Ingeniería de la Seguridad

Curso Académico: (2020 / 2021) **Fecha de revisión: 12-02-2021**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: ESTEVEZ TAPIADOR, JUAN MANUEL

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 3 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Criptografía y Seguridad de la Información
Redes de Ordenadores
Sistemas Operativos

OBJETIVOS

Los objetivos de esta asignatura son que el estudiante reconozca a la seguridad como un proceso global que interconecta múltiples y complejas dimensiones, de modo sólo una visión integrada de todas ellas (propia de una ingeniería) puede proporcionar a nuestros sistemas las soluciones de seguridad que la sociedad demanda. Además, como parte fundamental de esta visión propia de una ingeniería, aprenderá a desarrollar un plan de seguridad, que le permitirá familiarizarse con el ciclo de vida de las medidas de seguridad y su costo. Finalmente, deberá conocer las principales disposiciones legales, que regulan esta materia.
Para lograr estos objetivos el alumno debe adquirir una serie de conocimientos, capacidades y actitudes.

Por lo que se refiere a los conocimientos, al finalizar el curso el estudiante será capaz de:
- Entender que la seguridad es un proceso (más que un sistema) complejo y de múltiples dimensiones cuya robustez viene determinada por la más débil de éstas
- Dominar las normas de evaluación y certificación de la seguridad.
- Entender los riesgos específicos a que están sometidos los sistemas distribuidos y, particularmente, Internet.
- Identificar las amenazas físicas y las correspondientes medidas de seguridad.
- Conocer las partes constitutivas de un plan de seguridad
- Conocer las distintas partes del ciclo de vida de la seguridad y su retroalimentación.
- Conocer la regulación legal de la informática relativa a seguridad en los ámbitos nacional, europeo e internacional

Por lo que atañe a las capacidades se pueden desglosar en específicas y genéricas (destrezas).
En cuanto a las capacidades específicas, el alumno será capaz de:
- Analizar los protocolos de seguridad y gestionar los riesgos de los sistemas de información, singularmente los distribuidos. (PO: a,b)
- Evaluar la oportunidad de emplear unos u otros mecanismos en función del riesgo esperado. (PO: b, c, e)
- Elaborar un plan de seguridad, diseñando, aplicando y administrando las medidas de seguridad oportunas. (PO: a, c, e, f)
- Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados
- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.
- Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación

En cuanto a las capacidades generales o destrezas, durante el curso se trabajarán:
- La capacidad para investigar un sistema particular en un entorno concreto y hallar sus vulnerabilidades y amenazas. (PO: b, e)
- La capacidad para encontrar y seleccionar las informaciones relevantes para solucionar un problema concreto. (PO: b, c, e)

- La capacidad para aplicar conocimientos multidisciplinares (técnicos, organizativos y legales) a la resolución de un determinado problema. (PO: c, e, f)

En cuanto a las actitudes el alumno tras cursar el curso debería tener:

- Una actitud crítica respecto de la seguridad convencional basada en la acumulación de equipos y programas sin un estudio previo de los riesgos previstos ni una consideración del ciclo de vida de la misma. (PO: i, j, k)
- Una actitud de colaboración que le permita obtener de los responsables de un sistema las informaciones precisas para analizar y evaluar los riesgos y transmitirles las propuestas de solución. (PO: d, f, g)
- Una actitud favorable al trabajo en equipo que permite coordinar los distintos puntos de vista de los implicados en aras de conseguir una visión global de la seguridad (PO: d, f)
- Una actitud positiva ante las disposiciones legales que condicionan la aplicación de sistemas y productos de seguridad.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a la Ciberseguridad
1.1 ¿Qué es la Ciberseguridad?
1.2 La terna CIA
1.3 Vulnerabilidades
1.4 Amenazas y Atacantes
1.5 Riesgos
1.6 Controles

2. Autenticación y Control de Acceso
2.1 Contraseñas
2.2 Autenticación Biométrica
2.3 Tokens de Autenticación
2.4 Gestión Federada de la Identidad
2.5 Control y Políticas de Acceso
2.6 Implementación del Control de Acceso
2.7 Otros Paradigmas de Control de Acceso

3. Seguridad en Software
3.1 Desbordamientos de Buffer
3.2 Mediación Incompleta
3.3 Puntos de Acceso No Documentados
3.4 Condiciones de Carrera
3.5 Contramedidas

4. Malware
4.1 Código Malicioso
4.2 Tipos de Malware
4.3 Cargas
4.4 Transmisión y Propagación
4.5 Activación
4.6 Autodefensa

5. Seguridad Web
5.1 Ataques al Navegador
5.2 Ataques Web contra el Usuario
5.3 Obtención de Datos del Usuario o del Servidor
5.4 Ataques a través del Email

6. Seguridad en Sistemas Operativos
6.1 Nota Histórica
6.2 Diseño del SO para porteger objetos
6.3 Herramientas del SO para Implementar Seguridad
6.4 Principios de Diseño Seguro

7. Ataques en Redes
7.1 Ataques de Interceptación
7.2 Ataques de Hombre en el Medio
7.3 Ataques de Negación de Servicio

8. Protocolos de Seguridad: TLS
8.1 Historia y Obetivos de Diseño

8.2 El Protocolo de Handshake
8.3 El Protocolo Record
8.4 Interceptación
8.5 Pinning de Certificados

9. Privacidad
9.1 Privacidad en la Web: Web Bugs y ATS
9.2 Onion Routing: TOR
9.3 La Directiva General de Protección de Datos (GDPR)

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. Clases prácticas, donde el alumno resolverá ejercicios que le servirán para autoevaluar sus conocimientos y adquirir las capacidades necesarias.
3. Discusión de casos reales, que servirán para ilustrar lo expuesto en las clases teóricas.
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.

SISTEMA DE EVALUACIÓN

La evaluación se basará en los siguientes criterios:
(a) Resolución de prácticas de laboratorio: 50%. 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: 50%. 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 50% 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:	50
Peso porcentual del resto de la evaluación:	50

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