Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Ingeniería Informática
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Seguridad
Tipo:	Obligatoria
Créditos ECTS:	6
Curso:	4
Código:	3656
Periodo docente:	Séptimo semestre
Materia:	Ingeniería del Software
Módulo:	Tecnología Específica
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	150

Equipo Docente	Correo Electrónico
Constantino Malagón Luque	constantino.malagon@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

Los Sistemas de Información son una parte esencial de la gestión diaria de las organizaciones. La continuidad de las operaciones depende, en gran parte, de los Sistemas donde se trata la información y se concentra el conocimiento y el saber hacer de las empresas. Por este motivo, la seguridad de los Sistemas de Información es una parte relevante de cualquier diseño, desarrollo o mantenimiento que se pueda realizar, conclusión que sirve de hilo conductor de cómo dotar de seguridad a las infraestructuras y servicios asociados al tratamiento de la información y a la tecnología de las comunicaciones.

OBJETIVO

Comprender las metodologías de análisis y gestión de riesgos como parte esencial del enfoque de estudio de la Seguridad de los Sistemas de Información, analizando los procesos de negocio de las organizaciones, los activos de información que los soportan y las principales amenazas y vulnerabilidades a las que se puede enfrentar una empresa.

Los fines específicos de la asignatura son:

Entender, cómo la evolución de las tecnologías de la información ha comportado que el software se conciba para plataformas distribuidas y entornos Web y, llegada esta situación, se hace imprescindible tener en cuenta la seguridad en el software más allá de lo que tradicionalmente se ha hecho, es decir, desde el inicio del proyecto de ingeniería del software, realizando un análisis de requisitos de seguridad y desarrollando las actividades que aseguren el cumplimiento de dichos requisitos.

Tratar la seguridad del software otorgando un carácter relevante a la confidencialidad, la integridad y la disponibilidad, es decir, ya no sólo se atenderá a los riesgos de pérdida no intencionada del mismo sino también, a las acciones maliciosas e ilegítimas, los aspectos de confidencialidad y los derechos de propiedad intelectual.

Conocer las implicaciones técnicas, organizativas y legales de los atributos de confidencialidad, integridad y disponibilidad de la Seguridad de los Sistemas de Información, en base a la presentación de casos concretos donde se aúnan los conocimientos técnicos adquiridos y una visión integral de los orígenes de los incidentes de seguridad y de las soluciones propuestas para los mismos.

Aproximarse a la Seguridad de los Sistemas de Información como un proceso cuyos recursos técnicos y profesionales deben de ser gestionados durante las fases de planificación, diseño, desarrollo, implantación y mantenimiento de los mismos.

CONOCIMIENTOS PREVIOS

Los propios de los estudios en los cursos académicos anteriores.

CONTENIDOS

Tema 1 - Presentación. Introducción al Hacking ético

Tema 2 - Tecnicas de obtencion de informacion. escaneo de puertos y deteccion de vulnerabilidades
- Metodos no intrusivos para la obtencion de informacion.
- Conceptos basicos de TCP/IP, servicios y comunicaciones.
- Metodos intrusivos para la obtencion de informacion.
- Descubrimiento de equipos en la red. Uso de Netdiscover.
- Tecnicas de rastreo o sniffing. Uso de Wireshark.
- Escaneo de puertos. Uso de Nmap.
- Sistemas de deteccion de vulnerabilidades.

Tema 3 - Tecnicas de intrusion y ataque
- Tecnicas de ataque en redes locales usando ataque MItM (Man in the Midle). Uso de Bettercap.
- El servicio DNS. Ataques de DNS spoofing.
- Ataques a conexiones seguras basadas en el protocolo HTTPS.
- Detección de ataques MItM.
- Ataques a sistemas con vulnerabilidades. Uso de Metasploit.
- Tecnicas de auditoría de contrasenas. Uso de John the Ripper.
- Troyanos y puertas traseras. Uso de Veil.
- Ingeniería social. Uso de Beef.
- Esteganografía.

Tema 4 - Tecnicas de ocultacion o anonimato
- Rootkits.
- Navegacion anonima.
- Proxys anonimos. Encadenamiento de proxys.

Tema 5 - Seguridad en redes

-Seguridad mediante Firewalls. Concepto de DMZ.
- Firewall mediante iptables en Linux.
- Tecnicas para evitar los firewalls. Remote reverse shell.
-Trabajo en remoto seguro: SSH.
- Redes privadas virtuales (VPN)

Tema 6 - Sistemas de deteccion de intrusos
- Tipos de IDS. Arquitecturas IDS.
- Auditorias y analisis forense.
- Normativa legal.

ACTIVIDADES FORMATIVAS

Se combinan lecciones expositivas con clases prácticas de manera que se favorezca la participación y la interacción alumno/profesor y alumno/alumno como vía para fomentar el aprendizaje colaborativo y la capacidad de autoaprendizaje, todo ello mediante estrategias de resolución de situaciones y metodologías de intervención.
Las actividades no presenciales, que pueden ser tanto de tipo individual como colectivo, serán supervisadas por el profesor en clases y tutorías estando encaminadas a favorecer el aprendizaje autónomo y colaborativo. Se complementa la lección expositiva, por una parte, con las clases prácticas para la asimilación y aplicación de los conocimientos adquiridos y, por otra, con laboratorios que permitan realizar prácticas para la resolución de problemas y casos, con la supervisión directa del profesor y el enriquecimiento del trabajo en grupo.
Finalmente, con el fin de facilitar al alumno el acceso a los materiales y la planificación de su trabajo, así como la comunicación con el profesor y el resto de alumnos, se empleará el Aula Virtual de la Universidad.
Las actividades formativas, así como la distribución de los tiempos de trabajo, pueden verse modificadas y adaptadas en función de los distintos escenarios establecidos siguiendo las indicaciones de las autoridades sanitarias.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
68 horas	82 horas
Clase práctica 22h Lección expositiva 30h Taller 8h Tutorías 4h Examen 4h	Estudio y trabajo individual 60h Trabajo en grupo 22h

COMPETENCIAS

Competencias básicas

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

Competencias generales

Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.

Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.

Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como la legislación, regulación y normalización en el ámbito de los proyectos informáticos.

Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática.

Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad.

Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes.

Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

Competencias específicas

Capacidad para desarrollar, mantener y evaluar servicios y sistemas software que satisfagan todos los requisitos del usuario y se comporten de forma fiable y eficiente, sean asequibles de desarrollar y mantener y cumplan normas de calidad, aplicando las teorías, principios, métodos y prácticas de la Ingeniería del Software.

Capacidad de identificar y analizar problemas y diseñar, desarrollar, implementar, verificar y documentar soluciones software sobre la base de un conocimiento adecuado de las teorías, modelos y técnicas actuales.

Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

RESULTADOS DE APRENDIZAJE

Evaluar las repercusiones técnicas y de negocio de los requisitos de seguridad en el diseño, desarrollo, implantación y mantenimiento de los sistemas de información; así como de la necesidad de construir estos sistemas mediante proyectos cuya gestión se realice teniendo en cuenta criterios de seguridad de la información tratada

Aplicar metodologías y marcos de actuación que permitan analizar los riesgos de seguridad y evaluar diferentes escenarios, independientemente de los entornos tecnológicos y de negocio que los caractericen

Identificar las claves de la evolución de la Seguridad de los Sistemas de Información de acuerdo con la evolución tecnológica y las nuevas demandas sociales de movilidad y tratamiento de la información

Analizar las vulnerabilidades más relevantes de los sistemas, aplicaciones y bases de datos comerciales utilizadas actualmente en las organizaciones.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación contempla cuatro tipos de pruebas:

•Pruebas de carácter teórico-práctico: tiene un peso del 20% en la nota final.
•Pruebas de carácter teórico-práctico y defensa: tiene un peso del 40% en la nota final.
•Pruebas de carácter teórico-práctico: tiene un peso del 30% en la nota final.
•Participación en clase: tiene un peso del 10% en la nota final.

En las tres primeras pruebas es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura, siendo requisito imprescindible haber asistido como mínimo al 80% de las sesiones. En caso contrario este tipo de prueba se calificará con 0 puntos.

Para puntuar en el apartado de participación en clase, es necesario asistir al menos a un 80% de las clases.

Aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el mismo tipo de pruebas. El 10% de la participación en clase podrán obtenerlo asistiendo al menos a tres tutorías con el profesor responsable de la asignatura.

Recuperación en convocatoria extraordinaria

Los alumnos que no hayan alcanzado la nota mínima en el examen escrito y/o en las pruebas escritas teórico-prácticas y en la presentación y defensa de trabajos, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria.

En la recuperación extraordinaria el alumno se presentará sólo a las partes que tenga evaluadas por debajo de 5.

A efecto de cómputo de convocatorias en una asignatura, solamente se contabilizarán como consumidas aquellas en las que el alumno se haya presentado a todas las pruebas de evaluación, o a una parte de las mismas, siempre que su peso en la nota final supere el 50%, aunque no se presente al examen final. Se entenderá que un alumno se ha presentado a una prueba aunque la abandone una vez comenzada la misma. La condición de No Presentado en la convocatoria extraordinaria estará ligada a la no asistencia o entrega de ninguna prueba, práctica o trabajo que esté pendiente.

Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

Si los exámenes no se pudieran realizar de forma presencial, se realizarán de forma remota mediante las herramientas que determine la Universidad Francisco de Vitoria, garantizando siempre la evaluación de las competencias y resultados de aprendizaje de la asignatura.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Michael Gregg. Certified Ethical Hacker Exam Prep 2. (2012) Que editores.

María Angeles Caballero Velasco, Diego Cilleros Serrano, Abtin Shamsaifar. El Libro Del Hacker (2014). Editorial Anaya Multimedia

Abel Matas Garcia. La biblia del hacker. (2003) Anaya Multimedia

Complementaria

Brian Hatch. Hacking exposed Linux. 2nd Edition (2002). Ed. McGraw--Hill.

Michael D. Bauer. Linux Server Security. 2nd Edition (2005). O'Reilly.