ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2021/2022

Máster en Ingeniería Informática (Plan 2018)

DATOS DE LA ASIGNATURA			
Nombre:			
Seguridad en Comunicaciones e Infraestructuras			
Denominación en inglés:			
Security in Communications and Infrastructures			
Código:		**Carácter:**	
1180421		Optativo	
Horas:			
	Totales	**Presenciales**	**No presenciales**
Trabajo estimado:	75	30	45
Créditos:			
	Grupos reducidos		
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
2.07	0	0.93	0	0
Departamentos:		**Áreas de Conocimiento:**	
Ingeniería Electrónica, de Sistemas Informáticos y Automática		Ingeniería de Sistemas y Automática	
Ingeniería Electrónica, de Sistemas Informáticos y Automática		Tecnología Electrónica	
Curso:		**Cuatrimestre:**	
1º - Primero		Segundo cuatrimestre	

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Mateo Sanguino, Tomás de Jesús	tomas.mateo@diesia.uhu.es	959217665	P258 / Escuela Técnica Superior de Ingeniería / Campus del Carmen

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

Introducción a la ciberseguridad. Conceptos sobre vulnerabilidades, amenazas y técnicas de ataque. Protección de datos y privacidad. Protección contra ataques y malware. Contramedidas para la confidencialidad, integridad y disponibilidad de la información. Planes de respuesta y recuperación de desastres. Fortificación de infraestructuras. Reglas de conducta y leyes.

1.2. Breve descripción (en inglés):

Introduction to cybersecurity. Concepts about vulnerabilities, threats and attack techniques. Data protection and privacy. Protection against attacks and malware. Countermeasures for confidentiality, integrity and availability of information. Response and disaster recovery plans. Fortification of infrastructures. Rules of conduct and laws.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

La asignatura "Seguridad en Comunicaciones e Infraestructuras" es una materia que forma parte del bloque de asignaturas optativas y se imparte en el segundo cuatrimestre (2C) del Máster de Ingeniería Informática. La asignatura pertenece al itinerario de"Ciberseguridad", cuyo contenido se basa en el curso "Cibersecurity Essentials" de Cisco.
Nota: la certificación profesional "Cibersecurity Essentials" puede obtenerse cursando la asignatura sin requisito previo.

2.2. Recomendaciones:

No existen requisitos de conocimiento previo dado que el contenido de la asignatura está estructurado de tal forma que comienza con una introducción a la ciberseguridad y continúa con conocimientos avanzados. No obstante, se recomienda haber cursado las asignaturas impartidas en el Grado de Ingeniería Informática:

- Fundamentos de Redes de Computadores
- Interconexión de Redes de Computadores
- Administración y Gestión de Redes de Computadores
- Redes Avanzadas
- Seguridad en Redes

También se recomienda haber adquirido el conocimiento equivalente a través de las certificaciones de Cisco:

- CCNA R&S
- CCNA Security
- Introduction to Cibersecurity

3. Objetivos (Expresados como resultados del aprendizaje):

Con esta asignatura el alumno aprende los aspectos de la seguridad relacionados con el uso de infraestructuras corporativas tales como la importancia de la ciberseguridad, confidencialidad de los datos, prácticas sobre el uso de Internet y las redes sociales, seguridad física y de la información, impacto de ciberataques en redes y sistemas, tecnologías, procedimientos, defensa y mitigación de ataques.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

4.2. Competencias básicas, generales o transversales:

- **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
- **CB10:** Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
- **CG1:** Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática
- **CG2:** Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio
- **CG3:** Dirigir, planificar y supervisar equipos multidisciplinares
- **CG5:** Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería Informática siguiendo criterios de calidad y medioambientales
- **CG6:** Capacidad para la dirección general, dirección técnica y dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, en el ámbito de la Ingeniería Informática
- **CG8:** Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos
- **CT1:** Gestionar adecuadamente la información adquirida expresando conocimientos avanzados y demostrando, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en el campo de estudio.
- **CT2:** Dominar el proyecto académico y profesional, habiendo desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con un alto componente de transferencia del conocimiento.
- **CT3:** Desarrollar una actitud y una aptitud de búsqueda permanente de la excelencia en el quehacer académico y en el ejercicio profesional futuro.

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Las actividades formativas se dividen en presenciales y no presenciales.
Dentro de las actividades formativas presenciales se contemplan:

- Sesiones de exposición de teoría, problemas o casos prácticos sobre los contenidos del programa (6 horas)
- Sesiones prácticas en laboratorios especializados o en aulas de informática (6 horas)
- actividades académicamente dirigidas por el profesorado como seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, etc. (2 horas)
- Actividades de evaluación (1 hora)

Dentro de las actividades formativas no presenciales se incluyen:

- Lectura de los contenidos teórico-prácticos de los temas (12 horas)
- Entrega de ejercicios, prácticas o trabajos evaluables (2 horas)
- Actividades de autoevaluación (5 horas)
- Tutorías colectivas a través de plataformas de enseñanza virtual como foros, wikis o chats (5 horas)
- Trabajo individual/autónomo del estudiante (30 horas)
- Actividades con evaluación por pares (3 horas)
- Desarrollo cooperativo de trabajos utilizando herramientas de discusión asíncrona como foros o wikis (3 horas)

Las metodologías docentes se dividen en presenciales y no presenciales:
Dentro de las metodologías docentes presenciales se incluyen:

- Clase magistral participativa
- Desarrollo de prácticas en laboratorios especializados o en aulas de informática en grupos reducidos
- Tutorías individuales o colectivas con interacción directa entre profesorado-estudiantes
- Planteamiento, realización, tutorización y presentación de trabajos
- Evaluaciones y exámenes

Dentro de las metodologías docentes no presenciales se incluyen:

- Visualización y escucha de grabaciones con entrevistas a expertos en algunos temas claves de la materia o vídeos seleccionados que incentiven algunas competencias
- Tutorías en línea con utilización de foros y otros medios de comunicación/interacción con el profesorado
- Trabajos colaborativos consistentes en llevar a cabo una actividad basada en un objetivo común en el que el estudiante debe colaborar activamente para realizarla
- Metodologías basadas en la acción tales como revisión y planificación de las mejoras de trabajos con participación de estudiantes y profesorado

6. Temario desarrollado:

Capítulo 1. El Mundo de la Ciberseguridad
Delincuentes, especialistas, amenazas (ámbitos y sofisticación), comunidades.
Capítulo 2. Destrezas en Ciberseguridad
Principios, estado de los datos y medidas, confiabilidad, integridad y disponibilidad, contramedidas (tecnologías, formación y políticas), modelo ISO.
Capítulo 3. Amenazas, Vulnerabilidades y Ataques a la Ciberseguridad
Malware y código malicioso (tipos, ataques a correo y navegadores), ingeniería social, tipos de ataques (DoS, spoofing, man-in-the-middle, día cero, registro del teclado), ataques a aplicaciones (scripting, inyección de código, desbordamiento del búfer, ejecuciones remotas, ActiveX y Java).
Capítulo 4. Métodos de Protección
Criptografía (clave pública, clave privada, simetría y asimetría), controles de acceso (estrategias, identificación, autenticación, autorización y controles), ocultamiento de datos (enmascaramiento, esteganografía y ofuscación).
Capítulo 5. Integridad
Controles de integridad de datos (algoritmos hash, salting y HMAC), firmas digitales (ley y tecnología), certificados (aspectos básicos y creación), integridad de la base de datos (validación y requisitos).
Capítulo 6. Alta Disponibilidad
Diseño, mejora de la disponibilidad (administración, defensa, redundancia y recuperabilidad), respuesta ante incidentes, recuperación ante desastres (planificación de la recuperación y de la continuidad).
Capítulo 7. Protección Corporativa
Defensa de sistemas y dispositivos (protección del host y protección física), protección de servidores (acceso remoto seguro y medidas administrativas), protección de la red (equipos de voz y video), seguridad física (control de acceso físico y vigilancia).
Capítulo 8. Herramientas, Legalidad y Organismos de Seguridad
Ética y principios rectores, responsabilidad y leyes, organismos de seguridad, armas de ciberseguridad (escáneres, pruebas de penetración, analizadores y herramientas).

7. Bibliografía

7.1. Bibliografía básica:

- Cybersecurity Essentials. Autores: Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short. Ed. Sybex, 2018 784. ISBN: 978-1-119-36239-5
- CCNP Security Secure 642-637 Official Cert Guide. Autores: Sean Wilkins, Franklin H. Smith III. Ed. Cisco Press.

7.2. Bibliografía complementaria:

- Seguridad informática - Ethical Hacking. Autores: Marion AGÉ et. al. Ed. ENI
- Hacking y Seguridad en Internet. Edición 2011. Autores: Garcia-Moran, Jean Paul et. al. Ed. RA-MA.
- Hacker. Edición 2012, Ed. Anaya.
- Internal Hacking y Contramedidas en Entorno Windows, Kapfer, Philippe. Ed. ENI

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos

8.2. Criterios de evaluación y calificación:

El sistema de evaluación continuo diseñado para las convocatorias ordinarias I, II, III y la extraordinaria para finalización del título es el siguiente:

- Examen de teoría/problemas (40%)
- Pruebas de evaluación mediante plataformas de enseñanza virtual (35%)
- Participación en actividades propuestas (25%)

Aquellos alumnos que lo consideren, podrán acogerse a la evaluación final única en todas las convocatorias siguiendo la normativa establecida en el Reglamento de Evaluación para las Titulaciones de Grado y Máster Oficial de la Universidad de Huelva aprobado por Consejo de Gobierno. La evaluación única consistirá en tres pruebas:

1. Examen de teoría/problemas (40%)
2. Pruebas de evaluación mediante plataformas de enseñanza virtual (35%)
3. Participación en actividades propuestas (25%)

El alumno que se acoja a la evaluación final única deberá comunicarlo al profesorado responsable de la asignatura a través de su cuenta de correo electrónico de la Universidad de Huelva. Dicho profesor asignará la práctica de laboratorio correspondiente con peso equiparable al de la evaluación continua de la asignatura. La evaluación única se realizará en un aula de la Universidad de Huelva dentro del período de exámenes y tendrá una duración de 4 horas. El material didáctico para la preparación de las pruebas será el que se incluya en el Campus Virtual de la asignatura y el recogido en la bibliografía básica de esta guía docente. Las herramientas necesarias consitirán en medios físicos (papel) y medios informáticos (PC con simulador Packet Tracer).

Las competencias que se evaluarán tanto en el sistema de evaluación continuo como en la evaluación final única son las siguientes:

- Examen de teoría/problemas, defensa de trabajos e informes escritos, participación en actividades propuestas: competencias específicas (CETI1-CETI3) adquiridas en relación al temario incluido en esta guía docente
- Entrega de memorias y/o defensa de prácticas: competencias básicas (CB6-CB10), generales (CG1-CG8) y transversales (CT1-CT3) adquiridas en relación al temario incluido en esta guía docente

El examen de teoría/problemas constará de una prueba teórica formada por un cuestionario de 30 preguntas de tipo test. El examen se corregirá sobre un máximo de 10 puntos. Cada pregunta incorrecta resta una pregunta correcta, siendo necesario contestar el total de cuestiones planteadas para corregir el examen. No se requiere una nota mínima de corte para aplicar la media con las otras pruebas de la asignatura. En caso de obtener una nota negativa en el examen, esta se restará del resto de pruebas al aplicar la media.

La participación en actividades propuestas consistirá en una actividad académica dirigida (AAD). El periodo de tiempo se divide en una fase inicial de entrega de 3 semanas, tras la cual el profesor realizará un proceso de revisión y propondrá al alumno cambios para mejorar la calificación. Ello se podrá realizar durante una segunda fase de entrega de 1 semana adicional. En caso de no entregar la AAD dentro de las 3 primeras semanas, el alumno no recibirá la revisión del trabajo y obtendrá la calificación correspondiente sin posibilidad de mejora. Superado el plazo de 4 semanas, el alumno podrá seguir trabajando en la AAD hasta el día del examen. Cada semana de retraso restará 1 punto a la nota de la actividad. La nota de la AAD se evaluará sobre un máximo de 10 puntos y la asistencia a clase para la elaboración de AAD es obligatoria.

Las pruebas de evaluación mediante plataformas de enseñanza virtual consistirán en prácticas de laboratorio con los siguientes requisitos:

- Asistencia obligatoria (se permitirá un máximo de 2 faltas sin justificar)
- Mostrar individualmente al profesor el correcto funcionamiento de la solución elegida para cada una de las prácticas, así como responder correctamente a las preguntas que este tenga a bien formularle
- No se requiere la elaboración de memorias, salvo que el alumno no asista a la defensa de sus prácticas. En ese caso, deberá realizar una memoria donde se detallen las distintas cuestiones a resolver y la solución obtenida para cada unade ellas
- Cada práctica deberá entregarse en un plazo de 2 semanas desde la propuesta de su enunciado y se evaluará sobre un máximo de 10 puntos. A partir del plazo, cada semana restará 1 punto en la nota de la práctica. La nota de las prácticas se establecerá en función de las respuestas a las preguntas formuladas por el profesor y de las memorias entregadas si fuera el caso.
- Aquellos alumnos que no hayan superado las prácticas podrán realizar un examen de laboratorio en las convocatorias oficiales.
- Aquellos alumnos que por incompatibilidad laboral no puedan asistir a los grupos de laboratorio disponibles, deberán entregar un justificante debidamente firmado y sellado por la empresa indicando el horario laboral.

La mención de Matrícula de Honor podrá ser otorgada a los estudiantes que hayan obtenido una calificación igual o superior a 9,0 puntos. La mención no podrá exceder del 5% de los estudiantes matriculados en la asignatura durante el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola Matrícula de Honor. En caso de equidad, el criterio a seguir para obtener la mención de Matrícula de Honor será la mayor nota en el examen teórico, seguido de la mayor nota obtenida en prácticas de laboratorio, la mayor nota obtenida en la realización de AAD y en último lugar la participación en clase.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	2.97	0	0	1.31	0	Práctica virtual	Tema 1
#2	2.97	0	0	1.31	0	Práctica virtual	Tema 2
#3	2.97	0	0	1.31	0	Práctica virtual	Tema 3 y Tema 4
#4	2.97	0	0	1.31	0	Práctica virtual	Tema 5
#5	2.97	0	0	1.31	0	Práctica virtual	Tema 6
#6	2.97	0	0	1.31	0	Práctica virtual	Tema 7
#7	2.98	0	0	1.34	0	Actividad propuesta	Tema 8
#8	0	0	0	0	0		
#9	0	0	0	0	0		
#10	0	0	0	0	0		
#11	0	0	0	0	0		
#12	0	0	0	0	0		
#13	0	0	0	0	0		
#14	0	0	0	0	0		
#15	0	0	0	0	0		
	20.8	0	0	9.2	0		