Programa Oficial de Asignatura

Arquitecturas de Seguridad

Ficha Técnica

Titulación:	Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación		
Plan BOE:	BOE número 108 de 6 de mayo de 2015		
Asignatura:	Arquitecturas de Seguridad		
Módulo:	Mención Telemática		
Curso:	3º/4º	**Créditos ECTS:**	6
Tipo de asignatura:	Optativa	**Tipo de formación:**	Teórica y Práctica

Presentación

En esta asignatura, correspondiente a la mención en sistemas telemáticos, se pretende dar a conocer al estudiante los principales conceptos de seguridad asociados a las redes de comunicaciones.

En la seguridad de las redes entran en juego diferentes aspectos a tener en cuenta. En primer lugar se realizará un análisis somero de la importancia de las políticas de seguridad y los estándares correspondientes.

Un punto importante será el conocimiento de las amenazas existentes tanto en lo referente a vulnerabilidades, malware y la respuesta a los incidentes correspondientes. Ligado con este punto, herramientas para la protección serán también analizadas así como mecanismo para la seguridad en el uso de servicios en internet.

Dentro del contenido de la asignatura se propone la realización de ejercicios prácticos.

Competencias y/o resultados del aprendizaje

Resultados de aprendizaje:

- Conocimientos teóricos y prácticos para construir, explotar y gestionar redes, servicios, procesos y aplicaciones de telecomunicaciones, entendiéndolas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.
- Conocimientos prácticos sobre cómo aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y tráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.
- Conocimientos necesarios para diseñar arquitecturas de redes y servicios telemáticos.

Contenidos Didácticos

1 Principios básicos de seguridad informática

1.1 Qué se entiende por seguridad informática
1.2 Objetivos de la seguridad informática
1.3 Servicios de seguridad informática
1.4 Consecuencias de la falta de seguridad
1.5 Principio de "defensa en seguridad"
1.6 Políticas, planes y procedimientos de seguridad
1.6.1 Gestión de cuentas de usuarios
1.6.2 Identificación y autenticación de usuarios
1.6.3 Autorización y control de acceso lógico
1.6.4 Monitorización de servidores
1.6.5 Protección de datos
1.6.6 Seguridad en conexiones remotas
1.7 La importancia del factor humano

2 Estandarización y certificación en seguridad informática.
2.1 Estándares de seguridad
2.1.1 Propósito de los estándares
2.1.2 Organismos responsables
2.2 Estándares en EEUU
2.2.1 TCSEC
2.2.2 Federal Criteria
2.2.3 FISCAM
2.2.4 NIST SP 800
2.3 Estándares Europeos
2.3.1 ITSEC
2.3.2 ITSEM
2.3.3 Agencia Europea de Seguridad de la Información y las Redes
2.4 Estándares internacionales
2.5 Proceso de certificación

3 Amenazas a la seguridad informática: Vulnerabilidades y Malware.
3.1 Vulnerabilidades de los sistemas
3.1.1 Indicendetes de seguridad en las redes
3.1.2 Causas de las vulnerabilidades de los sitemas informáticos
3.1.3 Tipos de vulnerabilidades
3.1.4 Responsabilidades de los fabricantes de software
3.1.5 Herramientas para la evaluación de vulnerabilidades
3.2 Amenazas de la seguridad informática
3.2.1 Clasificación de los intrusos en redes
3.2.2 Motivaciones de los atacantes
3.2.3 Fases de un ataque
3.2.4 Tipos de ataques
3.3 Virus informáticos
3.3.1 Características generales
3.3.2 Tipos de virus
3.3.3 Daños ocasionados por virus
3.3.4 Cómo combatir los virus

4 Ciberterrorismo y Respuesta a Incidentes.
4.1 La amenaza del ciberterrorismo y de las guerras informáticas

- 4.2 Consecuencias de los fallos y ataques en las empresas
- 4.3 El espionaje en las redes de ordenadores

5 Identificación de usuarios y sistemas biométricos.
- 5.1 Autenticación autorización y registro de usuarios
  - 5.1.1 Modelo de seguridad AAA
  - 5.1.2 Control de acceso
  - 5.1.3 Identificación de usuarios
  - 5.1.4 Verificación de contraseñas
  - 5.1.5 Autenticación con certificados digitales
  - 5.1.6 Identificación remota de usuarios
  - 5.1.7 Inicio de sesión único
  - 5.1.8 Gestores de contraseñas
- 5.2 Sistemas biométricos
  - 5.2.1 Características generales
  - 5.2.2 Tipos de sistemas biométricos
  - 5.2.3 Implantación de los sistemas

6 Fundamentos de Criptografía y protocolos criptográficos.
- 6.1 Fundamentos de criptografía
  - 6.1.1 Critptografía, criptoanálisis y criptología
  - 6.1.2 Funcionamiento de un sistema criptográfico
  - 6.1.3 Historia de los sistemas criptográficos
  - 6.1.4 Criptoanálisis
  - 6.1.5 Clasificación de los sistemas criptográficos
  - 6.1.6 Sistemas criptográficos simétricos
  - 6.1.7 Sistemas criptográficos asimétricos
  - 6.1.8 Autenticación con sistemas criptográficos
- 6.2 Firma electrónica
  - 6.2.1 Qué es la firma electrónica
  - 6.2.2 Características de la firma electrónica
  - 6.2.3 Autoridades de certificación
  - 6.2.4 Certificados digitales
  - 6.2.5 Sistemas basados en el tercero de confianza
  - 6.2.6 Utilización de la firma electrónica
  - 6.2.7 DNI electrónico
  - 6.2.8 Factura electrónica

7 Herramientas para la seguridad en redes.
- 7.1 El problema de la seguridad en la conexión a internet
- 7.2 La seguridad en la red externa
- 7.3 El papel de los servidores Proxy
- 7.4 El papel de los cortafuegos
- 7.5 Servidores de autenticación para conexiones remotas
- 7.6 El análisis de los registros de actividad
- 7.7 Sistemas de detección de intrusiones
- 7.8 Los señuelos

8 Seguridad en redes privadas virtuales e inalámbricas.
- 8.1 Seguridad en redes privadas virtuales
  - 8.1.1 El papel de las VPN
  - 8.1.2 Protocolos para VPNs

8.2 Seguridad en redes inalámbricas
- 8.2.1 Seguridad tradicional en redes inalámbricas
- 8.2.2 Posibles ataques en redes inalámbricas
- 8.2.3 El protocolo WEP
- 8.2.4 Estándares para seguridad en redes inalámbricas
- 8.2.5 Recomendaciones para reforzar la seguridad

9 Seguridad en el uso de servicios de internet.
- 9.1 Navegación segura en la web
  - 9.1.1 El servicio www
  - 9.1.2 Problemas de seguridad en www
  - 9.1.3 Recomendaciones de seguridad
  - 9.1.4 Protección de la privacidad en internet
- 9.2 Seguridad en correo electrónico
  - 9.2.1 Características del correo electrónico
  - 9.2.2 Problemas de seguridad en el correo electrónico
  - 9.2.3 Recomendaciones de seguridad en el correo electrónico
  - 9.2.4 Servicios de correo electrónico avanzados
  - 9.2.5 Uso de correo electrónico por empleados
- 9.3 El SPAM
- 9.4 El phising

10 Control de contenidos
- 10.1 La distribución de contenidos a través de internet
- 10.2 Medidas legales para combatir los contenidos ilícitos
- 10.3 Filtrado, catalogación y bloqueo de contenidos
- 10.4 Daños a la imagen y reputación.

Contenidos Prácticos

Durante el desarrollo de la asignatura se realizarán las siguientes actividades prácticas:

- Cifrado de mensajes
- Firewalls
- VPN

Evaluación

El sistema de evaluación del aprendizaje de la UDIMA contempla la realización de diferentes tipos de actividades de evaluación y aprendizaje. El criterio de valoración establecido se detalla a continuación:

Actividades de aprendizaje	10%
Controles	10%
Actividades de Evaluación Continua (AEC)	20%
Examen final presencial	60%
TOTAL	**100%**

Bibliografía

- Enciclopedia de la Seguridad Informática. Álvaro Gómez Vieites. Ra-Ma Editorial 2011

- Seguridad Informática para Empresas y Particulares. Álvarez Marañón, Gonzalo; Pérez García, Pedro Pablo. McGraw-Hill España, Jan 1, 2004

- Introducción a la Seguridad Informática Baca Urbina, Gabriel Grupo Editorial Patria, Jan 1, 2016

- Auditoría de Seguridad Informática Gómez Vieites, Álvaro. RA-MA Editorial, Jan 1, 2014