Ingeniería de la Ciberseguridad

Curso Académico: (2023 / 2024) **Fecha de revisión: 12-04-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: ESTEVEZ TAPIADOR, JUAN MANUEL

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 4 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Criptografía y Seguridad de la Información (Curso 3, Cuatrimestre 1)
Redes de Ordenadores (Curso 3, Cuatrimestre 1)
Sistemas Operativos (Curso 2, Cuatrimestre 2)

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE

¿ Conocer las principales amenazas, riesgos y vulnerabilidades de los sistemas informáticos y en redes.
¿ Concebir, diseñar y evaluar soluciones que combinen algoritmos criptográficos, modelos de acceso y protocolos para proteger la información de un sistema informático ante determinadas amenazas
¿ Conocer la regulación en materia de ciberseguridad sobre privacidad y protección de datos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a la Ciberseguridad
1.1. ¿Qué es la ciberseguridad?
1.2. La terna CIA
1.3. Vulnerabilidades, amenazas, riesgos y controles
1.4. Atacantes
1.5. Principos de diseño
1.6. Áreas de estudio en ciberseguridad

2. Autenticación
2.1. Autenticación de usuarios
2.2. Factores de autenticación
2.3. Contraseñas y gestores de contraseñas
2.4. Autenticación biométrica
2.5. Gestión Federada de la Identidad

3. Control de acceso
3.1. El problema de la protección
3.2. Modelos de control de acceso
3.3. Control de acceso en Linux (I): credenciales y sistema de permisos
3.4. Control de acceso en Linux (II): POSIX ACLs y capacidades

4. Seguridad en redes
4.1. Seguridad en las comunicaciones
4.2. Problemas de seguridad en redes TCP/IP
4.3. Descubrimiento y escaneo de redes
4.4. Seguridad web
4.5. Cortafuegos
4.6. Sistemas de detección de intrusiones

5. Protocolos de Seguridad: TLS
5.1. Historia y obetivos de diseño
5.2. El protocolo de handshake
5.3. El protocolo record
5.4. Interceptación y pinning de certificados

6. Vulnerabilidades
6.1. Tipos de vulnerabilidades
6.2. Numeración (CVE) y métricas (CVSS)
6.3. Ciclo de vida

7. Malware
7.1. Código dañino
7.2. Tipos de malware
7.3. Cargas, transmisión, propagación y activación
7.4. Casos de estudio

8. Regulación en ciberseguridad
8.1. Regulación en EE.UU.
8.2. Regulación en la UE
8.3. Regulación sobre privacidad y protección de datos

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente incluye:
1. Clases magistrales, donde se presentan los conocimientos que los alumnos deben adquirir. Los alumnos recibirán las notas de clase y diversos documentos suplementarios, así como textos básicos de referencia que les permitan completar y profundizar en el estudio de los temas expuestos. (2 ECTS)
2. Clases prácticas, donde el alumno resolverá ejercicios que le servirán para autoevaluar sus conocimientos y adquirir las capacidades necesarias. (1 ECTS)
3. Discusión de casos reales, que servirán para ilustrar lo expuesto en las clases teóricas. (1 ECTS)
4. Clases en aulas informáticas, donde se aprenderá el uso de técnicas y herramientas de distintos ámbitos de la ciberseguridad: análisis de binarios, análisis de seguridad de aplicaciones distribuidas, seguridad en redes, etc. (2 ECTS)

SISTEMA DE EVALUACIÓN

La evaluación se basará en los siguientes criterios:
(a) Resolución de prácticas de laboratorio: 40%. Estas prácticas tienen carácter obligatorio y se evalúan mediante corrección de los entregables correspondientes y, en algunos casos, exposición en clase de los resultados.
(b) Examen final: 60%. La realización de examen final es obligatoria, siendo necesario obtener, al menos, el 50% de la nota máxima posible en este examen para poder superar la asignatura.

En la convocatoria extraordinaria, el alumno que haya seguido la evaluación continua podrá, si lo desea, realizar un examen por valor del 60% de la nota, calificándose la asignatura de la misma manera que en la convocatoria ordinaria. Alternativamente, también podrá realizar exclusivamente un único examen final, en cuyo caso este valdrá el 100% de la nota final.

En todo lo no contemplado aquí, se aplicará lo establecido en la normativa aprobada por el Consejo de Gobierno del 31 de mayo de 2011.

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

BIBLIOGRAFÍA BÁSICA

- Anderson, Ross SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTRED SISTEMS (2nd edition), Wiley, 2008
- Pfleeger, Charles. Pfleeger, Shari L SECURITY IN COMPUTING (4ª edition), Prentice Hall, 2007

BIBLIOGRAFÍA COMPLEMENTARIA

- Vacca, John R. (Editor). COMPUTER AND INFORMATION SECURITY HANDBOOK., Elsevier (The Morgan Kaufmann Series in Computer Security)., 2009.

RECURSOS ELECTRÓNICOS BÁSICOS

- ENISA . Publications: http://www.enisa.europa.eu
- INCIBE . OSI/CERTSI: Https//www.incibe.es
- NIST . Special Publications (NIST-SP): http://www.nist.gov/publication-portal.cfm