Análisis de Riesgos en Ciberseguridad

Curso Académico: (2024 / 2025) **Fecha de revisión: 25-04-2024**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: DIAZ SANCHEZ, DANIEL

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

- Partiendo del inventario de activos de una organización aplicar alguna de las metodologías existentes para realizar el análisis de riesgos y saber transmitir los resultados a la organización. (CE9).

RESULTADOS DEL APRENDIZAJE

*Desarrollar un análisis de riesgos para una organización que permita la identificación y la evaluación de los mismos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción y conceptos generales de Análisis de Riesgos.
1.1 Conceptos básicos: activos, amenazas, vulnerabilidades, salvaguardas, riesgo.
1.1.1 Análisis cualitativo y cuantitativo.
1.1.2 Análisis estático y dinámico.
1.2 Aspectos avanzados.
1.2.1 Modelado y categorización de Amenazas (STRIDE, DREAD, CAPEC). Amenazas de Sitios Web (WASC).
1.2.2 Evaluación de vulnerabilidades y Tests de Penetración (VAPT).
2. Metodologías de Análisis de Riesgos.
2.1 ISACA (COSO), CRAMM, EBIOS, PCI-DSS, NIST SP-800 ...
2.2 ISO-27005. MAGERIT.
3. Entornos actuales y futuros de aplicación.

3.1 Cloud Computing.
3.2 Big Data - AI.
3.3 Internet Of Things (IoT).
3.4 Entornos móviles (Wireles, Smartphones, ...).

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

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

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. Trabajos, individuales o colectivos, asignados por el profesor (50%).
   1.4. Participación en debates en clase (10%).

2. Examen final escrito sobre los contenidos de la asignatura (40% de la nota final).

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).

BIBLIOGRAFÍA BÁSICA

- AENOR NORMA ISO/IEC 27005, AENOR, 2008

- Adam. Shostack Threat modeling : designing for security, John Wiley and Sons, 2014

- John R. Vacca Cyber Security and IT Infrastructure Protection, Syngress, 2013

BIBLIOGRAFÍA COMPLEMENTARIA

- Gibson, Darril Managing Risk in Information Systems (2nd Edition), Jones & Bartlett Learning, 2014

- Gregory Allen Threat assessment and risk analysis : an applied approach, Butterworth Heinemann, 2016

- Marquina Llivisaca, Edgar Geovanny Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT, EAE, 2012

- Uceda Vélez, Tony ; Morana, Marco M.Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis, John Wiley & Sons Inc, 2015

RECURSOS ELECTRÓNICOS BÁSICOS

- CCN . PILAR : https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

- CSAE (MAP) . MAGERIT v.3: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WMqje_J

- CVE . Common Vulnerabilities and Exposures: https://cve.mitre.org/

- NVD . National Vulnerability Database: https://nvd.nist.gov/vuln

- OWASP . The OWASP¿ Foundation: https://www.owasp.org/index.php/Main_Page