1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad Informática
Clave de la asignatura:	IAD-1305
Créditos (Ht-Hp_ créditos):	2-3-5
Carrera:	Ingeniería en Tecnologías de la Información y Comunicaciones

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Tecnologías de la Información y Comunicaciones 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 la primera unidad, se abordan aspectos introductorios al curso, los cuales incluyen una breve introducción a la seguridad informática, el valor de la información, así como definiciones y los tipos de seguridad informática que se pueden dar, sus objetivos, incluyendo los posibles riesgos y técnicas de aseguramiento del sistema. Al estudiar cada parte, se incluyen los conceptos involucrados con ella para hacer un tratamiento más significativo, oportuno e integrado de dichos conceptos, haciendo una énfasis muy especial en la utilidad que tendrá para más adelante, tanto del desarrollo de la asignatura como de la carrera en general. Todos los apartados, en conjunto, servirán para fundamentar una visión general de la importancia que tiene y ha adquirido la seguridad en ámbitos informáticos.

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.

La siguiente unidad se refiere a un estudio introductorio a la seguridad en redes, considerando aspectos de la seguridad en las comunicaciones, analizando las debilidades de los protocolos TCP/IP, revisando los estándares existentes para la seguridad en redes, así como haciendo un estudio sobre la seguridad en redes inalámbricas, tan de moda actualmente. Cabe recordar que estos aspectos serán tratados más a profundidad en materias posteriores.

El temario culmina con algunos aspectos introductorios a la vigilancia de los sistemas de información, iniciando con la definición de vigilancia, la anatomía de un ataque (haciendo referencia y ejemplificando los conceptos vistos en las primeras unidades), a qué se refiere el escaneo, la identificación de vulnerabilidades, algunas posibles actividades de infiltración, la consolidación y terminará con una referencia más a fondo de la defensa perimetral y su importancia.

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

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Ciudad Hidalgo, Michoacán, Octubre 2013.	Academia de la carrera de Ingeniería en Tecnologías de la Información y Comunicaciones	Análisis y enriquecimiento de los programas por competencias generados en reuniones nacionales en el 2012.

4. Competencias a desarrollar

Competencia general 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.

Competencias específicas
• 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. • Hacer uso de las herramientas de software para contribuir a mejorar los niveles de seguridad informática en una organización.
Competencias genéricas
• Capacidad de análisis y síntesis. • Conocimiento informático • Desarrollos trabajar en equipos y proyecto multidisciplinarios. • Visión crítica e innovadora de la tecnología actual. • Capacidad para experimentar de una manera sistemática la búsqueda de soluciones adecuadas a la problemática que se le presente. • Capacidad de Aprendizaje individual. • Habilidades de investigación.

5. Competencias previas de otras asignaturas

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

	Subtemas

Temas		
No.	**Nombre**	
1.	Introducción a la seguridad informática	1.1. El valor de la información. 1.2. Definición y tipos de seguridad informática. 1.3. Objetivos de la seguridad informática. 1.4. Posibles riesgos. 1.5. Técnicas de aseguramiento del sistema.
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 redes	4.1. Aspectos de seguridad en las comunicaciones. 4.2. Debilidades de los protocolos TCP/IP. 4.2.1. Transmisión de paquetes y promiscuidad. 4.2.2. Redes locales (VLAN) y amplias (VPN). 4.2.3. Domicilios IP. 4.2.4. Vigilancia de paquetes. 4.3. Estándares para la seguridad en redes. 4.4. Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.
5.	Vigilancia de los sistemas de información	5.1 Definición de vigilancia. 5.2. Anatomía de un ataque. 5.2.1. Identificación de objetivos. 5.2.2. Reconocimiento inicial. 5.2.3. Técnicas de recopilación de información y análisis forense. 5.3. Escaneos. 5.3.1. Identificación y ataques a puertos TCP/UDP. 5.3.2. Identificación y ataques a servicios. 5.4. Identificación de vulnerabilidades. 5.4.1. Técnicas manuales. 5.4.2. Técnicas automáticas. 5.5. Actividades de infiltración. 5.5.1. Sistema operativo. 5.5.2. Aplicaciones. 5.5.3. Bases de datos. 5.6. Consolidación. 5.7. Defensa perimetral. 5.7.1. Creación de una DMZ. 5.7.2. Antivirus. 5.7.3. Nat. 5.7.4. Proxy

7. Actividades de aprendizaje

<table>
<tr><td colspan="2">Competencia específica y genéricas (a desarrollar y fortalecer por tema)</td></tr>
<tr><td colspan="2">Reconocer la importancia y complejidad que implica el concepto de seguridad en el ámbito de la informática y las diferentes áreas en las cuales está inmersa</td></tr>
<tr><td>Tema</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Unidad 1: Introducción a la seguridad informática</td><td>• Elaborar por medio de una lluvia de ideas el significado de seguridad en informática.
• Investigar y discutir cuál es el valor real que se le da a la información en nuestros días.
• Investigar la definición de seguridad en informática en fuentes no confiables y fuentes bien respaldadas. Comparar ambos resultados e identificar diferencias y similitudes.
• Realizar un mapa conceptual con la definición de seguridad informática.
• Investigar los objetivos que persigue la seguridad en el ámbito informático.
• Esquematizar estos objetivos en mapas mentales, conceptuales o cuadros sinópticos.
• Investigar los posibles riesgos a los que se enfrentan las empresas al no tomar en cuenta aspectos de seguridad informática.
• Discutir en una mesa panel estos posibles riesgos.
• Redactar las conclusiones de la mesa panel.
• Investigar y categorizar las diferentes técnicas existentes para el aseguramiento de un sistema.
• Discutir estas técnicas, desde el punto de vista de sus características, ventajas y desventajas, fortalezas y debilidades.
• Investigar posibles escenarios de uso de estas técnicas y ejemplos de aplicación para el cumplimiento de los objetivos de la seguridad en informática.</td></tr>
<tr><td colspan="2">Competencia específica y genéricas (a desarrollar y fortalecer por tema)</td></tr>
<tr><td colspan="2">Conoce los diferentes tipos de autenticación, comprende las firmas digitales y crea mecanismos de filtrado de paquetes</td></tr>
<tr><td>Tema</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Unidad 2: Criptografía</td><td>• Realiza un análisis de los diferentes tipos</td></tr>
</table>

	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.
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Conoce los diferentes tipos de autenticación, comprende las firmas digitales y crea mecanismos de filtrado de paquetes	
Tema	Actividades de aprendizaje
Unidad 3: Autenticación	• 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
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Crear conciencia y proteger la información de una empresa a través del reconocimiento de las debilidades inherentes de las tecnologías aplicadas a una red de computadoras.	
Tema	Actividades de aprendizaje
Unidad 4: Seguridad en redes	• Investigar y discutir en un debate los aspectos de seguridad generales de las comunicaciones. • Analizar el funcionamiento del protocolo TCP/IP. • Conocer como se da el control de acceso a los medios. • Investigar, distinguir e identificar las debilidades inherentes a los protocolos TCP/IP y demás relacionados con las redes, haciendo una comparación entre ellos. • Investigar los diferentes estándares existentes en el ámbito de la seguridad en redes de computadoras, analizando sus

	características, ventajas y desventajas y diseñando escenarios de aplicación. • Transpolar los conocimientos adquiridos anteriormente, para la seguridad en redes inalámbricas, haciendo énfasis en los protocolos WEP, WAP y WPA2. Haciendo una comparación entre estas redes y las basadas en cables. • Conocer y aplicar el funcionamiento de los protocolos que existen en redes y redes inalámbricas y sus diferencias. • Analizar de las diversas vulnerabilidades que pueden presentar las redes wireless.
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
Llevar al cabo una vigilancia e implementar medidas de seguridad efectivas de la información que circula	
Tema	Actividades de aprendizaje
Unidad 5: Vigilancia de los sistemas de información	• Realizar una lluvia de ideas acerca del significado del concepto de vigilancia, extrapolándolo, posteriormente, al ámbito informático. • Investigar los tipos de ataques que se pueden presentar a un sistema de información a través de una red de datos, haciendo una comparación con los tipos de ataques vistos en unidades anteriores, principalmente, en la parte de criptografía. • Identificar sus características, las vulnerabilidades en los sistemas a los cuales atacan, etc. • Investigar cuál es el concepto de escaneo y cuáles tipos hay, a qué va dirigido, de qué herramientas se valen, etc. • Investigar los diferentes métodos de infiltración que se pueden dar, a través de qué, utilizando cuáles herramientas, cómo funcionan dichas herramientas, etc. • Presentar escenarios en los cuales estos ataques se den. • Especificar la manera en que la defensa, a nivel perimetral, protege a los sistemas de información de este tipo de ataques, escenificando o ejemplificando estas situaciones. • Instalar herramientas de monitoreo y análisis de tráfico de una red, explicando su funcionamiento y haciendo referencia a

	los diferentes tipos de ataques y las vulnerabilidades de las que se aprovecha. • Investigar el origen del concepto de zona desmilitarizada (DMZ, por sus siglas en inglés) y su aplicación al ámbito informático. • Creación de una DMZ utilizando herramientas gratuitas.

8. Prácticas (para fortalecer las competencias de los temas y de la asignatura)

- 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 integrador (Para fortalecer las competencias de la asignatura con otras asignaturas)

- Habilitar,configurar y administrar servicios de web, DNS, correo electrónico, gestores de bases de datos a través de canales seguros.

10. Evaluación por competencias (específicas y genéricas de la asignatura)

Instrumentos y herramientas sugeridas para evaluar las actividades de aprendizaje:

- 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.

11. Fuentes de información (actualizadas considerando los lineamientos de la APA*)

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 Alafaomega

* American Psychological Association (*APA*)