Guía docente de la asignatura

Seguridad Avanzada en Redes (M92/56/2/15)

Fecha de aprobación por la Comisión Académica: 09/07/2024

Máster	Máster Universitario en Ingeniería de Telecomunicación
MÓDULO	Optatividad
RAMA	Ingeniería y Arquitectura
CENTRO RESPONSABLE DEL TÍTULO	Escuela Internacional de Posgrado

Semestre	Primero	**Créditos**	4.50	**Tipo**	Optativa	**Tipo de enseñanza**	Presencial

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Máster)

Políticas de seguridad. Diseño y despliegue de la seguridad. Auditorías. Herramientas de seguridad. Gestión de incidentes de seguridad.

COMPETENCIAS

COMPETENCIAS BÁSICAS

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en 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.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- 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.

COMPETENCIAS GENERALES

- CG01 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería de telecomunicación.
- CG08 - Capacidad para comprender la responsabilidad ética y la deontología profesional de la actividad de la profesión de Ingeniero de Telecomunicación.
- CG10 - Conocimiento, comprensión y capacidad para aplicar la legislación necesaria en el ejercicio de la profesión de Ingeniero de Telecomunicación.

COMPETENCIAS ESPECÍFICAS

- CE06 - Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
- CE07 - Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

COMPETENCIAS TRANSVERSALES

- CT01 - Capacidad para la aplicación de los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar conocimientos.

RESULTADOS DE APRENDIZAJE (Objetivos)

1. Describir las políticas de seguridad y los métodos de definición e implantación asociados.
2. Ser capaz de establecer una política de seguridad a partir del análisis de requisitos.
3. Ser capaz de desplegar mecanismos de seguridad en profundidad para proteger una red corporativa o residencial
4. Identificar vulnerabilidades, amenazas y ataques en un sistema de telecomunicación.
5. Seleccionar los métodos de defensa adecuados ante amenazas.
6. Identificar los mecanismos de prevención, detección y respuesta a incidentes de seguridad.
7. Identificar las técnicas y métodos necesarios para la realización de auditorías de seguridad en redes.
8. Identificar y ser capaz de aplicar técnicas forenses básicas para el análisis de incidentes de seguridad.
9. Ser capaz de utilizar herramientas de monitorización y gestión de la seguridad de una red.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

- Tema 0. Introducción a la asignatura (1 hora)

- Tema 1. Gestión de la seguridad (2 horas)
  - Normativa y estándares de seguridad
  - Políticas de seguridad
  - Gestión de riesgos
  - Planes de continuidad de negocio (BCP) y de recuperación ante desastres (DRP)

- Tema 2: Diseño de redes seguras. (4 horas)
  - Principios de diseño
  - Cortafuegos
  - Fortalecimiento de routers y sistemas
  - Diseño de redes seguras

- Tema 3: Auditorías de seguridad y test de penetración (3h)
  - Introducción
  - Footprinting
  - Fingerprinting
  - Explotación
  - Fases finales del test de penetración

- Tema 4: Monitorización de la seguridad en redes (7 horas)
  - Introducción: sistemas de monitorización de la seguridad
  - Sistemas de detección de intrusos
  - Recolección de datos
  - Honeypots

- Tema 5: Gestión de incidentes. (3 horas)
  - Análisis de incidentes
  - Respuesta ante incidentes
  - Análisis forense.

PRÁCTICO

SEMINARIOS

- Seminario 1. Metodologías para auditorías de seguridad y test de penetración (2 h)
- Seminario 2. Explotación de vulnerabilidades (2 h)
- Seminario 3. Sistemas SIEM (2 h)
- Seminario 4. Clasificación y gestión de incidentes: procedimientos de gestión de incidentes (2 h)

PRÁCTICAS DE LABORATORIO

- Práctica 1. Configuración avanzada de cortafuegos (4 h)
- Práctica 2. Test de penetración (4 h)
- Práctica 3: Monitorización de incidentes de seguridad (4h)
- Práctica 4. Análisis forense de trazas de red (3 h)

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- TEMA 1: J, Stewart, M. Chapple, D. Gibson: CISSP : Certified Information Security Professional Study Guide (6th Edition). Ed. Wiley, 2012. ISBN: 1118314174
- TEMA 2: Stephen Northcutt, Lenny Zeltser, Scott, Winters, Karen Kent, Ronald W. Ritchey: Inside Network Perimeter Security (2nd Edition). Sans institute. 2005. ISBN: 978-0672327377
- TEMA 3: Michael Gregg: Certified Ethical Hacker (CEH) Cert Guide, Publisher: Pearson Certification, 2013, ISBN-10: 0-7897-5127-5
- TEMAS 4 y 5: Sanders, Chris; Smith, Jason.: Applied Network Security Monitoring, Syngress, 2014 ISBN: 978-0-12-417208-1

BIBLIOGRAFÍA COMPLEMENTARIA

Fry, Chris; Nystrom, Martin: Security Monitoring, O'Reylly, 2009 ISBN: 978-0-596-51816-5

METODOLOGÍA DOCENTE

- MD01 Lección magistral/expositiva
- MD02 Resolución de problemas
- MD04 Prácticas de laboratorio
- MD06 Realización de trabajos individuales
- MD07 Tutorías académicas

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

El artículo 17 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que la convocatoria ordinaria estará basada preferentemente en la evaluación continua del estudiante, excepto para quienes se les haya reconocido el derecho a la evaluación única final.

Con objeto de evaluar la adquisición de los contenidos y competencias a desarrollar en la materia, se utilizará un sistema de evaluación diversificado, seleccionando las técnicas de evaluación más adecuadas para las asignaturas en cada momento, que permita poner de manifiesto los diferentes conocimientos y capacidades adquiridos por el alumnado.

- Para la parte teórica se realizará un examen final. La ponderación de este bloque será del 50%.
- Para la parte práctica se realizarán prácticas de laboratorio y se valorará la asistencia y las entregas de los informes/memorias realizados por los alumnos, o en su caso las entrevistas personales con los alumnos y las sesiones de evaluación. La ponderación de este bloque será del 30%.
- La parte de trabajo autónomo y los seminarios se evaluarán teniendo en cuenta la asistencia a los seminarios, los problemas propuestos que hayan sido resueltos y entregados por los alumnos, en su caso, las entrevistas efectuadas durante el curso y la presentación oral de los trabajos desarrollados. La ponderación de estos será del 20%.

La calificación global de la asignatura corresponderá a la suma de las calificaciones correspondientes a la parte teórica, la parte práctica y la correspondiente a los seminarios, de manera que la superación de la materia precisará la concurrencia de dos hechos:

1) La calificación de la parte teórica deberá ser igual o superior al 40% del máximo de esta parte, esto es, >=2 puntos sobre 5.

2) La calificación global deberá ser igual o superior a 5 puntos sobre 10.

Todo lo relativo a la evaluación se regirá por la normativa sobre planificación docente y organización de exámenes vigente en la Universidad de Granada.

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional.

EVALUACIÓN EXTRAORDINARIA

El artículo 19 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria dispondrán de una convocatoria extraordinaria. A ella podrán concurrir todos los estudiantes, con independencia de haber seguido o no un proceso de evaluación continua. De esta forma, el estudiante que no haya realizado la evaluación continua tendrá la posibilidad de obtener el 100% de la calificación mediante la realización de una prueba y/o trabajo.

Esta modalidad de evaluación estará formada por las siguientes pruebas orientadas a acreditar que el estudiante ha adquirido la totalidad de las competencias generales y específicas descritas en el apartado correspondiente de esta Guía Docente:

- Prueba sobre el contenido teórico (50% de la calificación final). Se requiere una calificación superior a 2 sobre 5 para poder superar la asignatura.
- Prueba sobre el contenido práctico (30% de la calificación), según se indica en el siguiente párrafo.
- Prueba sobre el contenido de seminarios (20% de la calificación).

En la convocatoria extraordinaria el alumno mantendrá la calificación obtenida en la convocatoria ordinaria para la parte práctica, a menos que lo solicite al profesor con una antelación mínima de 48 horas antes de la convocatoria de examen, en cuyo caso realizará una prueba sobre un supuesto práctico derivado de las prácticas de laboratorio que podrá realizarse en el propio laboratorio en fecha diferente a la de la prueba final. Esta prueba computará por el total correspondiente a la parte práctica (30% de la calificación final).

EVALUACIÓN ÚNICA FINAL

El artículo 8 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que podrán acogerse a la evaluación única final, el estudiante que no pueda cumplir con el método de evaluación continua por causas justificadas.

Para acogerse a la evaluación única final, el estudiante, en las dos primeras semanas de impartición de la asignatura o en las dos semanas siguientes a su matriculación si ésta se ha producido con posterioridad al inicio de las clases o por causa sobrevenidas. Lo solicitará, a través del procedimiento electrónico, a la Coordinación del Máster, quien dará traslado al profesorado

correspondiente, alegando y acreditando las razones que le asisten para no poder seguir el sistema de evaluación continua.

Para los estudiantes que se acojan a la evaluación única final, esta modalidad de evaluación estará formada por las siguientes pruebas escritas orientadas a acreditar que el estudiante ha adquirido la totalidad de las competencias generales y específicas descritas en el apartado correspondiente de esta Guía Docente:

- Prueba sobre el contenido teórico (50% de la calificación final). Se requiere una calificación superior a 2 sobre 5 para poder superar la asignatura.
- Prueba sobre el contenido práctico (30% de la calificación).
- Prueba sobre el contenido de seminarios (20% de la calificación).

INFORMACIÓN ADICIONAL

Información de interés para estudiantado con discapacidad y/o Necesidades Específicas de Apoyo Educativo (NEAE): Gestión de servicios y apoyos (https://ve.ugr.es/servicios/atencion-social/estudiantes-con-discapacidad).

SOFTWARE LIBRE

Se utiliza el siguiente software libre:

- Virtualbox
- Sistema operativo Linux (distribuciones Kali, SecurityOnion y Ubuntu)
- Metasploit Framework
- NMAP Scanning tool
- OpenVAS
- IPtables
- Snort
- Wireshark