Guía Docente

Seguridad en Sistemas Informáticos

I.- Datos iniciales de identificación

Nombre de la asignatura:	*Seguridad en Sistemas Informáticos*
Carácter:	*Obligatoria*
Titulación:	*Máster en Sistemas y Servicios en la Sociedad de la Información* *Especialidad en Gestión y Desarrollo de Servicios y Aplicaciones Web*
Ciclo:	*Postgrado*
Créditos:	*3 ECTS*
Departamento:	*Informática*
Profesor Responsable:	*Carlos Pérez Conde*

II.- Introducción a la asignatura

La seguridad de los sistemas informáticos es un atributo esencial de los sistemas y servicios en la denominada sociedad de la información. Incluso dentro de un ámbito en construcción, como lo es la sociedad de la información, los requisitos de seguridad cambian a un ritmo especialmente rápido, el el sentido de hacerse cada vez más estrictos. Este cambio está lógicamente relacionado con los avances continuos en las tecnologías que posibilitan la implantación de nuevos mecanismos de seguridad, cada vez más refinados.

En este contexto, la asignatura está planteada para servir al mismo tiempo como complemento final a lo abordado en los estudios previos (de grado cuando se implanten y, de momento, en las ingenierías e ingenierías técnicas relacionadas con la informática) y como actualización para los profesionales que desean conocer el estado actual de la práctica profesional de la seguridad.

Las aplicaciones y servicios web, objeto de la especialidad del máster en el que se ubica esta asignatura, deben satisfacer requisitos de seguridad cada vez más exigentes. Ello hace imprescindible que cualquier tipo de aplicación o servicio se ejecute en un sistema que garantice un nivel de seguridad apropiado. Esta asignatura facilita al estudiante la posibilidad de adquirir los conocimientos necesarios para establecer el nivel de seguridad adecuado para cada caso y las medidas técnicas adecuadas para garantizarlo.

III.- Volumen de trabajo

La asignatura tiene asignados 3 ECTS. Considerando que cada ECTS debe corresponderse con un volumen de trabajo de entre 25 y 30 horas, supone un volumen total de entre 75 y 90 horas a

repartir durante el cuatrimestre.

Para el cálculo del volumen de trabajo se ha tomado como referencia un total de 18 horas presenciales que incluyen tanto las clases de teoría como las de prácticas. La distribución prevista del trabajo es la siguiente:

Asistencia a clases teóricas y prácticas:	*18 horas presenciales*	*18*
Preparación de trabajos:	*1 trabajo * 20 horas*	*20*
Estudio-preparación de las clases:	*2 horas/hora presencial * 18 horas*	*36*
Estudio para preparación de exámenes:	*10 horas/examen * 1 examen*	*10*
Realización de exámenes:	*2 horas/examen * 1 examen*	*2*
Asistencia a seminarios:	*1 seminario* *(incluido en las horas presenciales)*	
Asistencia a tutorías:	*2 horas*	*2*
	Volumen total de trabajo:	*88*

IV.- Objetivos generales

- Mostrar el estado actual de la práctica profesional de la seguridad de sistemas informáticos.
- Que el alumno adquiera la capacidad de establecer el nivel adecuado de seguridad, de seleccionar e implantar las medidas necesarias para garantizarlo y de colaborar en su mantenimiento.
- Que el alumno se capacite para seguir los cambios relacionados con la seguridad.

V.- Contenidos

- El proceso de la seguridad. Descripción de las diferentes etapas y actividades relacionadas con la seguridad de los sistemas informáticos, que suponen un proceso continuo y que permiten mantener el nivel de seguridad adecuado.
- Riesgos y vulnerabilidades de los sistemas informáticos. Descripción de las amenazas a las que se enfrentan los sistemas.
- Seguridad de los nodos. Estudio de las medidas a tomar para garantizar la seguridad de cada uno de los computadores que forman parte de los sistemas informáticos.
- Seguridad perimétrica. Estudio de las medidas necesarias para interconectar redes entre sí, centrándose sobre todo en la conexión de la red de la organización con Internet.

- Detección de intrusos. Estudio de medidas complementarias destinadas a detectar violaciones de la política de seguridad establecida y que los métodos de seguridad de los nodos y de seguridad perimétrica tratan de hacer cumplir.
- Análisis forense. Estudio de la forma correcta de analizar sistemas sospechosos que pueden haber sido víctima de un ataque.

VI.- Destrezas a adquirir

- Diseñar y evaluar la política de seguridad de una organización, incluyendo tanto el análisis previo como la gestión de incidentes.
- Diseñar, implantar y evaluar los mecanismos de seguridad necesarios para garantizar el cumplimiento de la política de seguridad.
- Diseñar, implantar y evaluar los mecanismos necesarios para detectar incidentes y para poder tratarlos adecuadamente.

VII.- Competencias y habilidades sociales

- Capacidad de mantenerse al día de los avances en seguridad.
- Coordinarse con otros profesionales técnicos (administradores de sistemas, de redes, de bases de datos, de aplicaciones...) para lograr un correcto funcionamiento de los sistemas informáticos.
- Ser capaz de informar adecuadamente de las incidencias de seguridad.
- Ser capaz de interpretar de forma adecuada los avisos de seguridad lanzados por otros, especialmente las de los centros de respuesta (CERTs).
- Ser capaz de explicar de forma efectiva tanto a los usuarios como a los directivos el porqué de las medidas de seguridad.

VIII.- Temario y planificación temporal

Asumiendo 9 semanas con 2 horas de clase por semana.

1 Visión general de la seguridad informática (2 horas)

1.1 El proceso de la seguridad

1.2 Riesgos y vulnerabilidades

1.3 La política de seguridad

1.4 Tratamiento de incidentes

2 Seguridad centrada en el nodo (5 horas)

2.1 Seguridad física

2.2 Autentificación y control de acceso

2.3 Implicaciones de seguridad de los servicios

2.4 Control de acceso mediante envolventes (*wrappers*)

2.5 Auditoría y registros

2.6 Integridad del sistema

2.7 Detección de intrusos

3 Seguridad perimétrica (5 horas)

3.1 Concepto de cortafuegos

3.2 Filtrado de paquetes

3.3 Proxies

3.4 Diseño de cortafuegos

3.5 Integración de VPNs

3.6 Detección de intrusos

4 Análisis forense (4 horas)

4.1 Conceptos básicos

4.2 Análisis de sistemas de ficheros

4.3 Análisis de programas malintencionados (*malware*)

5 Exposición de trabajos realizados por los alumnos (2 horas)

IX.- Bibliografía de referencia

Biblografía básica:

- *Practical Unix & Internet Security.* S. Garfinkel, G. Spafford, A. Schawartz. O'Reilly.
- *Inside Network Perimeter Security.* S. Northcutt, L. Zeltser, S. Winters, K.K. Frederick, R.W. Ritchey. New Riders.
- *Forensic Discovery.* D. Farmer, W. Venema. Addison-Wesley.

Bibliografía complementaria:

- *Building Internet Firewalls.* D.B. Chapman, E.D. Zwick. O'Reilly.
- *Network Intrusion Detection.* S. Northcutt, J. Novak. New Riders.
- *Maximum Security.* Anonymous, SAMS.
- *Hackers. Secretos y soluciones para la seguridad de redes.* S. McClure, J. Scambray, G. Kurtz. McGraw-Hill.
- *Applied Cryptography.* B. Scheneier. John Wiley & Sons, Inc.
- *Secrets and Lies: Digital Security in an Networked World.* B. Scheneier. John Wiley & Sons, Inc.
- *The art of deception.* K.D. Mitnick, W.L. Simon. John Wiley & Sons, Inc.

X.- Conocimientos previos

- Conceptos básicos de sistemas operativos: procesos, memoria, ficheros y entrada/salida.
- Conceptos básicos de redes: pila TCP/IP, protocolos y servicios comunes (HTTP, FTP, DNS...).
- Conceptos básicos de administración de sistemas: gestión de usuarios y grupos, espacio de almacenamiento, puesta en marcha y parada de servicios...

XI.- Metodología

El desarrollo de la asignatura se basa en tres elementos fundamentales:

- Clases de teoría. Durante estas clases se introducirán los conceptos clave y se presentarán las herramientas más relevantes para aumentar la seguridad. Asimismo, se discutirán las ventajas e inconvenientes de los enfoques más adecuados para cada caso.

  Aunque en estas clases el profesor tendrán papel relevante, se valorará positivamente y se incentivará la participación de los alumnos, proporcionando por anticipado el guión de las clases y las referencias bibliográficas adecuadas para su preparación.
- Clases prácticas. Consistirán en la aplicación práctica de los conceptos abordados en la clase de teoría a un caso práctico. En estas clases, los alumnos serán los protagonistas, limitándose el profesor a ejercer el papel de consultor/supervisor del trabajo.
- Realización de un trabajo en grupo que habrá de ser expuesto en público en la última sesión presencial del curso. Este trabajo, que podrá orientarse a cualquier faceta del ejercicio profesional de la seguridad, tiene un triple objetivo. Por una parte, potenciar la capacidad de aplicar lo tratado en la asignatura, por otra, fomentar la capacidad de colaborar y coordinarse con otros profesionales para aumentar la seguridad de los sistemas y, finalmente, aumentar la capacidad exponer de forma resumida y precisa el trabajo realizado.
- Aula virtual. Durante el periodo lectivo se utilizará la herramienta Aula Virtual para distribuir el material docente (transparencias, documentos, enlaces a material complementario...), para avisar a los alumnos de eventos relacionados con la asignatura (charlas, clases prácticas...), para la entrega de ejercicios, y para fomentar la reflexión y profundización sobre los contenidos de la asignatura mediante el foro de discusión que se creará a tal efecto.

XII.- Evaluación del aprendizaje

El requisito para superar la asignatura es conseguir 5 puntos sobre 10 en la evaluación final. En dicha evaluación se tendrán en cuenta los siguientes apartados:

- Participación en las clases de teoría, hasta un máximo de 1 punto.
- Participación en las clases prácticas, hasta un máximo de 2 puntos.
- Participación en el trabajo en grupo, hasta un máximo de 2 puntos.

- Participación en la exposición del trabajo, hasta un máximo de 1 punto.
- Calificación obtenida en el examen final de la asignatura, hasta un máximo de 6 puntos.

El examen final constará de cuestiones cortas en las que los alumnos deberán demostrar que son capaces de aplicar los conocimientos adquiridos para: resolver problemas concretos, explicar por qué son necesarias las medidas de seguridad estudiadas y en qué casos es recomendable aplicarlas...

La participación en clases de teoría se valorará teniendo en cuenta el número de veces y la calidad de las intervenciones de cada alumno. Para fomentar la participación, el profesor planteará cuestiones durante las explicaciones que, dependiendo del caso, podrán dar lugar a pequeños debates. Las opiniones de los alumnos serán siempre valoradas de forma positiva o neutra (si no aportan nada significativo o están equivocadas), pero en ningún caso restarán puntos.

La participación en clases prácticas se evaluará de dos formas. Durante la realización de los ejercicios, el profesor planteará cuestiones a los alumnos sobre los avances que éstos vayan realizando, para comprobar que comprenden y que saben explicar el trabajo que realizan. Al finalizar cada ejercicio, los alumnos entregarán en aula virtual el resultado final del trabajo realizado durante la sesión, que será evaluado posteriormente.