UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2022/23*

51203 - CIBERSEGURIDAD EN REDES

CENTRO: *415 - IU de Microelectrónica Aplicada*
TITULACIÓN: *5048 - MU Electrónica y Telecomunicación Aplicadas*
ASIGNATURA: *51203 - CIBERSEGURIDAD EN REDES*
CÓDIGO UNESCO: *3304.99* **TIPO:** *Optativa* **CURSO:** *1* **SEMESTRE:** *2º semestre*
CRÉDITOS ECTS: *4,5* **Especificar créditos de cada lengua:** **ESPAÑOL:** *4,5* **INGLÉS:** *0*

SUMMARY

Cybersecurity is a main concern nowadays, not just for companies and institutions but also for individuals who see their privacy or even their money and physical security in risk. Privacy, attacks, vulnerabilities, malware, cyberwar, cryptocurrencies, etc are already familiar concepts in nowadays life. We all relay on Internet and technology for almost everything making our lifes easier and better, but also making it possible for attackers to act remotely and access a wider range of targets with less risk.
Knowledge in this field is highly valued being one of the most in demand professions nowadays.

Throughout this course, we will try to describe the problems and attacks that can occur in the software, in the hardware itself, or simply taking advantage of vulnerabilities in the protocols. Of course we will dive into cryptographic algorithms and protocols and security countermeasures against different types of attacks. There are many systems that, despite using cryptographic techniques to protect them, have been broken by design errors and security breaches in the implementation. That is why it is essential for any professional who is going to dedicate himself to this field, both professionally and from a research point of view, to know the correct techniques of implementation of these algorithms as well as to know the state of the art in relation to the cryptanalysis and different attacks that arise continuously in this field.

At the end of the course, the student should be able to handle security concepts such as authentication, encryption, electronic signature, the use of electronic certificates, data protection, risk management, network server protection, etc. The student should also know the main technical standards and legislation in this field.

REQUISITOS PREVIOS

Conocimientos básicos de programación

Plan de Enseñanza (Plan de trabajo del profesorado)

Contribución de la asignatura al perfil profesional:

La seguridad es una materia que afecta de forma transversal a casi todas las demás materias del Master y los conocimientos en este campo son cada vez más valorados e incluso exigidos en muchos perfiles profesionales. Cabe destacar la existencia de certificaciones a nivel internacional como CISSP, CISM, CISA, CCSP, etc que son muy valoradas por las empresas a la hora de contratar personal cualificado. Esta asignatura pretender abarcar los temas más importantes que se

imparten en estas certificaciones así como sensibilizar al alumno en la importancia de incorporar al menos un análisis de seguridad en todos los desarrollos para identificar posibles debilidades y evaluar los posibles riesgos. No siempre es obligatorio establecer mecanismos de seguridad pero si lo es conocer los posibles riesgos para poder tomar decisiones bien fundadas.

Competencias que tiene asignadas:

CG2 - Que los estudiantes conozcan y sean capaces de analizar desde un punto de vista crítico y analítico las técnicas para el diseño de sistemas en el ámbito de la ingeniería electrónica y de telecomunicación avanzada.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CE13 - Ser capaz de analizar el nivel de seguridad requerido en múltiples entornos, especialmente en redes telemáticas y de comunicaciones electrónicas, ofreciendo soluciones hardware y software viables para su implantación eficaz.

Objetivos:

Obj 1. Evaluar adecuadamente los riesgos y el coste asociado a los mismos y ser capaz de diseñar esquemas de seguridad adaptados a las necesidades concretas de un sistema dado.
Obj 2. Entender la importancia de la seguridad y la privacidad, tanto a nivel profesional como personal
Obj 3. Conocer qué es y como se diseña un plan de contingencia
Obj 4. Entender la importancia del factor humano en el diseño de un sistema de seguridad
Obj 5. Conocer los principales problemas existentes en el desarrollo software en relación a la seguridad y cómo se pueden evitar.
Obj 6. Conocer los principales mecanismos de identificación personal y de control de acceso así como su aplicación a entornos online.
Obj 7. Conocer los conceptos básicos de criptografía para su aplicación en el entorno de las Telecomunicaciones.
Obj 8. Conocer las debilidades de los protocolos y sistemas de comunicaciones actuales así como las medidas necesarias para protegerlos frente a estos ataques.
Obj 9. Capacidad de aplicar los protocolos de seguridad en función de las necesidades específicas de cada sistema basado en comunicaciones en red.
Obj 10. Conocer y saber aplicar las infraestructuras de clave pública (PKI).
Obj 11. Conocer la legislación y normativa vigente relacionada con la seguridad y en particular todo lo relacionado con la firma electrónica.

Contenidos:

Bloque Temático 1: Conceptos básicos de seguridad (6 horas de Teoría)
Arquitectura de seguridad e ingeniería
Seguridad de la Información y Gestión de Riesgos
El factor humano en la seguridad

Competencias del bloque: CG2, CB6, CB7, CE13
Objetivos del bloque: OBJ-1, OBJ-2, OBJ-3, OBJ-4

Bloque Temático 2: Criptografía y su aplicación en sistemas complejos (10 horas de Teoría y 2 horas de Aula)
- Criptografía y protocolos de comunicación seguros
- Tokens criptográficos y hardware específico para seguridad
- Seguridad en pagos electrónicos y criptomonedas

Competencias del bloque: CG2, CB6, CB7, CE13
Objetivos del bloque: OBJ-7, OBJ-8, OBJ-9, OBJ-10

Bloque Témático 3: Seguridad en campos específicos (9 horas de Teoría y 6 horas de Aula)
- Gestión de identidad y control de acceso
- Seguridad en el software
- Seguridad en dispositivos móviles e IoT
- seguridad en las comunicaciones
- Seguridad perimetral
- Auditorías de seguridad y análisis forense

Competencias del bloque: CG2, CB6, CB7, CE13
Objetivos del bloque: OBJ-5, OBJ-6

Bloque Temático 4: Legislación y normativa (3 horas de Teoría, 2 horas de evaluación y 7 horas de practicas)
- Legislación, normativa y certificaciones de seguridad

Competencias del bloque: CG2, CB6, CB7, CB9, CE13
Objetivos del bloque: OBJ-11

Metodología:

Método expositivo/Lección magistral. Enseñanza directa expositiva y demostrativa para aquellos contenidos esenciales y/o que requieran una explicación detallada por parte del profesor.
Actividades prácticas. Actividades presenciales que requieren la transferencia de conocimientos conceptuales con los procedimentales, favoreciendo la autonomía y la capacidad de reflexión de los estudiantes, así como fomentando las habilidades personales, y las interpersonales mediante el trabajo en equipo.
Trabajos, proyectos y memorias. Realización y/o exposición individual o en grupo de trabajos monográficos sobre la asignatura.
Actividades no presenciales: destinadas al fomento del estudio y al desarrollo por parte del alumno de las competencias de trabajo autónomo y de autoaprendizaje.
Exámenes. Realización de exámenes parciales y/o finales correspondientes a las distintas asignaturas del plan de estudios.

Evaluacion:

Criterios de evaluación

Las dos partes de que consta la asignatura (teoría y prácticas) se evalúan por separado, si bien en ambas partes se intenta abarcar todas las competencias (CG2, CB6, CB7, CB9 y CE13)
Para evaluar la parte teórica se realizará un examen escrito y se combinará con ejercicios en clase que fomenten la participación de los alumnos así como su iniciativa.
La parte práctica se evaluará en base a la elaboración, presentación y defensa de las prácticas.
Sistemas de evaluación

La evaluación se re realiza, principalmente, a través de un examen y de la realización, redacción, presentación y discusión de un trabajo sobre un tema relacionado con cualquiera de los aspectos de la investigación tratados en la asignatura. El trabajo tutelado podrá tener un enfoque teórico o un enfoque práctico, dependiendo de los intereses del estudiante y de la naturaleza del trabajo. En función de la complejidad del trabajo se decidirá si éste se realiza y se presenta de forma individual o en grupos. Para la superación de la asignatura será necesario:
• Realizar el trabajo tutelado indicado por el profesor.
• Entregar al profesor una memoria escrita que contenga, al menos, los siguientes apartados: introducción, estado del arte, análisis del problema, soluciones planteadas y conclusiones obtenidas.
• Realizar una presentación dirigida al profesor y al resto de estudiantes de la asignatura en la cual se resuman los aspectos más relevantes contenidos en la memoria.
• Responder a las preguntas que surjan a modo de debate a partir de la presentación realizada por parte del profesor y de los estudiantes.
Sistema de calificación:
- La asistencia y participación en clase se valorarán hasta un 10% de la nota total.
- Examen de teoría: El examen teórico tiene una valoración de un 50% de la nota total.
- Prácticas: La nota de la parte práctica será la media de las notas de todas las prácticas, contribuyendo un 10% de la nota total.
- El trabajo de curso contribuye un 30% a la nota total.

A la hora de realizar la evaluación, se tendrán en cuenta los criterios que se describen a continuación relativos al trabajo, a la memoria, a la presentación y al debate.
Relativos al trabajo:
• Grado de consecución de los objetivos planteados.
• Originalidad de la solución propuesta.
• Grado de autonomía en el desarrollo del trabajo.
• Viabilidad de las soluciones aportadas.
Relativos a la memoria:
• Organización de la memoria clara y adecuada a la temática del trabajo tutelado.
• Calidad de la redacción de la memoria en términos de expresión escrita.
• Completitud y actualidad del estado del arte aportado.
• Análisis adecuado del problema a resolver.
• Validez del análisis crítico y de las conclusiones extraídas.
Relativos a la presentación:
• Organización de la presentación clara y adecuada a la temática del trabajo tutelado.
• Calidad de la presentación en términos de la expresión oral utilizada.
• Calidad visual de la presentación.
• Destreza en el uso de los recursos empleados en la presentación.
Relativos al debate:
• Grado de aclaración a las preguntas realizadas.
• Grado de precisión en las respuestas a las preguntas realizadas.
• Dominio de la terminología usada en las respuestas.
Criterios de calificación

Sistema de calificación
Teoría:
- Asistencia a clase: La asistencia a clase se valorará hasta un 10% de la nota de teoría, debiendo asistir al menos a un 80% de las clases y participar activamente en las clases.
- Examen de teoría: El examen teórico tiene una valoración de un 50% de la nota de
teoría. Para aprobar la asignatura se requiere haber obtenido al menos una puntuación de 5 sobre 10 en este examen.

- Realización de prácticas en laboratorio: 10%
- Trabajo de curso: Los alumnos deberán elaborar un trabajo sobre un tema específico de la asignatura, presentarlo y defenderlo en clase. Este trabajo tendrá una valoración de un 30% de la nota (20% la redacción del trabajo y un 10% la presentación del mismo).

Prácticas: La nota de la parte práctica será la media de las notas de todas las prácticas.
A la hora de realizar la evaluación, se tendrán en cuenta los criterios que se describen a continuación relativos al trabajo, a la memoria, a la presentación y al debate.
Relativos al trabajo:
• Grado de consecución de los objetivos planteados.
• Originalidad de la solución propuesta.
• Grado de autonomía en el desarrollo del trabajo.
• Viabilidad de las soluciones aportadas.
Relativos a la memoria:
• Organización de la memoria clara y adecuada a la temática del trabajo tutelado.
• Calidad de la redacción de la memoria en términos de expresión escrita.
• Completitud y actualidad del estado del arte aportado.
• Análisis adecuado del problema a resolver.
• Validez del análisis crítico y de las conclusiones extraídas.
Relativos a la presentación:
• Organización de la presentación clara y adecuada a la temática del trabajo tutelado.
• Calidad de la presentación en términos de la expresión oral utilizada.
• Calidad visual de la presentación.
• Destreza en el uso de los recursos empleados en la presentación.
Relativos al debate:
• Grado de aclaración a las preguntas realizadas.
• Grado de precisión en las respuestas a las preguntas realizadas.
• Dominio de la terminología usada en las respuestas.

Plan de Aprendizaje (Plan de trabajo de cada estudiante)

Tareas y actividades que realizará según distintos contextos profesionales (científico, profesional, institucional, social)

Las tareas y actividades estarán enfocadas hacia el aprendizaje mediante experimentación, análisis y discusión para llegar a soluciones adecuadas para distintos entornos.

Contexto científico: Estudio de los avances en criptografía y seguridad
Contexto profesional: Desarrollo de sistemas y políticas de seguridad para entornos empresariales o privados.
Contexto institucional y social: Estudio de aplicaciones e implementaciones prácticas contextualizando los conocimientos adquiridos en el ámbito social, local y global.

Temporalización semanal de tareas y actividades (distribución de tiempos en distintas actividades y en presencialidad - no presencialidad)

La asignatura consta de 4.5 créditos ECTS de los cuales 1.8 créditos (45 horas) son presenciales y 2.7 créditos (67.5 horas) se corresponderán al estudio del alumno.

Las horas presenciales se realizarán a 3 horas por semana que combinarán la parte teórica y práctica en función de los temas a tratar en cada momento.

Bloque Temático 1: Conceptos básicos de seguridad
Semanas de la 1 a la 2
Bloque Temático 2: Criptografía y su aplicación en sistemas complejos
Semanas de la 3 a la 7
Bloque Temático 3: Seguridad en campos específicos
Semanas de la 8 a la 12
Bloque Temático 4: Legislación y normativa
Semanas de la 13 a la 15

	Presencial					No Presencial				
Semanas	CLT	CPA	LAB	Eva	T.P	NP1	NP2	NP3	NP4	NP5	T.NP
Semana 1	3	0	0	0	3	0	2.5	0	0	0	2.5
Semana 2	3	0	0	0	3	0	3	0	0	0	3
Semana 3	2	1	0	0	3	0	3	0	0	0	3
Semana 4	2	1	0	0	3	0	3	0	0	0	3
Semana 5	0	3	0	0	3	0	0	0	0	0	3
Semana 6	3	0	0	0	3	0	0	0	0	0	3
Semana 7	2	1	0	0	3	0	0	0	0	0	3
Semana 8	2	1	0	0	3	0	0	0	0	0	3
Semana 9	2	1	0	0	3	0	0	0	0	0	3
Semana 10	3	0	0	0	3	0	0	0	0	0	3
Semana 11	3	0	0	0	3	0	0	0	0	0	3
Semana 12	3	0	0	0	3	0	0	0	0	0	3
Semana 13	0	0	1	2	3	0	1	3	0	0	4
Semana 14	0	0	3	0	3	0	1	3	0	0	4
Semana 15	0	0	3	0	3	0	1	3	0	0	4
Semana 16	0	0	0	0	0	0	1	3	0	0	4
Semana 17	0	0	0	0	0	0	0	4	0	0	4
Semana 18	0	0	0	0	0	0	0	4	0	0	4
Semana 19	0	0	0	0	0	0	0	4	0	0	4
Semana 20	0	0	0	0	0	0	0	4	0	0	4
Total	28	8	7	2	45	0	39,5	28	0	0	67.5

Actividades Presenciales
CLT: Clase teórica
CPA: Clase práctica de aula
LAB: Laboratorio
Tut: Tutoría
Eva: Evaluación
Actividades No Presenciales
NP1: Trabajo teórico
NP2: Estudio teórico
NP3: Trabajo práctico
NP4: Estudio práctico
NP5: Actividades complementarias

Recursos que tendrá que utilizar adecuadamente en cada uno de los contextos profesionales.

Los recursos necesarios para esta asignatura consistitán en el material bibliográfico, documentación adicional que será accesible a través del campus virtual y el equipamiento hardware y software disponible en el laboratorio de Redes de Area Local, Extensa y RDSI.

Resultados de aprendizaje que tendrá que alcanzar al finalizar las distintas tareas.

Al final de la asignatura, el alumno deberá manejar con soltura los conceptos de seguridad, tales como autenticación, cifrado, firma electrónica, el uso de certificados electrónicos, la protección de datos, gestión del riesgo, la protección de servidores en red, etc. También deberá conocer los principales estándares técnicos y legislación aplicable en este campo.

Plan Tutorial

Atención presencial individualizada (incluir las acciones dirigidas a estudiantes en 5ª, 6ª y 7ª convocatoria)

Se usará para aclarar dudas, asesorar al estudiante en las tareas individuales y optimizar su rendimiento. El profesor atenderá consultas del alumnado en su horario de tutorías. Las citas se pueden concertar a través del correo electrónico institucional o utilizando las herramientas proporcionadas por el Campus Virtual. Los estudiantes en 5ª, 6ª y 7ª convocatoria tendrán prioridad frente al resto de compañeros en el horario de tutoría del profesor.

Atención presencial a grupos de trabajo

Semanalmente, se harán reuniones de seguimiento de los trabajos y prácticas de los alumnos. En función del carácter específico de los trabajos en curso se plantearán reuniones en grupo o individuales.

Atención telefónica

El profesor de la asignatura estará disponible via telefónica para cuestiones puntuales que le pudieran surgir al estudiante en su labor de trabajo personal.

Atención virtual (on-line)

El profesor de la asignatura estará disponibles a través de correo electrónico o en el Campus Virtual de la ULPGC.

Datos identificativos del profesorado que la imparte.

Datos identificativos del profesorado que la imparte

Dr./Dra. Fernando De la Puente Arrate *(COORDINADOR)*

Departamento: *238 - INGENIERÍA TELEMÁTICA*

Ámbito: *560 - Ingeniería Telemática*

Área: *560 - Ingeniería Telemática*

Despacho: *INGENIERÍA TELEMÁTICA*

Teléfono: *928458048* **Correo Electrónico:** *fernando.puente@ulpgc.es*

Bibliografía

[1 Básico] CISSP training kit /

David R. Miller.

O'Reilly Media,, Sebastopol, California : (2013)

978-0-7356-5782-3

[2 Básico] Metasploit para Pentesters /

Pablo González Pérez, Chema Alonso.
0xWORD,, Madrid : (2018) - (4{486}. ed. rev. y ampl.)
978-84-697-6034-5

[3 Básico] Applied cryptography: protocols,algorithms and source code in C.

Schneier, Bruce
John Wiley & Sons,, Chichester : (1996) - (2nd. ed.)
0471117099

[4 Básico] CISSP All-in-One Exam Guide, Eighth Edition

Shon Harris
- (2018)
978-1260142655

[5 Recomendado] Authentication systems for secure networks.

Oppliger, Rolf
Artech House,, Boston : (1996)
0890065101