- Sabe analizar, diseñar e implantar redes de computadoras.
- Sistemas operativos de red.
- Introducción a las Ciencias Computacionales
- Teoría de la computación
- Organización de Computadoras

6. Temario

Unidad	Temas	Subtemas
1	INTRODUCCIÓN	1.1. Definición de seguridad en cómputo 1.2. Historia de la seguridad 1.3. Modelos de seguridad 1.4. Conceptos de seguridad 1.5. Niveles de seguridad 1.6. Cultura de la seguridad 1.7. Casos de Estudio 1.7.1 Incidencias. 1.7.2 Ataques y Vulnerabilidades
2	GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. ESTÁNDAR ISO/IEC 27002.	2.1. Introducción al estándar ISO/IEC 27002 2.2. Evaluación de Riesgos. 2.3. Requerimientos de seguridad. 2.4. Políticas de seguridad. 2.5. Organización de la seguridad. 2.6. Gestión de Activos.
3	CRIPTOGRAFIA	3.1 Criptografía 3.1.1 Clave Privada (simétrica) 3.1.2 Clave Pública (asimétrica) 3.1.3 Firmas digitales 3.2 Cuentas y contraseñas 3.3 Controles de acceso 3.4 Protección a Sistemas de Archivos
4	SEGURIDAD EN RED	4.1 Protocolos de comunicación 4.2 La seguridad en Internet 4.2.1 Metasploit 4.2.1 Firewalls 4.3 SSL/TSL 4.4 Autenticación
5	SEGURIDAD FISICA	5.1 Protección del equipo de cómputo 5.1.1 Protección física

		5.1.2 El área de trabajo 5.2 Protección de datos 5.2.1 Sistemas redundantes de respaldo de datos 5.3 Sistemas redundantes de Energía 5.3.1 Líneas eléctricas 5.3.2 No-break

7. Actividades de aprendizaje de los temas

Introducción	
Competencias	Actividades de aprendizaje
Específica(s): Identificar la importancia de la cultura de seguridad como herramienta de prevención. Genéricas: **Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organización y planificación • Comunicación oral y escrita en su propia lengua • Capacidad de gestión de la información (habilidad para buscar y analizar información proveniente de fuentes diversas) **Competencias interpersonales:** • Razonamiento critico • Trabajo en equipo • Habilidades en las relaciones Interpersonales • Compromiso ético	Analizar la necesidad de establecer la cultura de la seguridad informática en un centro de cómputo. Analizar casos de estudio acerca de violaciones a la seguridad informática. Elaborar reportes de las investigaciones realizadas.
Gestión de la Seguridad de la Información.	
Competencias	Actividades de aprendizaje
Específica(s): Identificar los elementos clave de la gestión de la seguridad para su correcta implementación. Genéricas: **Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organización y planificación • Comunicación oral y escrita en su propia lengua	Investigar sobre políticas de seguridad implementadas en las organizaciones Discutir sobre el diseño de buenas prácticas de seguridad implementadas. Investigar y exponer los resultados obtenidos acerca de las implicaciones legales de violaciones a las políticas de seguridad.

• Capacidad de gestión de la información (habilidad para buscar y analizar información proveniente de fuentes diversas) **Competencias interpersonales:** • Razonamiento critico • Trabajo en equipo • Habilidades en las relaciones Interpersonales • Compromiso ético	

Criptografía

Competencias	Actividades de aprendizaje
Específica(s): Analizar los conceptos acerca de la criptografía para proporcionar un sistema seguro. Genéricas: **Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organización y planificación • Comunicación oral y escrita en su propia lengua • Capacidad de gestión de la información (habilidad para buscar y analizar información proveniente de fuentes diversas) **Competencias interpersonales:** • Razonamiento critico • Trabajo en equipo • Habilidades en las relaciones Interpersonales • Compromiso ético	Identificar los métodos modernos de encriptación de datos. Describir el uso de la autentificación mediante cuentas y contraseñas. Analizar diversas técnicas de monitoreo básico de la seguridad. Diseñar una serie de práctica acerca del uso de: RC4, Firmas digitales, encriptación de cuentas. Exponer los modelos prácticos argumentando los resultados obtenidos.

Seguridad en la Red

Competencias	Actividades de aprendizaje
Específica(s): Analizar los elementos básicos para proporcionar un sistema seguro en redes IP. Genéricas: **Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organización y	Identificar las variantes existentes para proporcionar mecanismos de seguridad en la red IP. Analizar los diversos algoritmos de seguridad para autenticación en redes WAN.

planificación • Comunicación oral y escrita en su propia lengua • Capacidad de gestión de la información (habilidad para buscar y analizar información proveniente de fuentes diversas) **Competencias interpersonales:** • Razonamiento critico • Trabajo en equipo • Habilidades en las relaciones Interpersonales • Compromiso ético	Diseñar una serie de prácticas acerca de las siguientes tecnologías: Intrusión remota, VPN, Firewall, SSL. Exponer los modelos prácticos argumentando los resultados obtenidos.
Seguridad Física	
Competencias	Actividades de aprendizaje
Específica(s): Analizar los elementos básicos de la seguridad física de los equipos de cómputo para su correcta implementación. Genéricas: **Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organización y planificación • Comunicación oral y escrita en su propia lengua • Capacidad de gestión de la información (habilidad para buscar y analizar información proveniente de fuentes diversas) **Competencias interpersonales:** • Razonamiento critico • Trabajo en equipo • Habilidades en las relaciones Interpersonales • Compromiso ético	Identificar las diversas técnicas existentes para proporcionar seguridad a un centro de cómputo. Analizar de las tecnologías existentes para proporcionar sistemas redundantes para la protección de centros de datos. Identificar las diversas variantes de sistemas redundantes de respaldo de energía eléctrica.

8. Práctica(s)

Unidad I 1. Ataque de ingeniería social Unidad III 1. Máquina Enigma

2. Criptoanálisis por Kasiski
3. Certificados Digitales
4. Ataque al protocolo WEP
5. Ataque al protocolo WPA2
6. Uso de la herramienta PGP
7. Ataque por fuerza bruta

Unidad IV

1. Ataque remoto usando Metaesploit
2. Implementación de un Firewall con IPTables
3. Implementación del protocolo SSL/TSL
4. Implementación de una conexión VPN (IPSec)

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 especificas 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

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

- Reportes escritos de las prácticas realizadas durante clase y las actividades inherentes, así como de las conclusiones obtenidas.
- Análisis de la información obtenida durante las investigaciones solicitadas plasmada en documentos escritos.
- Descripción de otras experiencias concretas que podrían realizarse adicionalmente.

- Exámenes escritos para comprobar el manejo de aspectos teóricos y declarativos.
- Presentación y exposición de cada actividad de aprendizaje. Algunas se evaluarán por equipos.
- La evaluación debe incluir todas las actividades realizadas durante el curso, como: asistencia y participación en clase, reportes de investigación documental, informes de prácticas y resultados de exámenes escritos, entre otras.

11. Fuentes de información

1. ISO/IEC 17799. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. 2da. Edición. 2005.
2. Cunningham, Dykstra, Fuller, Gatford, Gold,..Best Damn IT Security Management Book Period. Syngres. 2007
3. Anderson. Ross. Security Engineering.Second edition.Wiley. 2008. Capítulo 25.
4. Jackson. Chris. Network Security Auditing. Cisco Press.2010.
5. Redes de Computadoras. Andrew S. Tanenbaum. Ed. Pearson/Prentice Hall. Cuarta Edición. 2003
6. Auditoria Informática, un enfoque práctico. Mario G. Piattinni. Emilio del Peso. Segunda Edición. Alfaomega, RA-MA. 2001.
7. Seguridad en Microsoft Windows 2000. Jeff Schmidt. Ed. Prentice Hall. 2001.
8. CERT UNAM - Equipo de Respuesta a Incidentes de Seguridad en Cómputo. http://www.seguridad.unam.mex.
9. Hacking y Seguridad en Internet, Fernando Picouto, Alfaomega Ra-Ma. 2008.
10. Superutilidades Hackers. Keith J. Jones y otros. Mc Graw Hill.