ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2018/2019

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**
2.08	0	0.92	0	0

Departamentos:	**Áreas de Conocimiento:**
Ingeniería Electrónica, Sistemas Informáticos y Automática	Ingeniería de Sistemas y Automática
Ingeniería Electrónica, 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	Edif. Torreumbría TUP1-02

*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 los cursos "Introduction to Cibersecurity" y "Cibersecurity Essentials" de Cisco.
Nota: las certificaciones de los cursos "Introduction to Cibersecurity" y "Cibersecurity Essentials" pueden 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 "Fundamentos de Redes de Computadores", "Interconexión de Redes de Computadores", "Administración de Redes de Computadores", "Redes Avanzadas" y "Seguridad en Redes" impartidas en el Grado de Ingeniería Informática. También se recomienda haber adquirido el conocimiento equivalente a través de las certificaciones CCNA R&S y CCNA Security de Cisco.

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 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 de Resolución de Problemas.
- 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.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Conferencias y Seminarios.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Las actividades formativas se dividen en presenciales y no presenciales.
Dentro de las actividades formativas que requieren un 100% de presencialidad 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 que requieren un 100% de presencialidad se incluyen:
- clase magistral participativa
- desarrollo de prácticas en laboratorios especializados o en aulas de informática en grupos reducidos
- resolución de problemas y ejercicios prácticos
- tutorías individuales o colectivas con interacción directa entre profesorado-estudiantes
- planteamiento, realización, tutorización y presentación de trabajos
- conferencias y seminarios
- 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. Necesidad de la Ciberseguridad
Datos personales, datos empresariales, atacantes y profesionales de la ciberseguridad, guerra cibernética.
Capítulo 2. Ataques, Conceptos y Técnicas
Análisis de un ciberataque (vulnerabilidades, tipos de malware y síntomas, métodos de infiltración y DoS), panorama de la ciberseguridad (ataque combinado y reducción del impacto).
Capítulo 3. Protección de Datos y Seguridad Personal
Protección de datos (dispositivos, red y mantenimiento de datos), protección de la privacidad en línea (autenticación y cesión de información).
Capítulo 4. Protección de la Organización
Cortafuegos (tipos, dispositivos, detección en tiempo real, detección de malware y prácticas recomendadas), comportamiento a seguir (Botnet, Kill Chain y NetFlow), enfoque de CISCO (CSIRT, estrategias e IDS/IPS).
Capítulo 5. El Mundo de la Ciberseguridad
Delincuentes, especialistas, amenazas (ámbitos y sofisticación), comunidades.
Capítulo 6. Destrezas en Ciberseguridad
Principios, estado de los datos y medidas, confiabilidad, integridad y disponibilidad, contramedidas (tecnologías, formación y políticas), modelo ISO.
Capítulo 7. 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 8. 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 9. 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 10. 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 11. 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 12. 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:

- Seguridad informática - Ethical Hacking. Autores: Marion AGÉ et. al. Ed. ENI
- CCNP Security Secure 642-637 Official Cert Guide. Autores: Sean Wilkins, Franklin H. Smith III. Ed. Cisco Press.

7.2. Bibliografía complementaria:

- 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:

Los sistemas de evaluación diseñados son los siguientes:

- Examen de teoría/problemas (30%)
- Defensa de trabajos e informes escritos (30%)
- Defensa de prácticas (30%)
- Participación en las actividades propuestas (10%)

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 1	Tema 1
#2	2.97	0	0	1.31	0	Práctica 2	Tema 2 y Tema 3
#3	2.97	0	0	1.31	0	Práctica 3	Tema 4 y Tema 5
#4	2.97	0	0	1.31	0	Práctica 4	Tema 6 y Tema 7
#5	2.97	0	0	1.31	0	Práctica 5	Tema 8 y Tema 9
#6	2.97	0	0	1.31	0	Práctica 6	Tema 10 y Tema 11
#7	2.98	0	0	1.34	0	AAD	Tema 12
#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		