

Curso Académico: ( 2019 / 2020 )

Fecha de revisión: 27-04-2017

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: RUBIO MANSO, JOSE MARIA

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

## OBJETIVOS

### COMPETENCIAS BÁSICAS

- 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 (CB8).
- 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 (CB9).
- Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando (CB10).

### COMPETENCIAS GENERALES

- Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad (CG4).
- Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) (CG5).

### COMPETENCIAS ESPECÍFICAS

- Conocer de manera somera los requisitos y el procedimiento de certificación de sistemas seguros (CE9).

### RESULTADOS DEL APRENDIZAJE

- \* Desarrollar un análisis de riesgos para una organización y a partir de él, y conociendo el umbral de riesgo y el riesgo asumible, gestionar los riesgos resultantes.
- \* Conocer los principales criterios (singularmente los Commons Criteria) y las correspondientes metodologías de evaluación y certificación de la seguridad y sus implicaciones en el desarrollo de arquitecturas seguras.
- \* Conocer el Esquema Nacional de Evaluación y Certificación de las Tecnologías de la Información, los requisitos y las funciones de los laboratorios de evaluación y del Organismo de Certificación, así como el alcance del acuerdo de reconocimiento mutuo de certificados.

## DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Análisis de Riesgos y Certificación de Sistemas:

1. Análisis y Gestión de Riesgos
  - 1.1. Conceptos
  - 1.2. Estándares. UNE/ISO 31000 y 27005. ENS. PCI-DSS
  - 1.3. Metodologías y Herramientas. MAGERIT/PILAR
  - 1.4. Mitigación de Riesgos y Selección de Controles
2. Evaluación y Certificación de Productos y Sistemas
  - 2.1. Introducción y Conceptos
  - 2.2. ISO/IEC 15408. Common Criteria. Otros Criterios
  - 2.3. Perfiles de protección
  - 2.4. Metodologías de Evaluación. ISO/IEC 18045
  - 2.5. Reconocimiento Mutuo de Certificados

3. Orden PRE 2740/2007.
- 3.1. Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
- 3.2. Laboratorios de Evaluación. Acreditación
- 3.3. Organismo español de Certificación

## ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

### ACTIVIDADES FORMATIVAS

- Clase teórica
- Clases teórico prácticas
- Tutorías
- Trabajo en grupo
- Trabajo individual del estudiante

### METODOLOGÍAS DOCENTES

- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
- Lectura crítica de textos recomendados por el profesor de la asignatura:  
Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
- Elaboración de trabajos e informes de manera individual o en grupo

## SISTEMA DE EVALUACIÓN

La evaluación de la asignatura para la convocatoria ordinaria se compone de:

1. Evaluación continua (60% de la nota final) desglosada en los siguientes apartados:
  - 1.1. Cuestionarios de evaluación (40%).
  - 1.2. Trabajos, individuales o colectivos, asignados por el profesor (15%).
  - 1.4. Participación en debates en clase (5%).
2. Examen final escrito (40% de la nota final) sobre los contenidos de la asignatura.

Para la convocatoria extraordinaria, se pueden dar tres situaciones según que el estudiante:

- a) Haya seguido el proceso de evaluación continua y desee mantener la nota de esta. En este caso, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.
- b) No haya seguido el proceso de evaluación continua. En este caso, tendrá derecho a realizar un examen con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso.
- c) Haya seguido el proceso de evaluación continua, pero desee ser calificado en la convocatoria extraordinaria en las mismas condiciones indicadas en el apartado b).

<b>Peso porcentual del Examen Final:</b>	40
<b>Peso porcentual del resto de la evaluación:</b>	60

## BIBLIOGRAFÍA BÁSICA

- null NORMA ISO/IEC 15408-1, ISO, 2009
- null NORMA ISO/IEC 15408-2, ISO, 2008
- null NORMA ISO/IEC 15408-3, ISO, 2005
- null NORMA ISO/IEC 18405, ISO, 2005
- null NORMA ISO/IEC 27005, AENOR, 2008
- null NORMA UNE-ISO 31000, AENOR, 2010

- null NORMA UNE-ISO/IEC 27000, AENOR, 2014
- null NORMA UNE-ISO/IEC 27001, AENOR, 2014
- null NORMA UNE-ISO/IEC 27002, 2015, AENOR

#### BIBLIOGRAFÍA COMPLEMENTARIA

- Debra S. Herrmann Using the Common Criteria for IT Security Evaluation, CRC Press, 2002
- Marquina Llivisaca, Edgar Geovanny Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT, EAE, 2012

#### RECURSOS ELECTRÓNICOS BÁSICOS

- . ISO Freely Available Standards: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
- . MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html#.WMqje\\_JRKnQ](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WMqje_JRKnQ)
- . Herramienta PILAR: <https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html>
- . Esquema Nacional de Seguridad (ENS): <https://administracionelectronica.gob.es/ctt/ens#.WMqkBvJRKnQ>
- . PCI Security Standards Council: <https://es.pcisecuritystandards.org/minisite/en/>
- . Portal Common Criteria: <https://www.commoncriteriaportal.org/>
- . Esquema Nacional de Evaluación y Certificación de la Seguridad de los Sistemas de Información: [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Estrategias/pae\\_Seguridad\\_Inicio/pae\\_evaluacion\\_y\\_certificacion\\_de\\_la\\_seguridad/pae\\_Seguridad\\_Evaluacion\\_Esquema\\_Nacional.html?comentarioContenido=0#.WMqk3PJRNQ](https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_evaluacion_y_certificacion_de_la_seguridad/pae_Seguridad_Evaluacion_Esquema_Nacional.html?comentarioContenido=0#.WMqk3PJRNQ)