FICHA DE ASIGNATURA

Título: Amenazas y análisis de riesgos

Descripción: En esta asignatura vamos a profundizar en el concepto de “gestión de riesgos” y, en particular, de los riesgos asociados al uso de las tecnologías por parte de las organizaciones.

Carácter*:* Obligatoria

Créditos ECTS: 3

Contextualización: Nos adentraremos en el proceso de gestión de riesgos general, los principales conceptos relacionados con este tema, y las metodologías que se emplean más habitualmente. Asimismo, presentaremos algunas situaciones más comunes que, en la práctica, requieren de la realización de análisis de riesgos por parte de las empresas.

Modalidad*:* Online

Temario:

- Seguridad en redes. Identificación de amenazas y vectores de ataque.
- El proceso de gestión de riesgos: introducción y definiciones
- Etapas del proceso de gestión de riesgos: metodologías (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), NIST SP 800-30.
- Aplicaciones del proceso de análisis y gestión de riesgos.

Competencias Específicas:

CE4 – Identificar las vulnerabilidades, amenazas, y software malicioso a los que estén expuestos los diferentes activos de una organización.

CE7 - Conocer las tendencias actuales en ciberataques, técnicas de ocultación y principales vectores utilizados.

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	15	100%
Desarrollo de actividades del portafolio	12	0
Trabajo autónomo del alumno	48	0

Metodologías docentes

- Clases síncronas

- Vídeos con píldoras de conceptos teóricos

- Caso práctico

- Soporte a consultas

Sistema de Evaluación

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Examen	40%	60%
Trabajo individual	40%	60%

Bibliografía:

- ISO - International Organization for Standardization:
- ISO/IEC 27001:2013 -- Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC 27002:2013 -- Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27005:2011 -- Information technology -- Security techniques -- Information security risk management
- ISO 31000:2009 -- Risk management -- Principles and guidelines
- ISO 22301:2012 -- Societal security -- Business continuity management systems --- Requirements
- NIST -- National Institute for Standards and Technology -- U.S Department of Commerce:
- NIST 800-30 - Guide for conducting Risk Assessments - Information Security
- Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 -- Febrero 2014.
- Information Security Forum (ISF): Information Risk Assessment Methodology 2
- ISACA: COBIT 5
- Ministerio de Hacienda y Administraciones Públicas - MAGERIT versión 3.0
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información -Libro I - Método
- Diario Oficial de la Unión Europea - REGLAMENTOS - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- EBA (European Banking Authority) - EBA/GL/2017/05 - Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)
- Agencia Estatal Boletín Oficial del Estado Gobierno de España - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA -- La fábrica del pensamiento Buenas prácticas en gestión de riesgos -- Ciberseguridad -- Una guía de supervisión -- octubre 2016.