XV JENUI. Barcelona, 8-10 de julio de 2009
ISBN: 978-84-692-2758-9
http://jenui2009.fib.upc.edu/

Propuesta de diseño de la asignatura de Seguridad de Sistemas Informáticos

Miguel Riesco, M. Ángeles Díaz, José Manuel Redondo, Néstor García
Departamento de Informática
Universidad de Oviedo
c/ Calvo Sotelo, s/n. 33007 Oviedo
{albizu, fondon, redondojose, nestor}@uniovi.es

Resumen

Muchos de los actuales planes de estudios de informática carecen de asignaturas específicas sobre las materias relacionadas con la seguridad de los sistemas informáticos, y, dada la importancia creciente de esta materia, es de esperar que sea clave en los futuros planes de estudios. Además, su cuerpo curricular no está tan claro como en otras asignaturas más clásicas (sistemas operativos, bases de datos, etc).

En este artículo se plantea una propuesta de diseño de dicha asignatura, desde las competencias que se pretenden lograr hasta los contenidos a impartir y la metodología de trabajo, siguiendo la filosofía planteada por el Espacio Europeo de Educación Superior (EEES).

1. Introducción

La seguridad de los sistemas informáticos es una cuestión de creciente importancia en todos los ámbitos. El incremento del uso de los ordenadores, su utilización por usuarios sin conocimientos básicos de seguridad, la explosión de Internet y todos los servicios que lleva asociados, han hecho que aumenten exponencialmente el número de ataques y de potenciales atacantes a los sistemas informáticos. En los últimos años la gestión de la seguridad informática ha pasado a primer plano en todas empresas.

Sin embargo, esta situación no ha tenido reflejo inmediato en los planes de estudios de las titulaciones informáticas que se cursan hoy en día en las universidades españolas.

Haciendo un análisis de los planes de estudios actuales de las 156 titulaciones de Ingeniería Informática (tanto técnica como superior) existentes en España, se ha podido constatar que la materia de Seguridad sólo aparece en 66 de las mismas como asignatura con entidad propia. Además, una buena parte de ellas se centran casi exclusivamente en el estudio de la criptografía y sus aplicaciones.

Es de suponer que esta situación cambiará radicalmente con los nuevos planes de estudios, dada la importancia que esta materia ha ido adquiriendo en los últimos años. Esta necesidad ya lleva tiempo siendo apuntada [3].

El Computer Curricula 2005 de ACM [1] refleja también esta importancia, dado que aparecen dos materias (*Security: issues and principles* y *Security: implementation and management*) que forma parte del currículo de las 5 especialidades en él propuestas.

En este trabajo se describe en detalle una propuesta para el diseño de una asignatura de Seguridad de Sistemas Informáticos dentro del marco propuesto por el EEES.

2. Contexto académico

En el plan de estudios actual de la E. U. Ingeniería Técnica en Informática de Oviedo, la asignatura de Seguridad de Sistemas Informáticos aparece como optativa dentro de la intensificación de Admón. de Sistemas. Es una asignatura cuatrimestral que cuenta con 6 créditos, 3 teóricos y 3 prácticos. Está pensada para que la cursen alumnos de tercer curso.

Dentro de esta intensificación, se cursa previamente la asignatura de *Administración de Sistemas y Redes*, con la que está íntimamente relacionada.

Otra asignatura relacionada y que aparece en el plan de estudios es *Aspectos Legales, Éticos y Profesionales de la Informática.*

3. Competencias a desarrollar

Para iniciar el diseño de la asignatura, partimos de la competencia o competencias que ésta tiene

asignadas dentro de la definición proporcionada por la titulación [2]. Para la asignatura de Seguridad de Sistemas Informáticos, la principal competencia puede ser enunciada de la siguiente manera: *Gestionar la seguridad del sistema informático de una empresa.* Para lograr esta competencia puede subdividirse en tres subcompentecias técnicas y 4 transversales:

1. *Identificar los riesgos que pueden comprometer la seguridad de un sistema informático.* Es necesario conocer los distintos tipos de amenazas y riesgos en general, así como los tipos de daños que pueden afectar a un sistema informático. El primer paso que debe realizar el experto en seguridad es analizar los tipos de riesgos a los que puede enfrentarse para, a partir de ahí, diseñar la política de seguridad adecuada
2. *Plantear políticas de gestión de riesgos y de aseguramiento de la seguridad*. Partiendo del análisis de un sistema y con unos requisitos de seguridad propuestos, el experto deberá diseñar la política de seguridad adecuada.
3. *Desplegar las medidas planteadas en la política definida*. El experto en seguridad debe conocer y manejar los mecanismos de control de riesgos que puede tener disponibles, en los distintos niveles, sistema operativo, redes, programas, etc.

Dentro de la gestión de la seguridad de un sistema informático, el profesional debe contar con ciertas habilidades transversales indispensables para un buen desenvolvimiento en el trabajo:

4. *Ser capaz de mantenerse al día*. La gestión y mantenimiento de la seguridad de un sistema informático no logra su objetivo si no mantiene un altísimo nivel de actualización
   4.1 *Aprendizaje autónomo*. Como consecuencia de la necesidad de actualización diaria, el aprendizaje autónomo constituye el principal modo de trabajo.
   4.2 *Búsqueda de información actualizada*. Es una habilidad fundamental para poder mantenerse al día.
5. *Comunicación interpersonal*. Uno de los aspectos que competen al experto en seguridad de un sistema es el trato con el resto de los trabajadores de la empresa, a los que debe informar y concienciar de la realización de ciertos protocolos de seguridad
   5.1 *Habilidad de comunicación y expresión oral*. La capacidad para explicar a los usuarios del sistema las normas necesarias para lograr niveles de seguridad adecuados resulta decisiva a la hora de incorporar políticas de seguridad eficientes.
   5.2 *Capacidad de liderazgo*. El experto en seguridad deberá, no sólo comunicar al resto de empleados la necesidad de realización de tareas y protocolos de seguridad que, en principio, pueden dificultar el trabajo cotidiano, sino convencerlos de manera no impositiva de su capital importancia.
6. *Elaboración de documentación técnica*. Resulta fundamental una buena documentación de las políticas diseñadas, de forma que el lenguaje sea claro y adaptado a los distintos tipos de usuarios a los que vaya dirigido.
7. *Ética y deontología profesional*. Es evidente que el conocimiento de los riesgos y soluciones que afectan a un sistema informático debe siempre ir acompañado de un uso profesionalmente correcto de todo ello. Por otra parte, el experto en seguridad deberá conocer la legislación vigente en todos los aspectos relativos a la seguridad del sistema.

4. Competencias previas

Para poder cursar con éxito la asignatura el alumno debe poseer las siguientes competencias antes de estudiar la asignatura:

1. Conocer los fundamentos de la arquitectura de sistemas informáticos
2. Conocer los fundamentos de redes de ordenadores
3. Conocer los fundamentos de administración de sistemas operativos

5. Objetivos de aprendizaje

Mediante esta asignatura se pretende que el alumno se capaz de:

1. Identificar los riesgos que pueden comprometer la seguridad de un sistema informático.
   1.1 Conocer las amenazas, vulnerabilidades, técnicas de ataque y el resto de factores

que intervienen en la seguridad de un sistema informático.
1.2 Identificar los daños que pueden causarse a un sistema.
2. Plantear políticas de gestión de riesgos y de aseguramiento de la seguridad.
2.1 Conocer distintos modelos de seguridad.
2.2 Utilizar metodologías de gestión de riesgos.
2.3 Diseñar sistemas informáticos seguros.
3. Desplegar las medidas planteadas en la política definida.
3.1 Manejar mecanismos de seguridad proporcionados por el sistema operativo.
3.2 Manejar mecanismos de seguridad en el uso de redes.
3.3 Implantar mecanismos de seguridad física.
3.4 Solventar posibles vulnerabilidades de aplicaciones.
4. Ser capaces de adaptarse de manera autónoma a las nuevas amenazas y tecnologías que van apareciendo.
5. Ser capaz de concienciar a los usuarios del sistema para que sigan los protocolos establecidos.
6. Coordinar y desenvolverse en equipos de trabajo.
7. Desarrollar documentación sobre la seguridad del sistema adaptada a distintos niveles de usuarios
8. Adquirir un código ético de comportamiento de todos los aspectos relativos a la gestión de un sistema informático y la información que soporta.

6. Contenidos a desarrollar

A continuación se describe una propuesta de selección de contenidos a desarrollar en la asignatura, en base a los objetivos propuestos y a la situación actual de la tecnología. Esta selección deberá adaptarse dinámicamente a los cambios producidos en la tecnología, que deben ser revisados anualmente, dada la rápida evolución que éstos sufren.

En el planteamiento el contenido no se desglosa en teoría y práctica, sino que ambos aspectos están entrelazados y no se conciben de forma aislada cada uno de ellos.

Los contenidos a tratar serán los siguientes:

1. Visión general de la seguridad
1.1 Factores que intervienen en la seguridad de un sistema informático: amenazas, vulnerabilidades, componentes afectados, daños.
1.2 Modelos de estrategia de defensa y políticas de seguridad.
2. Seguridad en Sistemas Operativos.
2.1 Autenticación de usuarios y máquinas.
2.2 Control de acceso a recursos.
2.3 Sistemas de encriptación de ficheros.
2.4 Sistemas de control de ejecución de programas confiables (código firmado).
2.5 Vulnerabilidades del SSOO.
3. Seguridad en redes.
3.1 Riesgos en las comunicaciones.
3.2 Conceptos de criptografía.
3.3 Protocolos de red seguros: SSL, IPSEC, PPTP, L2TP/IPSEC, https, etc.
3.4 Certificados y firmas digitales.
3.5 Riesgos en protocolos DHCP, DNS, NAT y PAT.
3.6 Cortafuegos.
3.7 Redes privadas virtuales (VPN).
3.8 Otras soluciones: NAC, NAP, etc.
4. Seguridad en aplicaciones.
4.1 Vulnerabilidad de aplicaciones instaladas (servidores web, bases de datos, P2P ...)
4.2 Prevención de vulnerabilidades en el desarrollo de aplicaciones.
5. Seguridad física.
5.1 Seguridad en el acceso físico.
5.2 Seguridad en la instalación.

7. Metodología docente

El plan de trabajo propuesto se aleja del modelo tradicional de "clase de teoría - clase de prácticas", planteándose en su lugar una serie de actividades que cubran los objetivos de aprendizaje sobre los contenidos propuestos. Así pues, cada actividad integrará elementos teóricos, prácticos, de trabajo autónomo, de trabajo en grupo, de seguimiento y control, etc.

En estas actividades se utilizarán diversas técnicas, en función de los objetivos buscados en cada caso. El diseño de las actividades está pensado para cubrir tanto el tiempo presencial en el aula, donde el profesor controla el proceso de aprendizaje, como tiempo no presencial en el

que el alumno tiene marcadas las pautas de trabajo por su cuenta.

Los métodos a utilizar serán algunos de los siguientes:

- Lección magistral.
- Uso de mapas conceptuales.
- Utilización de wikis
- Trabajo en equipo, técnica del puzzle.
- Trabajo práctico individual.
- Trabajo práctico en grupo.
- Trabajo autónomo del alumno.

A continuación se detalla el uso de cada técnica en las distintas actividades propuestas.

8. Plan de trabajo detallado

A continuación se enumeran las distintas actividades que se van a desarrollar para cumplimentar los objetivos de aprendizaje en base a los contenidos planteados.

El curso está planificado para un total de 15 semanas con 2 clases de 2 horas a la semana.

8.1. Actividad 1. Visión General

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 1, 4, 7 y 6 en base a los contenidos 1.1.

Descripción de la actividad

Para identificar los riesgos que pueden comprometer la seguridad de un sistema informático (objetivo 1) se plantea una actividad basada en la técnica del puzzle.

A partir de una pequeña introducción por parte del profesor, donde se describe, a través de un mapa conceptual, los principales aspectos relativos a los riesgos de seguridad de un sistema, se plantean 5 temas de trabajo, que se distribuyen entre 5 grupos (objetivo 6) de 4 alumnos.

Cada grupo deberá investigar (objetivo 4) sobre el tema asignado, utilizando tiempo presencial y no presencial.

1	Presentación. Propuesta trabajos.
2	Trabajo en grupo asignado.
3	Puzzle. Exposición general. Conclusiones.

Tabla 1. Planificación Actividad 1

Tras esta fase de investigación y elaboración del trabajo, los alumnos de cada grupo se redistribuyen por el resto de los grupos (según técnica del puzzle), explicando el trabajo realizado al resto de los compañeros del nuevo grupo.

Finalmente se plantea una sesión de puesta en común en la que se verifica que estén contemplados todos los aspectos a considerar y se obtiene un documento final consensuado.

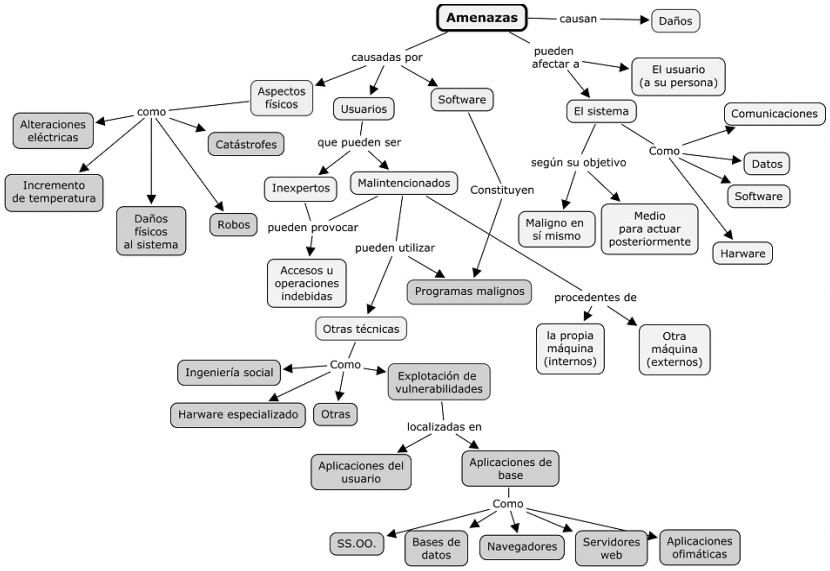

Figura 1. Mapa introductorio de la actividad 1

8.2. Actividad 2. Amenazas

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 1, 4, 7 y 8 en base a los contenidos 1, 2.5, 3.1, 4.1 y 5.

Descripción de la actividad

Esta actividad tiene como objetivo profundizar en el aspecto técnico de los riesgos más habituales. El alumno debe tomar el papel de cracker, para lo cual llevará a cabo una búsqueda de herramientas para desarrollar su papel (objetivos 1 y 4).

Cada alumno buscará información y elegirá una herramienta de ataque a sistemas, y realizará un pequeño trabajo (utilizando un wiki) sobre su finalidad, forma de uso, etc.

4	Propuesta. Búsqueda información.
5	Prueba. Elaboración documentación.

Tabla 2. Planificación Actividad 2

Un aspecto importante a considerar en cada caso es la búsqueda en la legislación las consecuencias jurídicas que tendría un ataque del tipo elegido (objetivo 8).

8.3. Actividad 3. Políticas de seguridad

Finalidad

En esta actividad se desarrollan los objetivos 2.1, 2.2, 4, 6 y 7 en base al contenido 1.2.

Descripción de la actividad

Para trabajar sobre gestión de riesgos y las políticas de seguridad (objetivo 2.1 y 2.2), el profesor expondrá una visión general de todos los aspectos involucrados, apoyándose en mapas conceptuales que los relacionen.

6	Exposición y propuesta de trabajo.
7	Trabajo en grupo asignado.
8	Puzzle. Exposición general. Conclusiones.

Tabla 3. Planificación Actividad 3

A partir de ahí se propondrá al alumno, trabajando en grupo (objetivo 6), la profundización sobre aspectos concretos, mediante la búsqueda de información a partir de una *guía de lectura*, en la que se enumeran los puntos a considerar en el trabajo. El resto de la actividad será similar a la primera, utilizando la técnica del puzzle.

8.4. Actividad 4. Seguridad en Windows

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 3.1 y 4 en base al contenido 2.

Descripción de la actividad

Esta actividad tiene por objeto conocer y utilizar las técnicas relativas a la seguridad que ofrece el sistema Operativo Windows, por lo que se trata fundamentalmente de desarrollar habilidades técnicas.

La actividad alternará la explicación del profesor sobre aspectos concretos con la puesta en práctica real de los mismos por parte de los alumnos. En muchos casos será necesaria la consulta de los manuales del sistema para llevar a cabo los ejercicios propuestos (objetivo de aprendizaje autónomo 4).

9	Presentación. Instalación VmWare.
11	Seguridad Windows: NTFS.
12	Seguridad Windows: EFS.
13	Seguridad Windows: Active Directory.
14	Seguridad Windows: Políticas de grupo.

Tabla 4. Planificación Actividad 4

Esta actividad, por tanto, sigue un modelo que denominaremos de *práctica dirigida* con trabajo individual del alumno.

8.5. Actividad 5. Seguridad en Linux

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 3.1 y 4 en base al contenido 2.

15	Introducción a SELinux. Instalación.
16	SELinux. Control de acceso.
17	SELinux. Usuarios y aplicaciones.
18	SELinux. Ficheros de configuración.

Tabla 5. Planificación Actividad 5

Descripción de la actividad

El desarrollo de esta actividad es equivalente a la actividad anterior, pero desarrollando habilidades técnicas sobre el sistema operativo Linux.

8.6. Actividad 6. Seguridad en redes

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 3.2 y 4 en base al contenido 3.

Descripción de la actividad

Esta actividad se desarrollará de manera similar a las dos anteriores.

Para cada protocolo o servicio de red se alternarán explicaciones breves del profesor con la configuración, por parte de los alumnos, de los equipos para utilizar el protocolo o servicio correspondiente y/o en la utilización de herramientas de monitorización para comprobar los problemas que pueden producirse.

19	Introducción. Conceptos de criptografía.
20	Certificados. Protocolos ssh, https.
21	Protocolo IPSEC.
22	DHCP, DNS, NAT, PAT. Cortafuegos.
23	PPTP, L2TP/IPSEC
24	NAC, NAP.

Tabla 6. Planificación Actividad 6

En esta actividad se irá alternando también el trabajo sobre Windows y sobre Linux.

8.7. Actividad 7. Seguridad de aplicaciones

Finalidad

Esta actividad está destinada al desarrollo de los objetivos 3.4 y 5 en base a los contenidos 4.

25	Exposición y propuesta de trabajo.
26	Trabajo en grupo asignado.
27	Exposición del trabajo realizado.

Tabla 7. Planificación Actividad 7

Descripción de la actividad

Esta actividad comenzará con la exposición del profesor de vulnerabilidades conocidas en aplicaciones (inyección sql, inyección XML, envenenamiento de cookies, URL Jumping, etc…).

A continuación, se asignará a cada grupo un tipo de vulnerabilidad o de ataque para que realicen un estudio más profundo sobre él, documentándolo usando el wiki, y realizando, finalmente, una presentación pública de su trabajo.

8.8. Actividad 8. Diseño de una política de seguridad

Finalidad

Se trata de una actividad integradora que pretende afianzar todos los objetivos planteados. Esta actividad está destinada al desarrollo de los objetivos 1, 2, 3, 4, 6, 7 y 8 en base a los contenidos 1, 2, 3, 4 y 5.

Descripción de la actividad

Por medio de esta actividad el alumno demostrará su competencia para diseñar y establecer una política de seguridad para una empresa tipo.

Aquí será fundamental el trabajo del alumno, puesto que se asignará a cada grupo un tipo de empresa con unas determinadas características y el grupo deberá diseñar la política de seguridad de la empresa, así como describir los mecanismos que implantarán dicha política.

28	Exposición y propuesta de trabajo.
29	Trabajo en grupo asignado.
30	Trabajo en grupo asignado.

Tabla 8. Planificación Actividad 8

Durante tres sesiones presenciales se irá guiando el trabajo de los alumnos para, al final, publicar un informe técnico que recoja el trabajo realizado.

9. Verificación de la propuesta

Para verificar que todos los contenidos previstos son cubiertos por las actividades a realizar se ha confeccionado la Tabla 9a, donde se muestran los contenidos que cubre cada actividad.

	1.1	1.2	2.1	2.2	2.3	2.4	2.5	3.1	3.2	3.3	3.4	3.5	3.6	3.7	4.1	4.2	5
1	■																
2	■	■					■	■							■		■
3		■															
4			■	■	■	■	■										
5			■	■	■	■	■										
6								■	■	■	■	■	■	■			
7															■	■	
8	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

(a) Actividades-Contenidos

	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	3.4	4	5	6	7	8
1	■	■								■		■	■	
2	■	■								■		■	■	■
3			■	■						■		■	■	
4						■				■				
5						■				■				
6							■			■				
7									■		■			
8	■	■	■	■	■	■	■	■	■	■	■	■	■	■

(b) Actividades-Objetivos de aprendizaje

Tabla 9. Relación entre las actividades y los contenidos y objetivos sobre las que trabajan

Por su parte, la Tabla 9b muestra los objetivos cubiertos por cada actividad.

Puede observarse en la primera de las tablas cómo las actividades van cubriendo los contenidos en secuencia, salvo la actividad 2 donde el alumno investiga sobre cualquier problema de seguridad que más tarde se estudiará en detalle.

Otro aspecto a destacar es la aparición en la Tabla 9b de una "columna" bajo el objetivo 4 (*Ser capaces de adaptarse de manera autónoma a las nuevas amenazas y tecnologías que van apareciendo*), puesto que este objetivo se trabaja en prácticamente todas las actividades. Esto no es casual, sino que se corresponde con la importancia que se quiere dar a este objetivo en la asignatura. Las amenazas y ataques que sufren los sistemas informáticos son cada vez más numerosos y novedosos, por lo que un profesional de la informática debe ser capaz de actualizar constantemente su formación de manera autónoma a lo largo de su vida.

Por último, incidir también la función integradora que tiene la actividad 8 (*Diseño de una política de seguridad*), lo que se ve reflejado en las dos tablas al cubrir esta actividad todos los objetivos y contenidos.

10. Evaluación

Dado que la asignatura consta de un conjunto de actividades que el alumno debe realizar, se utilizará un portafolios del alumno para realizar el seguimiento de todos sus trabajos.

Dicho portafolios estará soportado por la plataforma de campus virtual existente en la Universidad.

La evaluación de cada actividad dependerá del tipo de la misma. En cualquier caso, se evaluará tanto el resultado final como el proceso de realización del trabajo.

Dado que todos los trabajos alternan actividades presenciales y no presenciales, las fases presenciales serán utilizadas por el profesor para ir guiando y corrigiendo a los alumnos, así como para evaluar el proceso de realización de la actividad.

El uso de *guías de lectura* dirige al alumno en el proceso de búsqueda de información. Las *tablas de criterios de evaluación* permiten que el alumno se autoevalúe como parte del proceso de realización del trabajo. También será utilizada por el profesor para calificar la actividad en cuestión.

11. Infraestructura de prácticas

Como se ha expuesto en los apartados anteriores, esta asignatura tiene un alto contenido práctico. Este contenido, además, tiene unas características peculiares que hacen que deba pensarse en una infraestructura no habitual en otras asignaturas. Entre estas particularidades podemos citar las siguientes:

- Es necesario disponer de máquinas con distintos sistemas operativos.
- Esas máquinas deben estar en red y funcionando simultáneamente.
- Se van a realizar pruebas que pueden interferir con el funcionamiento normal tanto de las máquinas como de la red.
- Cada alumno debería disponer de su propia red y su conjunto de máquinas.
- El alumno debería poder reproducir la infraestructura de prácticas en su domicilio, con el fin de realizar allí los trabajos no presenciales y hacer sus propias pruebas.

En definitiva, lo que pretendemos es que cada alumno pueda disponer de una red privada con al menos 4 máquinas (un Windows Server, un cliente Windows, un servidor Linux y un cliente Linux) funcionando a la vez.

Obviamente, no se suele contar con laboratorios donde poner a disposición de cada alumno este número de recursos. Afortunadamente, la virtualización [4] aparece como una solución ideal para nuestro caso.

De todas las opciones de virtualización disponibles nos hemos decantado por utilizar el software VMware [6] puesto que, pese ser una herramienta comercial, la versión Server[1] es gratuita. Además, su instalación, configuración y uso es relativamente sencilla

En resumen, nuestra infraestructura de prácticas estará montada sobre la ejecución de VMware Server, sobre el cual tendremos creadas 4 máquinas virtuales, dos servidores y dos

[1] Se ha utilizado VMware Server versión 1.0.8, desaconsejándose la versión 2.0, por motivos, fundamentalmente, de rendimiento.

clientes, sobre las cuales realizaremos las pruebas. Los servidores serán configurados para evitar problemas de seguridad, mientras que los clientes realizarán distintas tareas de monitorización y ataque a la red y a los servidores.

12. Valoración de tiempo no presencial

En la Tabla 10 se muestra la previsión de horas a emplear por el alumno en cada actividad.

Actividad	Pres.	N.Pres.
1. Visión General	6	4
2. Amenazas	4	2
3. Políticas de seguridad	6	4
4. Seguridad Windows	10	5
5. Seguridad Linux	8	4
6. Seguridad Redes	14	7
7. Seguridad aplicaciones	6	4
8. Diseño política seguridad	6	10
Total	**60**	**40**

Tabla 10. Planificación temporal del trabajo

Como se puede ver en la tabla el tiempo presencial supera al no presencial, pero hay que considerar que la mayor parte de este tiempo se dedica a trabajo activo del alumno. Todas las clases son en el laboratorio, no haciendo distinción entre clase de teoría y clase de prácticas.

13. Conclusiones

La materia de Seguridad de Sistemas Informáticos pasará a constituir una materia crucial en los planes de estudios de todas las titulaciones informáticas. Actualmente, se están rediseñando dichos planes, para adaptarlos al marco que propone el EEES.

Bajo estas circunstancias resulta de gran ayuda disponer de referentes a la hora de plantear esta materia, sobre todo teniendo en cuenta que el número de titulaciones actuales que incluyen esta materia es relativamente bajo.

En este trabajo se ha realizado un diseño de una asignatura sobre Seguridad Informática siguiendo las directrices del EEES. Los aspectos fundamentales que contempla son los siguientes:

- Análisis de las competencias asignadas dentro de la titulación.
- Inclusión de competencias tanto técnicas como transversales
- Elaboración de los objetivos de aprendizaje a partir de las competencias asignadas.
- Selección de contenidos que desarrollan los objetivos planteados.
- Aplicación de una metodología basada en actividades, para lograr un aprendizaje activo.
- Diseño detallado del plan detallado, tanto presencial como no presencial.
- Evaluación formativa y continua, con seguimiento del proceso de aprendizaje y uso de portafolios del alumno como herramienta.

Este planteamiento constituye un diseño moderno, donde se ha trabajado en dos líneas: desde el punto de vista técnico, haciendo un análisis de las necesidades actuales de la empresa, y desde un punto de vista académico, aplicando la experiencia de innovación docente que hemos ido acumulando en los últimos años [5].

Referencias

[1] ACM/IEEE Joint Task Force for Computing Curricula (2005). *Computing Curricula 2005: The Overview Report*. http://www.acm.org/education/curricula.html#CC2005.

[2] Juan, A. A., de Andrés, J., Díaz Fondón, M. A. et al. *Definición de Competencias Específicas y Genéricas del Ingeniero en Informática*. En Docencia Universitaria: Proyectos de Innovación Docente. Documentos ICE. Universidad de Oviedo. 2006

[3] Ramió Aguirre, J. *Introducción de las enseñanzas de seguridad informática en los planes de estudios de las ingenierías del siglo XXI*. En Actas de las JENUI 2001, Palma de Mallorca, Julio 2001.

[4] Ribadas, F. J., Barcala, F. M., Darriba, V. y Otero, J. *Diseño de un entorno virtualizado para la docencia práctica de Seguridad en Sistemas de Información*. En Actas de las JENUI 2008, Granada, Julio 2008

[5] Rodríguez, R., Hernández, N.y Díaz Fondón, M.A. *Cómo planificar asignaturas para el aprendizaje de competencias*. Documentos ICE. Universidad de Oviedo. Oviedo, 2007.

[6] VMware: http://www.vmware.com/