1.- DATOS DE LA ASIGNATURA

Nombre de la asignatura:	Seguridad en Aplicaciones Móviles
Carrera:	Ingeniería en Informática
Clave de la asignatura:	ARD-1306
(Créditos) SATCA[1]	2-3-5

2.- PRESENTACIÓN

Caracterización de la asignatura.

La tendencia en el desarrollo de software y el uso de dispositivos móviles presenta un campo que debe aprovecharse, sin descuidar el aspecto de la seguridad que debe ir implícita. Esta asignatura aporta al perfil del egresado la capacidad para desarrollar aplicaciones seguras y su relación con la arquitectura de software y es posterior a la materia de Fundamentos de Arquitectura de Software.

Intención didáctica.

La asignatura cubre la necesidad que tiene el ingeniero al enfrentarse a la forma de intercambiar información a través de sus aplicaciones, los diferentes dispositivos, incluyendo los dispositivos móviles y en particular a la seguridad de las aplicaciones.

El temario está organizado en cinco unidades:
La primera unidad, introduce al estudiante a la seguridad en las redes.
La segunda unidad, el estudiante aplica los diferentes tipos de cifrado y autenticación en las comunicaciones.
La tercera unidad, el estudiante implementará los mecanismos de seguridad necesarios en la comunicación de datos.
La cuarta unidad, el estudiante Implementará los mecanismos de seguridad necesarios en las redes inalámbricas de área local y dispositivos móviles.
La quinta unidad, se le brinda al estudiante una visión general sobre la seguridad de cómputo en la nube.

3.- COMPETENCIAS A DESARROLLAR

Competencias específicas:	**Competencias genéricas**
Identificar la importancia de la seguridad en cómputo móvil. Identificar los mecanismos de seguridad necesarios en las redes de computadoras,. Garantizar la confidencialidad, integridad y disponibilidad de la información que soportan los dispositivos móviles. Configurará los mecanismos de seguridad necesarios en las redes de computadoras. Configurará los mecanismos de seguridad necesarios en las aplicaciones móviles.	**Competencias instrumentales**: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Conocimientos básicos de la carrera. • Comunicación oral y escrita. • Habilidades del manejo de la computadora. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. **Competencias interpersonales**: • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales.

	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.

4.- HISTORIA DEL PROGRAMA

Lugar y fecha de elaboración o revisión	Participantes	Observaciones (cambios y justificación)
Instituto Tecnológico de Hermosillo, del 1 al 8 de Marzo de 2013.	Francisco Gabriel Ibarra Lemas Daniel Pérez Pérez Julio César Flores López	Reunión departamental de Diseño curricular y definición de la Especialidad de la carrera de Ingeniería en Sistemas Computacionales.

5.- OBJETIVO(S) GENERAL(ES) DEL CURSO (competencias específicas a desarrollar en el curso)

- Identificar la importancia de la seguridad en cómputo móvil.
- Identificar los mecanismos de seguridad necesarios en las redes de computadoras.
- Garantizar la confidencialidad, integridad y disponibilidad de la información que soportan los dispositivos móviles.
- Configurará los mecanismos de seguridad necesarios en las redes de computadoras.
- Configurará los mecanismos de seguridad necesarios en las aplicaciones móviles.

6.- COMPETENCIAS PREVIAS.

- Identificar las implicaciones actuales de la programación móvil.
- Identificar las características de los diferentes emuladores para dispositivos móviles.
- Identificar los problemas de comunicación entre sistemas.

7.- 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 Servicios y mecanismos de seguridad

2	Criptografía y Autenticación	2.1. Tipos de cifrado 2.1.1. Cifrado por sustitución. 2.1.2. Cifrado por transposición. 2.2 Principios criptográficos fundamentales. 2.2.1 Redundancia. 2.2.2 Actualización. 2.3. Protocolos de autenticación. 2.3.1. Claves secretas compartidas. 2.3.2. Centros de distribución de claves. 2.3.3. Claves públicas. 2.3.4. Ejemplos de protocolos de autenticación. 2.4. Firmas digitales. 2.4.1. Firmas digitales de clave simétrica. 2.4.2. Firmas digitales de llave pública.
3	Seguridad en la comunicación de datos.	3.1 Cortafuegos (firewalls) 3.1.1 Alcances y limitaciones 3.1.2 Componentes 3.1.3 Filtros de paquetes 3.1.4 Filtro de servicios 3.1.5. IPtables 3.2. Redes privadas virtuales (VPN) 3.2.1 Definición 3.2.2 Protocolos de redes privadas virtuales 3.3. Asignación segura de nombres de dominio (DNS) 3.4. Seguridad en Sistemas WEB. 3.6. Seguridad en correo electrónico, protocolos POPS, IMAPS, SMTPS. 3.6.1. Correo con privacidad mejorada (PEM) 3.6.2. MIME seguro. 3.6.3. Protocolo PGP.
4.	Seguridad en redes inalámbricas y dispositivos móviles.	4.1 Riesgos y amenazas en las redes inalámbricas 4.2 Mecanismos de protección en las redes inalámbricas 4.2.1 Privacidad equivalente al cableado (WEP) 4.2.2 Acceso inalámbrico Protegido (WPA) 4.2.3 Listas de Control de Acceso (Filtrado MAC) 4.3 Uso de portales cautivos (hotspot). 4.4 Uso de software Autenticación Remota Radius con Base de Datos. 4.5. Factores que afectan la seguridad de dispositivos móviles. 4.6. Requisitos de seguridad en el desarrollo de aplicaciones en las diferentes plataformas móviles. 4.7. Seguridad en la transmisión de voz.
5	Seguridad en la nube.	5.1. Seguridad en la Infraestructura. 5.2. Seguridad en los datos almacenados. 5.3. Manejo del acceso y la autenticación. 5.4. Seguridad en el manejo de la nube. 5.5. Privacidad.

8.- SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

El profesor 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 metacognición. Ante la ejecución de una actividad, señalar o identificar el tipo de proceso intelectual que se realizó: una identificación de patrones, un análisis, una síntesis, la creación de un heurístico, etc. Al principio lo hará el profesor, luego será el estudiante quien lo identifique.
• Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes.
• 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 practicas en equipo que permitan obtener un resultado a partir del trabajo de todos.
• 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.
• 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 reportes e informes de las actividades de experimentación, exponer al grupo las conclusiones obtenidas durante las observaciones.
• Propiciar el desarrollo de actividades intelectuales de inducción-deducción y análisis-síntesis, que encaminen hacia una posición crítica del estudiante.
• Desarrollar actividades de aprendizaje que propicien la aplicación de los conceptos de seguridad, 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.
• Relacionar los contenidos de la asignatura con el cuidado del medio ambiente; así como con las prácticas.
• Cuando los temas lo requieran, utilizar medios audiovisuales para una mejor comprensión del estudiante.

9.- SUGERENCIAS DE EVALUACIÓN

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 observaciones hechas durante las actividades realizadas en el laboratorio, así como de las conclusiones obtenidas de dichas observaciones.
• Reportes escritos de las soluciones a problemas desarrollados fuera de clase.
• Información obtenida durante las investigaciones solicitadas plasmada en documentos escritos.
• Exámenes escritos para comprobar el manejo de aspectos teóricos.
• Desarrollo de programas de ejemplo.
• Descripción de otras experiencias concretas que podrían realizarse adicionalmente (participación, integración, entrega de proyectos en tiempo, etc.)

10.- UNIDADES DE APRENDIZAJE

Unidad 1: Introducción a la seguridad en redes.

Competencia específica a desarrollar	Actividades de Aprendizaje
Identificar la importancia de la seguridad en cómputo móvil.	• Investigar en distintas fuentes, la importancia de la seguridad en dispositivos móviles. • Investigar en distintas fuentes los usos y tipos de seguridad en aplicaciones móviles. • Identificar los dispositivos de seguridad utilizados por las diferentes plataformas.

Unidad 2: Criptografía y Autenticación.

Competencia específica a desarrollar	Actividades de Aprendizaje

Identificar diferentes formas de cifrado Así como protocolos de autenticación.	• Investigar en distintas fuentes, las diferentes formas de cifrado así como los protocolos de autenticación. • Realizar un análisis de ventajas de la seguridad en la redes. • Investigar en distintas fuentes los usos y tipos de seguridad en redes y sus aplicaciones en móviles. • Identificar los dispositivos de seguridad utilizados por las diferentes tipos de redes.

Unidad 3: Seguridad en la comunicación de datos.

Competencia específica a desarrollar	**Actividades de Aprendizaje**
Garantizar la confidencialidad, integridad y disponibilidad de la información mediante el uso de comunicaciones seguras.	•Investigar los diferentes tipos Protocolos de comunicación segura. •Instalar y Configurar algunos Protocolos de comunicación segura para servicios como web, correo, vpn, etc.

Unidad 4: Seguridad en redes inalámbricas y dispositivos móviles.

Competencia específica a desarrollar	**Actividades de Aprendizaje**
Configurará mecanismos de seguridad para redes inalámbrica y dispositivos móviles.	•Investigar los diferentes tipos cifrado para redes inalámbricas. •identificar los Factores que afectan la seguridad de dispositivos móviles.

Unidad 5: Seguridad en la nube.

Competencia específica a desarrollar	**Actividades de Aprendizaje**
Identificar la importancia de la seguridad en cómputo en la nube.	• Investigar en distintas fuentes, la importancia de la seguridad en la nube. • Investigar en distintas fuentes los usos y tipos de seguridad de aplicaciones en la nube.

11.- FUENTES DE INFORMACIÓN

Fuentes impresas (libros)

1. **Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Author: Tim Mather. Subra Kumaraswamy y Shahed Laitf (Octubre 2009).**
2. **Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. Author: Stephen Fried.**
3. **Robert Gellman. (2009), Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Estados Unidos.**

12.- PRÁCTICAS PROPUESTAS