Proyecto/Guía docente de la asignatura Adaptada a la Nueva Normalidad

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	1er. CUATRIMESTRE	**Tipo/Carácter**	OPTATIVA (OBLIGATORIA DE LA MENCIÓN)
Nivel/Ciclo	GRADO	**Curso**	4º
Créditos ECTS	6 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	Francisco Javier Merino Caminero		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 6383 . E-MAIL: , framer@tel.uva.es		
Horario de tutorías	Ver Tutorías en: http://www.uva.es/export/sites/uva/2.docencia/2.01.grados/2.01.02.ofertaformativagrados/2.01.02.01.alfabetica/Grado-en-Ingenieria-de-Tecnologias-Especificas-de-Telecomunicacion/		
Departamento	TEORÍA DE LA SEÑAL Y COMUNICACIONES E INGENIERÍA TELEMÁTICA		

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,….., conceptos que 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.

De forma excepcional para este curso 2020-2021, se disminuye la presencialidad, pasando del 40% establecido en la memoria de verificación a una presencialidad del 35%/30%, con el objetivo de optimizar los espacios seguros disponibles, ajustando su utilización al calendario de actividades lectivas y al tamaño más pequeño de los grupos y buscando la máxima presencialidad del estudiante a nivel del título.

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”.

Dado el escenario de "nueva normalidad" y atendiendo a la posible evolución de los acontecimientos, en esta asignatura se utilizan o se podrán utilizar herramientas docentes online para la docencia y la evaluación. El alumno deberá contar con medios informáticos y telemáticos suficientes para interactuar con el Campus Virtual y con los sistemas de videoconferencia.
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.

3. Objetivos

Al finalizar la asignatura el alumno deberá ser capaz de:

- Comprender los principales tipos de vulnerabilidades en el funcionamiento de las redes y sistemas telemáticos y conocer las principales técnicas para solucionarlas.
- Determinar los procedimientos a aplicar y las herramientas a utilizar para incrementar el nivel de seguridad de una red telemática y de la información manejada por la misma
- Conocer, interpretar y aplicar legislación, normativa y metodologías del ámbito de la seguridad telemática y de la protección de datos
- Encontrar y analizar información técnica relacionada con la seguridad telemática y realizar informes técnicos con dicha información.
- Trabajar en equipo en problemas multidisciplinares relacionados con el diseño de redes seguras, así como presentar los resultados obtenidos

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: 0.7

a. Contextualización y justificación

Este bloque consta de tres temas que pretenden implicar al alumno en el problema de la gestión de la seguridad. Para ello se presenta al alumno una introducción a 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 y conceptos básicos.

1.1 Introducción
1.2 Seguridad del entorno.
1.3 Seguridad del sistema.
1.4 Seguridad de la red.

TEMA 2: Gestión de la Seguridad. Análisis y gestión de riesgos

2.1 Introducción
2.2 Análisis de riesgos y amenazas.
2.3 Políticas de Seguridad.
2.4 Seguridad y análisis de Riesgos.

TEMA 3: Legislación y normativa de seguridad

3.1 Introducción
3.2 Reglamento General de Protección de Datos Europeo (25/5/2018)
3.3 Metodologías ISO 27000

d. Métodos docentes

Se empleará:

- Clase magistral participativa
- Experimentación en prácticas de laboratorio
- Aprendizaje colaborativo

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, realizados por los alumnos en grupos de dos personas.
- Prueba escrita al final del bloque, que incluye una parte de teoría, y otra de laboratorio. Será necesario alcanzar una nota mínima tanto en la parte de teoría y de laboratorio para aprobar la asignatura.

.

g Material docente

g.1 Bibliografía básica

- Antonio Villalón Huerta. “Seguridad en Unix y Redes”. Versión 2.1. Julio, 2002. Temas 1 a 5 y 22.
- Castro Gil, Manuel Alonso “Seguridad en las comunicaciones y en la información”. Ed: UNED. 2002 Temas 1 y 6.
- Emmett Dulaney “Seguridad Informática.CompTIA Security+” Ed: Anaya. 2013
- William Stallings, "Network Security Essentials Applications and standards”, Ed.6 Pearson Education, 2016

g.2 Bibliografía complementaria

- J. Ramiro Aguirre. “Libro Electrónico de seguridad informática y criptografía” Ed: Universidad Politécnica de Madrid.2006

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

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.	0.7 ECTS	Semanas 1 a 2
Bloque 2: Criptografía. Tipos de cifrado. Infraestructura de clave pública.	2.6 ECTS	Semanas 2 a 7
Bloque 3: Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.	2.6 ECTS	Semanas 7 a 13

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

Carga de trabajo en créditos ECTS: 2.6

a. Contextualización y justificación

Este bloque consta de seis 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 HMAC, MD5 y SHA-1.
- 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 4: Criptografía.

4.1 Introducción a la Criptografía.

4.2 Cifrado clásico

4.3 Técnicas de Sustitución y de Permutación...

Tema 5: Criptografía simétrica.

5.1 Introducción al cifrado en flujo. RC4,A5

5.2 Introducción al cifrado en bloque.

5.3 Algoritmos simétricos Cifrado Bloque. DES y 3DES,AES

5.4 Distribución de claves

Tema 6: Teoría de Números.

6.1 Congruencia.CCR Conjunto Completo de restos

6.2 Inversos dentro de un cuerpo n

6.3 CRR Conjunto Reducido de restos

6.4 Función de Euler

Tema 7: Criptografía Asimétrica.

7.1 Introducción Criptografía Asimétrica.

7.2 Algoritmos asimétricos. RSA.

7.3 Curvas elípticas

7.4 Diffie-Hellman.

Tema 8: Autentificación. Hash. Firmas Digitales.

8.1 Introducción

8.2 Funciones MAC

8.3 Funciones HASH. MD5, SHA

8.4 HMAC

8.5 Firma digital

Tema 9: Certificados digitales y PKI.

9.1 Introducción

9.2 Certificados digitales.

9.3 Autoridades de certificación.

9.4 PKI (Infraestructura de Clave Pública)

d. Métodos docentes

Se empleará:

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

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, realizados por los alumnos en grupos de dos personas.
- Prueba escrita al final del bloque, que incluye una parte de teoría, y otra de laboratorio. Será necesario alcanzar una nota mínima tanto en la parte de teoría y de laboratorio para aprobar la asignatura.

g Material docente

g.1 Bibliografía básica

- William Stallings, “Cryptography and network security: principles and practice” Ed. 7.Pearson Education, 2016
- William Stallings, "Network Security Essentials Applications and standards”, Ed.6 Pearson Education, 2016
- Amparo Fúster Sabater, "Técnicas criptográficas de protección de datos ", Ed. RA-MA, 2003

g.2 Bibliografía complementaria

- Bruce Schneier. “Applied Cryptography”.Ed. John Wiley & Sons., 1996
- J. Ramiro Aguirre. “Libro Electrónico de seguridad informática y criptografía” Ed: Universidad Politécnica de Madrid.2006

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

En Campus Virtual

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

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.	0.7 ECTS	Semanas 1 a 2
Bloque 2: Criptografía. Tipos de cifrado. Infraestructura de clave pública.	2.6 ECTS	Semanas 2 a 7

Bloque 3: Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.	2.6 ECTS	Semanas 7 a 13

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

Carga de trabajo en créditos ECTS: 2.6

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 OSI/ TCP/IP, desde el nivel de aplicación hasta el nivel de enlace. Se estudiará, en el Nivel de Aplicación los protocolos, HTTS, SSH, Kerberos, PGP y S/MIME, en el nivel de Transporte los protocolos SL/TSL, en el Nivel de Red el protocolo IPSec, y en el nivel de enlace el protocolo EAP, y la seguridad WIFI. AL estudiar estos protocolos, veremos soluciones de “Redes Privadas Virtuales”.

Posteriormente se estudian los métodos no criptográficos utilizados para la implantación de la seguridad. Se analizan las distintas tecnologías de cortafuegos, Redes Privadas Virtuales y los Sistemas de Detección de Intrusos,

Se finaliza estudiando aspectos de software maligno “Malware”, y como protegernos. Es necesario conocer las herramientas de hacking 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 y hacking ético.

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, sMIME, PGP, SSL, TLS e IPSec.
- Conocer la utilidad y diseñar una red privada virtual.
- Conocer la utilidad de un cortafuego 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 nmap y nexus.
- Configurar un servidor web seguro mediante certificados digitales.
- Conocer herramientas de hacking existentes para poder descubrir las vulnerabilidades.

c. Contenidos

Tema 10: Protocolos de Seguridad a nivel de transporte

10.1 Introducción

10.2 Protocolo Secure Socket Layer (SSL)

10.3 Protocolo Transport Layer Security (TLS)

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 aplicación.

12.1 HTTS,

12.2 SSH,

12.3 Sistema Kerberos,

12.4 Seguridad en el correo electrónico PGP, S/MIME.

Tema 13: Seguridad a nivel de Enlace: EAP, 801.1x, Seguridad WIFI

13.1 Protocolo EAP.

13.2 Arquitectura 802.1x. Servidor Radius.

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

Tema 14: Sistemas de Defensa Perimetral.

14.1 Tipos

14.2 Cortafuegos.

14.3 Sistemas de Detección de Intrusos.

14.4 Señuelos (Honeypots)

14.5 Redes Privadas Virtuales

Tema 15. Malware

15.1 Virus y otras amenazas.

15.2 Análisis de Malware

15.3 Auditoría de vulnerabilidades.

d. Métodos docentes

Se empleará:

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

e. Plan de

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, realizados por los alumnos en grupos de dos personas.

- Prueba escrita al final del bloque, que incluye una parte de teoría, y otra de laboratorio. Será necesario alcanzar una nota mínima tanto en la parte de teoría y de laboratorio para aprobar la asignatura.

g Material docente

g.1 Bibliografía básica

- William Stallings, “Cryptography and network security: principles and practice” Ed. 7. Pearson Education, 2016
- William Stallings, "Network Security Essentials Applications and standards”, Ed.6 Pearson Education, 2016

g.2 Bibliografía complementaria

- Carlos Tori, “Hacking Etico” 2008

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

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.	0.7 ECTS	Semanas 1 a 2
Bloque 2: Criptografía. Tipos de cifrado. Infraestructura de clave pública.	2.6 ECTS	Semanas 2 a 7
Bloque 3: Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.	2.6 ECTS	Semanas 7 a 13

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	38
Laboratorios (L)	17		
Prácticas externas, clínicas o de campo	0		
Seminarios (S)	10		
Tutorías grupales (TG)	0		
Evaluación (fuera del periodo oficial de exámenes)			
Total presencial	**52**	**Total no presencial**	**98**
		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

Criterio: cuando al menos el 50% de los días lectivos del cuatrimestre transcurran en normalidad, se asumirán como criterios de evaluación los indicados en la guía docente. Se recomienda la evaluación continua ya que implica minimizar los cambios en la adenda.

BLOQUE	INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
EXA	Examenes Parciales por escrito al finalizar cada Bloque. Parte de teoría y problemas. En caso de no aprobar (5.0) con los exámenes parciales, será necesario realizar un examen final de toda la asignatura.	70%	Es condición necesaria (pero no suficiente) para superar la asignatura alcanzar una calificación igual o superior a 3 puntos sobre la calificación global de la asignatura (10 puntos).
LAB	Informes de las sesiones de laboratorio	25%	Es condición necesaria (pero no suficiente) para superar la asignatura entregar todos los informes de laboratorio y que la suma de las calificaciones del bloque (LAB) alcance 1,25 puntos sobre la calificación global de la asignatura (10 puntos).
	Test del laboratorio.	5%	Es condición necesaria (pero no suficiente) para superar la asignatura y que la suma de las calificaciones del bloque (LAB) alcance 0,5 puntos sobre la calificación global de la asignatura (10 puntos).

CRITERIOS DE CALIFICACIÓN
• **Convocatoria ordinaria:**

Los alumnos que no alcancen la mínima calificación exigida en cada una de las partes (LAB y EXA) tendrán una calificación global (sobre 10 puntos) igual a la de la menor calificación de las partes de la asignatura en las que no alcanzan el mínimo exigido.

Para superar la asignatura en la convocatoria ordinaria los alumnos deben superar:

(EXA) El examen escrito (problemas + teoría).

(LAB) La evaluación del laboratorio (informes + test).

- **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) en las condiciones que se indican a continuación. 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) en las condiciones que se indican a continuación.
- 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.

Todos los alumnos que tengan que recuperar la parte de (LAB) en la convocatoria extraordinaria deben realizar el test de laboratorio. Además, la realización de nuevos informes de laboratorio será obligatoria o voluntaria según las siguientes condiciones:

- Los alumnos que no hayan presentado alguno de los informes de laboratorio en la convocatoria ordinaria *deben* presentarlo en la extraordinaria.
- Los alumnos que hayan suspendido algún informe (han obtenido menos de la mitad de la nota máxima en ese informe) *pueden* presentarlo de nuevo (sin necesidad de asistir al laboratorio), de acuerdo con el enunciado de la convocatoria ordinaria. La nueva nota sustituirá a la anterior, sea mejor o peor. La fecha límite para esta entrega es el día del examen extraordinario, justo antes de comenzarlo.

8. Consideraciones finales

Adenda a la Guía Docente de la asignatura

A4. 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: 0.7

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

Carga de trabajo en créditos ECTS: 2.6

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

Carga de trabajo en créditos ECTS: 2.6

c. Contenidos Adaptados a formación online

Los contenidos son los mismos indicados previamente en el aparado 4.c.

d. Métodos docentes online

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

- Entorno de trabajo en la plataforma Moodle ubicado en el Campus Virtual de la Universidad de Valladolid.
- Documentación de apoyo ampliada.
- Clases grabadas en modo vídeo con los conceptos básicos de cada tema.
- Material de apoyo para la realización y resolución de ejercicios prácticos.
- Colección de recursos audiovisuales de apoyo para cada tema.
- Para la docencia de prácticas en Laboratorio, se empleará el método de docencia inversa, de forma que el alumno revisa con anterioridad el material docente puesto a su disposición por el profesor, y se realizan sesiones síncronas por videoconferencia donde se resuelven dudas.

e. Plan de trabajo online

Véase el Anexo I.

f. Evaluación online

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, realizados por los alumnos en grupos de dos personas.

- Examen Parcial: Prueba escrita al final del bloque, el examen consistirá en una serie de cuestiones realizadas a través de la plataforma Moodle del Campus Virtual, que el alumno ha de resolver en un tiempo prefijado y que permiten evaluar el grado de comprensión de los conceptos fundamentales del temario de la asignatura. Incluye una parte de teoría, y otra de laboratorio.

i. Temporalización

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.	0.7 ECTS	Semanas 1 a 2
Bloque 2: Criptografía. Tipos de cifrado. Infraestructura de clave pública.	2.6 ECTS	Semanas 2 a 7
Bloque 3: Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.	2.6 ECTS	Semanas 7 a 13

A5. Métodos docentes y principios metodológicos

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 ampliada.
- Acceso a los ordenadores del laboratorio a través de servidor virtual de sesiones. Este acceso estará disponible en las horas prefijadas para laboratorio en los horarios del centro.
- Herramienta OpenSSL, PILAR que los alumnos pueden instalar en su PC para trabajar desde casa.
- Clases grabadas en modo vídeo con los conceptos básicos de cada tema.
- Material de apoyo para la realización y resolución de ejercicios prácticos.
- Material de apoyo para la realización y resolución de las prácticas en laboratorio. Tutoriales guiados.
- Colección de recursos audiovisuales de apoyo para cada tema.

A6. Tabla de dedicación del estudiante a la asignatura

En el caso de docencia online, la tabla de dedicación del estudiante a la asignatura será equivalente a la de la guía docente. Únicamente las actividades presenciales pasan a ser a distancia con la misma distribución de horas. Dichas actividades podrán ser síncronas o asíncronas en función de las restricciones impuestas por las autoridades competentes.

ACTIVIDADES PRESENCIALES A DISTANCIA[2]	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	38
Laboratorios (L)	17		
Prácticas externas, clínicas o de campo	0		
Seminarios (S)	10		
Tutorías grupales (TG)	0		
Evaluación (fuera del periodo oficial de exámenes)			
Total presencial	**52**	**Total no presencial**	**98**
		TOTAL presencial + no presencial	**150**

(2) Actividad presencial a distancia en este contexto es cuando el grupo sigue por videoconferencia la clase impartida por el profesor en el horario publicado para la asignatura.

A7. Sistema y características de la evaluación

Criterio: cuando más del 50% de los días lectivos del cuatrimestre transcurran en situación de contingencia, se asumirán como criterios de evaluación los indicados en la adenda.

BLOQUE	INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
EXA	Examen Parcial al finalizar cada Bloque. El examen consistirá en una serie de cuestiones realizadas a través de la plataforma Moodle del Campus Virtual, que el alumno ha de resolver en un tiempo prefijado y que permiten evaluar el grado de comprensión de los conceptos fundamentales del temario de la asignatura. Estas cuestiones abarcarán los contenidos trabajados en la asignatura. Parte de teoría y problemas. En caso de no aprobar (5.0) con los exámenes parciales, será necesario realizar un examen final de toda la asignatura.	70%	Es condición necesaria (pero no suficiente) para superar la asignatura alcanzar una calificación igual o superior a 3 puntos sobre la calificación global de la asignatura (10 puntos).
LAB	Informes de las sesiones de laboratorio.	25%	Es condición necesaria (pero no suficiente) para superar la asignatura entregar todos los informes de laboratorio y que la suma de las calificaciones del bloque (LAB) alcance 1,25 puntos sobre la calificación global de la asignatura (10 puntos).
	Test del laboratorio.	5%	Es condición necesaria (pero no suficiente) para superar la asignatura y que la suma de las calificaciones del bloque (LAB) alcance 0,5 puntos sobre la calificación global de la asignatura (10 puntos).

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**
  Los alumnos que no alcancen la mínima calificación exigida en cada una de las partes (LAB y EXA) tendrán una calificación global (sobre 10 puntos) igual a la de la menor calificación de las partes de la asignatura en las que no alcanzan el mínimo exigido.
  Para superar la asignatura en la convocatoria ordinaria los alumnos deben superar:
  (EXA) El examen escrito (problemas + teoría).
  (LAB) La evaluación del laboratorio (informes + test).
- **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) en las condiciones que se indican a continuación. 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) en las condiciones que se indican a continuación.
  - 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.

  Todos los alumnos que tengan que recuperar la parte de (LAB) en la convocatoria extraordinaria deben realizar el test de laboratorio. Además, la realización de nuevos informes de laboratorio será obligatoria o voluntaria según las siguientes condiciones:
  - Los alumnos que no hayan presentado alguno de los informes de laboratorio en la convocatoria ordinaria *deben* presentarlo en la extraordinaria.
  - Los alumnos que hayan suspendido algún informe (han obtenido menos de la mitad de la nota máxima en ese informe) *pueden* presentarlo de nuevo (sin necesidad de asistir al laboratorio), de acuerdo con el enunciado de la convocatoria ordinaria. La nueva nota sustituirá a la anterior, sea mejor o peor. La fecha límite para esta entrega es el día del examen extraordinario, justo antes de comenzarlo.