Proyecto/Guía docente de la asignatura

Asignatura	SEGURIDAD EN REDES DE COMUNICACIONES		
Materia	PLANIFICACIÓN Y GESTIÓN DE REDES Y SERVICIOS TELEMÁTICOS		
Módulo	MATERIAS ESPECÍFICAS DE LA MENCIÓN EN TELEMÁTICA		
Titulación	GRADO EN INGENIERÍA TECNOLOGÍAS ESPECÍFICAS DE TELECOMUNICACIÓN		
Plan	512	**Código**	46667
Periodo de impartición	2º Cuatrimestre	**Tipo/Carácter**	OPTATIVA (OBLIGATORIA DE LA MENCIÓN)
Nivel/Ciclo	Grado	**Curso**	4º
Créditos ECTS	6		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Juan Carlos García Escartín y Manuel Rodríguez Cayetano		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 5542 y 5541 . E-MAIL: , juagar@tel.uva.es, manuel.rodriguez@tel.uva.es		
Departamento	TEORÍA DE LA SEÑAL Y COMUNICACIONES E INGENIERÍA TELEMÁTICA		
Fecha de revisión por el comité de título	8 de julio de 2024		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La Seguridad en las Redes de Comunicaciones ha pasado de ser un conjunto de conocimientos complementarios a otras materias a convertirse en una disciplina en sí misma. Además, la aportación que se hace desde la seguridad en las redes a la seguridad de toda la arquitectura telemática que engloba todos los sistemas de información implicados es incuestionable pues constituye la estructura básica de aplicación de criterios de seguridad en profundidad.

De esta manera, lo que hasta hace muy pocos años se planteaban como conocimientos muy específicos por una parte en el ámbito de la criptografía y sus modelos matemáticos asociados y por otra en el ámbito de la seguridad física y perimetral básica, actualmente ha explosionado, y hoy en día se habla de términos como seguridad en profundidad, acceso seguro a las redes, certificados digitales, identidad electrónica, gestión de la seguridad, … Todos estos conceptos en su conjunto generan una materia altamente multidisciplinar.

Como consecuencia de esta evolución los términos que estaban reservados a un conjunto de expertos en criptografía y seguridad física, han pasado a ser parte de la ocupación y preocupación de una gran cantidad de técnicos y gestores en el ámbito de las Tecnologías de la Información, y cada día se acercan en mayor medida a las actividades que realizan los usuarios al utilizar las referidas tecnologías.

Llegados a este punto, es necesario valorar que los nuevos modelos aplicados en los servicios de seguridad forman parte de la Sociedad de la Información con importancia creciente día a día, hasta llegar a la situación de que sin contar con algunos aspectos de la seguridad como son la identidad electrónica, no puede hablarse de un pleno desarrollo de la Sociedad de la Información.

De esta manera los profesionales involucrados en el diseño sistemas y servicios telemáticos deben conocer, entender y aplicar las metodologías, técnicas y servicios de seguridad de manera que en sus proyectos puedan garantizar las propiedades de la seguridad que sea necesario alcanzar.

1.2 Relación con otras materias

Esta asignatura está relacionada con la asignatura “Redes y Servicios Telemáticos”, pues dicha asignatura proporciona los conocimientos básicos para comprender la arquitectura de los sistemas telemáticos, los cuales deberán ser tratados adecuadamente para conseguir que resulten seguros, con la asignatura “Ingeniería de protocolos”, pues en dicha asignatura se estudian las bases de los protocolos de seguridad y con la asignatura “Administración y Gestión de Redes de Comunicaciones” , de tercer curso del Grado en Ingeniería Telemática en donde se comentan algunos conceptos generales de seguridad.

1.3 Prerrequisitos

No existen condiciones previas excluyentes para cursar esta asignatura, aunque sí recomendaciones lógicas que el alumno debería tener en cuenta. Como consecuencia y teniendo en cuenta el apartado anterior, es recomendable haber cursado la asignatura “Redes y Servicios Telemáticos” correspondiente a la materia

"Fundamentos de Protocolos, Redes y Servicios Telemáticos" dentro del módulo de "Materias Básicas de Telecomunicaciones" y haber cursado la asignatura de "Ingeniería de Protocolos".

Para la evaluación del aprendizaje de esta asignatura el alumno acepta utilizar los mecanismos técnicos que constan en esta Guía y aquellos que la Universidad determine y/o facilite.

2. Competencias

2.1 Generales

- GBE1. Conocimiento, comprensión y capacidad para aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico de Telecomunicación y facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento
- GBE3. Capacidad para resolver problemas con iniciativa, creatividad y razonamiento crítico.
- GBE4. Capacidad para diseñar y llevar a cabo experimentos, así como analizar e interpretar datos.
- GBE5. Capacidad para elaborar informes basados en el análisis crítico de la bibliografía técnica y de la realidad en el campo de su especialidad.
- GE3. Capacidad para desarrollar metodologías y destrezas de aprendizaje autónomo eficiente para la adaptación y actualización de nuevos conocimientos y avances científicos.
- GE6. Capacidad, y compromiso ético en la elaboración de soluciones de ingeniería y en las diversas situaciones de gestión de recursos humanos y de gestión económica, así como capacidad para comprender el impacto de las soluciones de Ingeniería en un contexto social global.
- GC1. Capacidad de organización, planificación y gestión del tiempo.
- GC2. Capacidad para comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.

2.2 Específicas

- TEL1. Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.
- TEL2. Capacidad para 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 teletráfico) 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.
- TEL3. Capacidad de construir, explotar y gestionar servicios telemáticos, utilizando herramientas analíticas de planificación, de dimensionado y de análisis.

4. Contenidos y/o bloques temáticos

Bloque 1: La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.

Carga de trabajo en créditos ECTS: 0,6

a. Contextualización y justificación

Este bloque consta de un tema introductorio que pretenden implicar al alumno en el problema de la gestión de la seguridad. Para ello se presenta al alumno una visión global de los problemas de seguridad en la empresa, en los sistemas y en los datos. Se contestará a las preguntas varias preguntas. ¿Qué queremos proteger? ¿De qué amenazas queremos protegerlo? ¿Cómo lo podemos proteger? Veremos amenazas, y las Salvaguardas o Mecanismos de Protección y Seguridad que se implantan.

Después, se discute el concepto de la política de seguridad y análisis de Riesgos, pues entre otras cosas se deben cumplir una serie de normas legales, que las obligan a que se realicen Auditorias de seguridad para comprobar que están implantados determinados mecanismos de seguridad. Por último, se verán los aspectos legales y normativos que están implicados. Especialmente el nuevo Reglamento Europeo del 25/5/2018.

b. Objetivos de aprendizaje

Al finalizar este bloque temático, el alumno deberá ser capaz de:

- Analizar los riesgos a los que está sometida una red telemática.
- Conseguir una reducción del riesgo obtenido del análisis mediante la aplicación de salvaguardas
- Conocer la metodología a aplicar para conseguir una adecuada gestión de la seguridad telemática
- Conocer las vulnerabilidades de las redes y sistemas telemáticos
- Conocer herramientas básicas para el análisis y gestión de riesgos
- Conocer, interpretar y aplicar legislación, normativa y metodologías del ámbito de la seguridad telemática y de la protección de datos
- Identificar vulnerabilidades, amenazas y ataques en un sistema de telecomunicación.
- Seleccionar los métodos de defensa adecuados ante amenazas.

c. Contenidos

TEMA 1: Introducción a la seguridad en redes de comunicaciones

1.1 Introducción

1.2 Análisis de riesgos y amenazas.

1.3 Consejos generales de diseño.

d. Métodos docentes

Se empleará:

Clase magistral participativa

Experimentación en prácticas de laboratorio

e. Plan de trabajo

Véase el Anexo I.

f. Evaluación

La evaluación de la adquisición de competencias se basará en:

- Valoración de la capacidad para expresar correctamente los conocimientos adquiridos a lo largo de la asignatura.

Informes sobre el trabajo de las sesiones de laboratorio.

Prueba al final del bloque.

g Material docente

El material docente necesario estará disponible en el Campus Virtual.

g.1 Bibliografía básica

Bibliografía disponible en el sistema Leganto: URL:
https://buc-uva.alma.exlibrisgroup.com/leganto/public/34BUC_UVA/lists/5051003080005774?auth=SAML

g.2 Bibliografía complementaria

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

- https://www.ccn-cert.cni.es Centro Criptográfico Nacional:
- http://www.agpd.es Agencia Española de Protección de Datos
- El portal de ISO 27000: http://www.iso27000.es/

h. Recursos necesarios

Serán necesarios los siguientes recursos, todos ellos facilitados por la UVA o el profesor:

- Entorno de trabajo en la plataforma Moodle ubicado en el Campus Virtual de la Universidad de Valladolid
- Documentación de apoyo.
- En el laboratorio el alumno dispondrá de los equipos necesarios (ordenadores personales y servidores) para la realización de las prácticas correspondientes.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
0,6 ECTS	Semanas 1 a 2

Bloque 2: Criptografía . Tipos de cifrado. Infraestructura de clave pública.

Carga de trabajo en créditos ECTS: 3,0

a. Contextualización y justificación

Este bloque consta de siete temas. El objetivo de este bloque es dar a conocer al alumno la criptografía como una de las herramientas para aumentar la seguridad en las redes de comunicaciones. Tras hacer una clasificación de los diferentes sistemas de cifrado en clásico y moderno, cifrado en bloque y en flujo, y cifrado simétrico y asimétrico, se estudia su funcionamiento, y ejemplos actuales de estos algoritmos de cifrado. Se analizan las funciones que proporcionan integridad y autentificación, las funciones hash y códigos MAC, junto con las firmas digitales. Se estudian los certificados digitales, las autoridades de certificación y la Infraestructura de Clave Pública (PKI) que se construye a nivel práctico para proporcionar seguridad con certificados.

b. Objetivos de aprendizaje

Al finalizar este bloque temático, el alumno deberá ser capaz de:

- Definir un sistema de cifrado.
- Clasificar los diferentes sistemas de cifrado (simétrico, asimétrico, en flujo, en bloque).
- Seleccionar el sistema de cifrado más adecuado a un escenario de trabajo.
- Conocer y explicar el funcionamiento de los sistemas de cifrado AES, DES, 3DES, RSA, Diffie-Hellman, RC4 y A5.

- Conocer la finalidad de las funciones hash y los algoritmos MAC.
- Explicar el funcionamiento de los sistemas de autenticación.
- Conocer la finalidad y el funcionamiento de la firma digital, los certificados digitales y las autoridades de certificación.
- Describir qué es un certificado digital, qué información contiene y cómo se obtiene.
- Describir qué es una Infraestructura de Clave Pública (PKI.)

c. Contenidos

Tema 2: Criptografía simétrica

2.1 Introducción al cifrado.

2.2 Cifrado por bloques.

2.3 Algoritmos simétricos. DES y 3DES, AES.

2.4 Modos de cifrado por bloques. ECB, CBC, OFB y CTR.

Tema 3: Teoría de Números

3.1 Introducción.

3.2 El grupo multiplicativo de enteros módulo N.

3.3 Función de Euler

3.4 Operaciones eficientes: inverso modular y exponenciación modular.

3.5 Tests de primalidad.

Tema 4: Criptografía Asimétrica

4.1 Introducción Criptografía Asimétrica.

4.2 Algoritmos asimétricos. RSA.

4.3 Curvas elípticas.

4.4 Diffie-Hellman.

Tema 5: Autentificación. Hash. Firmas Digitales

5.1 Introducción.

5.2 Funciones hash.

5.3 Propiedades.

5.4 Ejemplos de aplicación.

Tema 6: Canal seguro

6,1 Introducción.

6.2 Funciones MAC.

6.3 HMAC.

6.4 Ejemplo de diseño.

Tema 7: Certificados digitales y PKI

7.1 Introducción

7.2 Certificados digitales.

7.3 Autoridades de certificación.

7.4 PKI (Infraestructura de Clave Pública)

d. Métodos docentes

Se empleará:

- Clase magistral participativa
- Seminario
- Experimentación en prácticas de laboratorio

e. Plan de trabajo

Véase el Anexo I.

f. Evaluación

La evaluación de la adquisición de competencias se basará en:

- Valoración de la capacidad para expresar correctamente los conocimientos adquiridos a lo largo de la asignatura.
- Informes sobre el trabajo de las sesiones de laboratorio.
- Prueba al final del bloque.

g Material docente

El material necesario estará disponible en el Campus Virtual.

g.1 Bibliografía básica

Bibliografía disponible en el sistema Leganto: URL:
https://buc-uva.alma.exlibrisgroup.com/leganto/public/34BUC_UVA/lists/5051003080005774?auth=SAML

g.2 Bibliografía complementaria

-

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

En el Campus Virtual de la asignatura.

h. Recursos necesarios

Serán necesarios los siguientes recursos, todos ellos facilitados por la UVA o el profesor:

- Entorno de trabajo en la plataforma Moodle ubicado en el Campus Virtual de la Universidad de Valladolid
- Documentación de apoyo.
- En el laboratorio el alumno dispondrá de los equipos necesarios (ordenadores personales y servidores) para la realización de las prácticas correspondientes.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
3,0	Semanas 2 a 15

4. Contenidos y/o bloques temáticos

Bloque 3: Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.

Carga de trabajo en créditos ECTS: 2,4

a. Contextualización y justificación

La seguridad en Internet es uno de los principales temas de preocupación, estudio e investigación. En este bloque, se ven los protocolos de seguridad que se emplean en distintas capas de la arquitectura TCP/IP, desde el nivel de aplicación hasta el nivel de enlace. Se estudiará, en el Nivel de Aplicación los protocolos, HTTS, SSH, y Kerberos, en el nivel de Transporte los protocolos SSL/TSL, en el Nivel de Red el protocolo IPSec, y en el nivel de enlace el protocolo EAP, y la seguridad WIFI.

Posteriormente se estudian los métodos no criptográficos utilizados para la implantación de la seguridad. Se analizan las distintas tecnologías de cortafuegos y los Sistemas de Detección de Intrusos. Es necesario conocer las herramientas disponibles para poder descubrir las vulnerabilidades antes de que una persona externa a nuestra red lo haga. Por ello se verán técnicas de auditoría de vulnerabilidades.

b. Objetivos de aprendizaje

Al finalizar este bloque temático, el alumno deberá ser capaz de:

- Seleccionar en función del ámbito de trabajo los protocolos de seguridad más eficaces.
- Conocer el funcionamiento del protocolo de autenticación EAP.
- Conocer el motivo de aplicar seguridad en las distintas capas del modelo TCP/IP
- Describir el funcionamiento de los protocolos de seguridad Kerberos, SSL, TLS e IPSec.
- Conocer la utilidad de un cortafuegos y de un sistema detector de intrusos.
- Seleccionar la topología de cortafuegos más adecuada al ámbito de trabajo.
- Configurar filtros de control de acceso para seguridad en los encaminadores.
- Utilizar herramientas de seguridad existentes.
- Configurar un servidor web seguro mediante certificados digitales.
- Conocer herramientas existentes para poder descubrir las vulnerabilidades.

c. Contenidos

Tema 8: Sistemas de Defensa Perimetral.

8.1 Tipos
8.2 Cortafuegos
8.3 Sistemas de Detección de Intrusos
8.4 Señuelos (Honeypots)

Tema 9: Protocolos de Seguridad a nivel de transporte

9.1 Introducción
9.2 Protocolo Secure Socket Layer (SSL)
9.3 Protocolo Transport Layer Security (TLS)

Tema 10: Seguridad a nivel de aplicación

10.1 HTTPS

10.2 SSH

10.3 Sistema Kerberos

Tema 11: Seguridad a nivel de red: IPSEC

11.1 Introducción

11.2 Arquitectura IPSEC

11.3 Protocolo AH

11.4 Protocolo ESP

11.5 Protocolo IKE

Tema 12: Seguridad a nivel de Enlace: EAP, 801.1x, Seguridad WIFI

12.1 Protocolo EAP

12.2 Arquitectura 802.1x. Servidor Radius

12.3 Seguridad WIFI. WEP.WPA.WPA-2..RSN

d. Métodos docentes

Se empleará:

- Clase magistral participativa
- Seminario
- Experimentación en prácticas de laboratorio

e. Plan de trabajo

Véase el Anexo I.

f. Evaluación

La evaluación de la adquisición de competencias se basará en:

- Valoración de la capacidad para expresar correctamente los conocimientos adquiridos a lo largo de la asignatura.
- Informes sobre el trabajo de las sesiones de laboratorio.
- Prueba al final del bloque.

g Material docente

Bibliografía disponible en el sistema Leganto: URL:
https://buc-uva.alma.exlibrisgroup.com/leganto/public/34BUC_UVA/lists/5051003080005774?auth=SAML

g.1 Bibliografía básica

-

g.2 Bibliografía complementaria

-

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

h. Recursos necesarios

Serán necesarios los siguientes recursos, todos ellos facilitados por la UVA o el profesor:

- Entorno de trabajo en la plataforma Moodle ubicado en el Campus Virtual de la Universidad de Valladolid.
- Documentación de apoyo.
- En el laboratorio el alumno dispondrá de los equipos necesarios (ordenadores personales y servidores) para la realización de las prácticas correspondientes.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
2,4	Semanas 6 a 15

5. Métodos docentes y principios metodológicos

- Clase magistral participativa
- Prácticas en el laboratorio
- Trabajo en grupo en el laboratorio

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA(1)	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	**25**	**Estudio y trabajo autónomo individual**	**60**
Clases prácticas de aula (A)	**0**	**Estudio y trabajo autónomo grupal**	**30**
Laboratorios (L)	**25**		
Prácticas externas, clínicas o de campo	**0**		
Seminarios (S)	**10**		
Tutorías grupales (TG)	**0**		
Total presencial	**60**	Total no presencial	**90**
		TOTAL presencial + no presencial	**150**

(1) Actividad presencial a distancia es cuando un grupo sigue una videoconferencia de forma síncrona a la clase impartida por el profesor.

7. Sistema y características de la evaluación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
(EXA) Examen final.	50 %	Es necesario aprobar el examen (nota de 5 puntos sobre 10) para superar la asignatura.
(LAB) Informes de las prácticas de laboratorio	50 %	Es condición necesaria (pero no suficiente) para superar la asignatura entregar todos los informes de laboratorio y sacar una nota mayor o igual a 5 sobre 10 puntos.

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**
  - **Se debe aprobar cada parte (examen y prácticas) para supera la asignatura.**
- **Convocatoria extraordinaria:**
  - Los alumnos que han superado (LAB) pero no (EXA):
    - Salvo petición expresa en sentido contrario, indicada el día de la revisión de la convocatoria ordinaria, mantienen la nota alcanzada en (LAB) y deben realizar de nuevo (EXA).
    - Si el día de la revisión de la convocatoria ordinaria lo solicitan expresamente, pueden repetir de nuevo la parte de (LAB). Además deben realizar de nuevo (EXA).
  - Los alumnos que han superado (EXA) pero no (LAB):
    - Salvo petición expresa en sentido contrario, indicada el día de la revisión de la convocatoria ordinaria, mantienen la nota alcanzada en (EXA) y deben repetir la parte de (LAB).
    - Si el día de la revisión de la convocatoria ordinaria lo solicitan expresamente, pueden repetir de nuevo la parte de (EXA), además de repetir obligatoriamente la parte de (LAB).
  - Los alumnos no han superado ni (EXA) ni (LAB):
    - Deben repetir ambas partes.