1. Datos Generales de la asignatura

Nombre de la asignatura:	**Seguridad en Tecnologías de la Información**
Clave de la asignatura:	**ISB-1803**
SATCA:	**1-4-5**
Carrera	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

Esta materia forma parte de la especialidad y para poder cursarla, requiere la aprobación de materias como Fundamentos de Telecomunicaciones, Arquitecturas de Computadoras, Redes de Computadoras, que le darán el sustento para aprobar de manera satisfactoria la materia.

Aportando al perfil del Ingeniero en Sistemas Computacionales, los elementos necesarios para diseñar, desarrollar e implementar aplicaciones de seguridad basadas en las distintas plataformas y/o protocolos.

Intención didáctica

Se organiza el temario, en cuatro unidades, en la unidad uno: “Seguridad WAN”, se introducirá al estudiante en el contexto y los conceptos relacionados con la seguridad y amenazas de las redes WAN; haciendo uso de firewalls como herramientas de seguridad, servirá como un ejemplo y ejercicio introductorio a este importante aspecto de seguridad perimetral, incluyendo una revisión de los diferentes tipos de firewall, las ventajas que ofrece, sus limitaciones, las políticas de uso y configuración de un firewall, así como el tratamiento de los enlaces externos y la creación de lo que se denomina como una zona desmilitarizada (DMZ, por sus siglas en inglés) e implementar sistemas de firewall para contrarrestar los ataques a estas redes.

En la unidad dos: “Seguridad LAN”, identificará los diferentes tipos de ataques a la red local, e implementar políticas de seguridad para anular estos ataques y hacer uso de sistemas criptográficos, también analizar la aplicación de los sistemas firewall vistas en la unidad uno.

En la unidad tres: “Seguridad en Cómputo en la Nube y en la Niebla”, analizara los diferentes tipos de arquitecturas de seguridad en la nube y en la niebla, para garantizar la transmisión de los datos y analizar los diferentes tipos de vulnerabilidades que existen en las redes con aplicaciones en la nube y en la niebla.

En la unidad cuatro: “Certificados y firmas digitales”, es otra unidad básicamente conceptual, más que aplicada, (salvo al final), pero que permitirá tener una idea de la aplicación y complejidad en ésta que tienen los certificados y las firmas digitales. E inicia esta unidad con el concepto de la distribución de claves, de a qué se refiere la certificación, los componentes de una PKI (infraestructura de clave pública) y las diferentes arquitecturas PKI actualmente en uso, las características y diferencias entre las políticas y las prácticas de certificación, la comprensión de lo que implica la gestión de una PKI, así como el conocimiento de los estándares y protocolos de certificación vigentes. Al final,

se sugiere una práctica integradora con un generador de certificados gratuito, en línea y libre, como puede ser OpenCA, que sirva de referencia didáctica y en la cual se puedan ver ejemplificados los conceptos manejados a lo largo de la unidad.

El enfoque sugerido para la materia requiere que las actividades prácticas promuevan el desarrollo de habilidades para la experimentación, tales como: identificación, manejo y control de herramientas de desarrollo de software, lenguajes de programación, herramientas de software especializado para seguridad en redes; planteamiento de problemas y programación de algoritmos; 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 a cabo y entienda que está construyendo su 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, la curiosidad, la puntualidad, el entusiasmo, 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
Instituto Tecnológico de Aguascalientes, 8 de abril del 2016.	**Academia de Sistemas y Computación** (L.I. Mario Alberto Vargas Moreno, L.I. Gloria Leticia Betts Gómez, L.I. Jorge Humberto Dzul Bermejo, M.A. René Tristán Ávila, L.I. Miguel Ortiz Martínez, L.I. Miriam Malo Torres, L.I. Arturo López Ponce, Héctor de Jesús Carlos Pérez, MC. Javier Pantoja Mascorro, MC. Héctor Macías Figueroa, Ing. Rosendo Ramiro Sánchez, Dr. Marco Antonio Hernández Vargas, MSC. Luis Antonio Macías Cruz, Dr. Francisco Javier Luna Rosas).	Comisión para la elaboración de los planes y programas de estudio para la especialidad de la Carrera de Ingeniería en Sistemas Computacionales.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Hacer uso de las herramientas de software y hardware, para contribuir a mejorar los niveles de seguridad en la nube y en la niebla

5. Competencias previas

Conocimiento en el manejo y funcionalidad de los sistemas de información (bases de datos), redes de computadores, software base (sistemas operativos, lenguajes de programación).

6. Temario

No.	Temas	Subtemas
1.	Seguridad WAN	1.1. Amenazas modernas en la Seguridad de la red 1.2. Dispositivos de seguridad de red 1.3. Implementación de Tecnologías de Firewall 1.4. Implementación de Prevención de Infiltración

2.	Seguridad LAN	2.1. La seguridad en la red Local 2.2. Sistemas de Criptografía 2.3. Administrando la seguridad en la red
3.	Seguridad en cómputo en la nube y en la niebla	3.1. Arquitectura de seguridad en los diferentes tipos de nube. 3.2. Seguridad de Datos en la nube y en la niebla 3.3. Arquitectura de seguridad en cómputo en la niebla. 3.4. Desafíos de la seguridad en cómputo en la nube y en la niebla. 3.5. Vulnerabilidades en la nube y en la niebla 3.6. Protección en la nube y en la niebla
4.	Certificados y firmas digitales	4.1. Distribución de claves. 4.2. Certificación. 4.3. Componentes de una PKI. 4.4. Arquitecturas PKI. 4.5. Políticas y prácticas de certificación. 4.6. Gestión de una PKI. 4.7. Estándares y protocolos de certificación. 4.8. Ejemplo de un protocolo de seguridad: HTTPS. 4.9. SSL, TSL, SSH. 4.10. Prueba con un generador de certificados gratuitos, libre y en línea.

7. Actividades de aprendizaje de los temas

Unidad 1 Seguridad WAN	
Competencias	**Actividades de aprendizaje**
Específica(s): ➢ Crear conciencia y proteger la información de una empresa a través del reconocimiento de las debilidades inherentes de las tecnologías WAN aplicadas a una red de computadoras **Genéricas:** <u>Competencias instrumentales</u> ➢ Capacidad de análisis y síntesis. ➢ Capacidad de organizar y planificar. ➢ Conocimientos básicos de la carrera. ➢ Comunicación oral y escrita. ➢ Habilidades de manejo de la computadora. ➢ Habilidad para buscar y analizar información proveniente de fuentes diversas. ➢ Solución de problemas. ➢ Toma de decisiones. <u>Competencias interpersonales</u> ➢ Capacidad crítica y autocrítica. ➢ Trabajo en equipo. ➢ Habilidades interpersonales. <u>Competencias sistémicas</u> ➢ 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. ➢ Búsqueda del logro.	➢ Investigar y discutir en un debate los aspectos de seguridad generales de las comunicaciones. ➢ Conocer cómo se da el control de acceso a los medios. ➢ Investigar, distinguir e identificar las debilidades inherentes a los protocolos de enrutamiento y demás relacionados con las redes, haciendo una comparación entre ellos. ➢ Investigar los diferentes estándares existentes en el ámbito de la seguridad en redes WAN, analizando sus características, ventajas y desventajas y diseñar un escenario de aplicación ➢ Analizar de las diversas vulnerabilidades que pueden presentar las redes WAN ➢ Investigar, discutir y conocer los diferentes tipos de dispositivos y formas de seguridad de red WAN que existen en el mercado. ➢ Diseñar e implementar un sistema de prevención y seguridad en una red WAN

Unidad 2 Seguridad LAN	
Competencias	**Actividades de aprendizaje**
Específica(s): ➢ Crear conciencia y proteger la información de una empresa a través del reconocimiento de las debilidades inherentes de las tecnologías LAN aplicadas a una red de computadoras **Genéricas:** <u>Competencias instrumentales</u> ➢ Capacidad de análisis y síntesis. ➢ Capacidad de organizar y planificar. ➢ Conocimientos básicos de la carrera. ➢ Comunicación oral y escrita. ➢ Habilidades de manejo de la computadora. ➢ Habilidad para buscar y analizar información proveniente de fuentes diversas. ➢ Solución de problemas. ➢ Toma de decisiones. <u>Competencias interpersonales</u> ➢ Capacidad crítica y autocrítica. ➢ Trabajo en equipo. ➢ Habilidades interpersonales. <u>Competencias sistémicas</u> ➢ 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. ➢ Búsqueda del logro.	➢ Investigar y discutir en un debate los aspectos de seguridad generales de las comunicaciones. ➢ Conocer cómo se da el control de acceso a los medios. ➢ Investigar, distinguir e identificar las debilidades inherentes a los protocolos de enrutamiento y demás relacionados con las redes, haciendo una comparación entre ellos. ➢ Investigar los diferentes estándares existentes en el ámbito de la seguridad en redes LAN, analizando sus características, ventajas y desventajas y diseñar un escenario de aplicación ➢ Analizar de las diversas vulnerabilidades que pueden presentar las redes LAN ➢ Investigar, discutir y conocer los diferentes tipos de dispositivos y formas de seguridad de red LAN que existen en el mercado. ➢ Diseñar e implementar un sistema de prevención y seguridad en una red LAN

Unidad 3 **Seguridad en cómputo en la nube y en la niebla**	
Competencias	**Actividades de aprendizaje**
Específica(s): ➢ Conocer las vulnerabilidades y generar un sistema de protección de datos en la nube y en la niebla. **Genéricas:** <u>Competencias instrumentales</u> ➢ Capacidad de análisis y síntesis. ➢ Capacidad de organizar y planificar. ➢ Conocimientos básicos de la carrera. ➢ Comunicación oral y escrita. ➢ Habilidades de manejo de la computadora. ➢ Habilidad para buscar y analizar información proveniente de fuentes diversas. ➢ Solución de problemas. ➢ Toma de decisiones. <u>Competencias interpersonales</u> ➢ Capacidad crítica y autocrítica. ➢ Trabajo en equipo. ➢ Habilidades interpersonales. <u>Competencias sistémicas</u> ➢ 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. ➢ Búsqueda del logro.	➢ Investigar y discutir en un debate los aspectos de seguridad generales y particulares de los tipos de nube. ➢ Conocer los diferentes tipos de seguridad de datos aplicados a la nube y a la niebla. ➢ Investigar las arquitecturas de seguridad en cómputo aplicados a la nube ➢ Analizar y discutir los desafíos de seguridad que se presentan tanto en la nube como en la niebla ➢ Analizar las vulnerabilidades en la nube y en la niebla, realizando un foro de discusión sobre las formas o políticas para solventarlas. ➢ Diseñar e implementar un sistema de prevención y seguridad en nube y en la niebla

Unidad 4 Certificados y firmas digitales	
Competencias	**Actividades de aprendizaje**
Específica(s): ➢ Crear un certificado digital, con el fin de proteger la información de una entidad al momento de hacer transacciones en la web de una manera segura. **Genéricas:** <u>Competencias instrumentales</u> ➢ Capacidad de análisis y síntesis. ➢ Capacidad de organizar y planificar. ➢ Conocimientos básicos de la carrera. ➢ Comunicación oral y escrita. ➢ Habilidades de manejo de la computadora. ➢ Habilidad para buscar y analizar información proveniente de fuentes diversas. ➢ Solución de problemas. ➢ Toma de decisiones. <u>Competencias interpersonales</u> ➢ Capacidad crítica y autocrítica. ➢ Trabajo en equipo. ➢ Habilidades interpersonales. <u>Competencias sistémicas</u> ➢ 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. ➢ Búsqueda del logro.	➢ Investigar el funcionamiento de la distribución de claves, tanto en métodos simétricos (haciendo referencia a los algoritmos vistos en la unidad anterior), como asimétricos. ➢ Por lluvia de ideas, derivar el concepto de certificado y extrapolarlo al ámbito digital. ➢ Investigar el concepto de certificado digital y elaborar con ello un mapa conceptual, el cual intercambiará con sus demás compañeros. ➢ Investigar el proceso de certificación, identificando las partes involucradas, sus funciones, los requerimientos, etc. ➢ Elaborar un diagrama en el que se reflejen todos estos pasos o llevar al cabo un sociodrama en el que se refleje este procedimiento. ➢ Identificar los componentes de una infraestructura de clave pública, sus funciones y sus responsabilidades. ➢ Investigar las diferentes arquitecturas de una PKI, haciendo una comparación entre ellas, y analizando sus ventajas y desventajas, fortalezas y debilidades, así como el establecimiento de posibles escenarios de uso. ➢ Investigar los conceptos de prácticas y políticas de certificación, identificando su diferencia. ➢ Investigar el proceso de gestión de una PKI, identificando las partes involucradas, sus funciones y sus responsabilidades. ➢ Elaborar un diagrama en el cual se describa este proceso. Investigar y ejemplificar los estándares y protocolos existentes para el proceso de certificación, sus características, si están vigentes y

	en uso actualmente o no, funcionamiento, etc. ➢ Realizar una práctica de creación de certificado utilizando una herramienta gratuita y en línea, como es OpenCA.

8. Práctica(s)

- Instalación y administración de un sistema de cortafuegos:
- Firewall por hardware
- Firewalls por software
- Instalación de un servidor headless.
- Creación de un Servidor Proxy en diversas plataformas
- Uso de herramientas de monitoreo de red.
- Uso de IPSEC
- Llevar al cabo la elaboración de un certificado digital utilizando alguna herramienta gratuita y en línea, como puede ser OpenCA.
- Implementar una arquitectura de seguridad para la Nube y la Niebla
- Análisis de las vulnerabilidades de la Nube y la Niebla

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:

- Presentación de reportes de búsqueda de información en fuentes bibliográficas o digitales de reconocido valor, las cuales deben ir indicadas por el instructor.
- Participación en actividades para demostrar el entendimiento y comprensión de los conocimientos adquiridos a través de las investigaciones anteriores, tales como la elaboración de mesas panel, etc.
- Elaboración de proyectos de aplicación donde se incluyan e integren los algoritmos vistos en clase y programados fuera de ellos.
- Entrega de los algoritmos programados.
- Examen escrito donde se pueda comprobar el manejo de conocimientos teóricos y declarativos.
- Reportes escritos de las observaciones hechas durante las actividades, así como de las conclusiones obtenidas de dichas observaciones.
- Elaboración de manuales de instalación y configuración de las diferentes tecnologías abarcadas en el presente programa.

11. Fuentes de información

- Aguirre, Jorge R. "Aplicaciones Criptográficas." Segunda edición. Junio, 1999. Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España. ISBN 83-87238-57-2.
- Zimmermann, P. "An Introduction to Cryptograpy". Network Associates. 1999, available at: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf.
- Zimmermann, Philip R. "Cryptography for the Internet." Scientific American. October, 1998.
- Diffie, Whitfield; Landau, Susan Eva. "Privacy on the Line." MIT Press. ISBN: 0262041677.
- Biham, Eli; Shamir, Adi. "Differential Cryptanalysis of the Data Encryption Standard." Springer-Verlag. ISBN: 0-387-97930-1 A .
- Kaufman, Charlie; Perlman, Radia; Spencer, Mike. "Network Security: Private Communication in a Public World". Prentice Hall. ISBN: 0-13-061466-1. ➢ Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C." John Wiley & Sons. ISBN: 0-471-12845-7.
- Smith, Richard E. "Internet Cryptography." Addison-Wesley Pub Co. ISBN: 0201924803.

- Cheswick, William R.; Bellovin, Steven M. “Firewalls and Internet Security: Repelling the Wily Hacker.” Addison-Wesley Pub Co. ISBN: 0201633574.
- Cano-Barrón, José E.; Martínez-Peláez, Rafael; Soriano, Miquel. “Current Problems and Challenges in Developing a Standard Digital Rights Management System”. 5th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods (incorporating the 3rd International ODRL Workshop). Oct. 11 – 13, 2007. Koblenz, Alemania.
- Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. “Handbook of applied cryptography”. ISBN: 0-8493-8523-7. Oct., 1996.
- Koblitz, Neal. “A Course in Number Theory and Cryptography”. Springer-Verlag. ISBN: 0-387-94293-9.
- Aguirre, Jorge R. “Libro Electrónico de Seguridad Informática y Criptografía”. ISBN 84-86451-69-8 (2006); Depósito Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm.
- Lucena López, Manuel J. “Criptografía y Seguridad en Computadores”. Cuarta Edición. Versión 0.7.8. 9 de octubre de 2007. Criptografía y Seguridad en Computadores es un libro electrónico en castellano, publicado bajo licencia Creative Commons.
- Khan, David. “The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet”. Revised and Updated. Scribner. 1996. ISBN: 0684831309.
- Schneier, Bruce. “Applied Cryptography”. Second Edition. John Wiley & Sons, 1996. ISBN 0-471-11709-9.