Experiencia en la adaptación de una asignatura de máster para su impartición completa a distancia

1st Julián Viejo-Cortés
Dept. Tecnología Electrónica
Universidad de Sevilla
Sevilla, España
julian@us.es

2nd Alejandro Carrasco-Muñoz
Dept. Tecnología Electrónica
Universidad de Sevilla
Sevilla, España
acarrasco@us.es

3rd Jorge Juan-Chico
Dept. Tecnología Electrónica
Universidad de Sevilla
Sevilla, España
jjchico@dte.us.es

4th Paulino Ruiz-de-Clavijo-Vázquez
Dept. Tecnología Electrónica
Universidad de Sevilla
Sevilla, España
pruiz@us.es

5th Germán Cano-Quiveu
Dept. Tecnología Electrónica
Universidad de Sevilla
Sevilla, España
germancq@dte.us.es

***Resumen*—En la Sociedad de la Información actual, Internet está presente en la mayoría de las actividades cotidianas que realizan las personas. Este hecho ofrece a las Universidades nuevas posibilidades de acercar sus titulaciones a personas que difícilmente podrían cursarlas de forma presencial debido a no poder compatibilizar los horarios de dichas titulaciones con su vida laboral o personal. En esta comunicación se presenta la experiencia de adaptar una titulación de máster desde una modalidad presencial a otra totalmente a distancia. En concreto, se proporcionarán los resultados obtenidos tras impartir la asignatura "Gestión de Riesgos y Seguridad en Red" en el curso 2018-2019 siguiendo esta modalidad a distancia.**

***Index Terms*—Docencia en máster, educación a distancia, seguridad en redes de computadores**

I. Introducción

Este trabajo se enmarca dentro del Máster Universitario en Ingeniería Informática (MII) de la Escuela Técnica Superior de Ingeniería Informática (ETSII) de la Universidad de Sevilla y pretende presentar la experiencia adquirida tras la adaptación de esta titulación a una modalidad de educación totalmente a distancia.

El Máster Universitario en Ingeniería Informática en su modalidad presencial comenzó a impartirse en el curso 2014-2015. Su carga lectiva era de 90 créditos impartidos durante dos cursos académicos (60 créditos en el primero y 30 en el segundo). Esta duración se debió a que este máster cumplía con la Resolución de 8 de junio de 2009 de la Secretaría General de Universidades capacitando para el ejercicio de la profesión de Ingeniero en Informática. En este sentido, en las asignaturas impartidas se abordaron multitud de contenidos basados en los últimos estándares y tecnologías cubriendo entre otras: *Cloud Computing*, Transformación Digital, Internet de las Cosas, Ciberseguridad, Inteligencia Artificial, *Deep Learning*, *eHealth*, *Big Data*, etc.

Este trabajo ha sido parcialmente financiado por el Ministerio de Industria y Competitividad del Gobierno de España a través del proyecto TIN2017-89951-P (BootTimeIoT) y por el Fondo Europeo de Desarrollo Regional (FEDER).

Una característica importante de este máster fue que las asignaturas se organizaron de forma que no se impartían todas simultáneamente sino que se fueron distribuyendo de dos en dos a lo largo de todo el curso. Tomando como referencia una asignatura con una carga lectiva de 7,2 créditos, esto implicó concentrar todas las clases presenciales de esas dos asignaturas en una franja de tiempo de seis semanas, resultando un total de 12 horas de clase a la semana por cada asignatura. Así, la primera asignatura impartía los lunes y los miércoles un total de 10 horas (una sesión de 5 horas cada día) y la segunda hacía lo mismo los martes y los jueves. El viernes cada asignatura impartía dos horas.

Esta forma de organizar las asignaturas estuvo motivada por el tipo de metodología docente que se pretendió impartir en este máster. En concreto, se utilizaron metodologías de Aprendizaje Cooperativo (AC) y Aprendizaje Basado en Proyectos (ABP) [1]. En este sentido, en las sesiones de 5 horas se planteaban diversos proyectos que los alumnos de forma cooperativa debían completar usando la técnica del puzle [1]. Finalmente, los viernes debían presentar los resultados de los diferentes proyectos, procediendo los profesores a su evaluación. Este planteamiento obligaba a los alumnos a asistir a todas las clases programadas para la correcta realización en grupo de las diferentes actividades colaborativas.

De acuerdo al Autoinforme Global de Acreditación de Títulos [2] realizado en el año 2017, los indicadores de rendimiento y éxito de este máster se situaban en el 92,94 % y 100 % respectivamente, pero sin embargo el número de estudiantes de nuevo ingreso y la demanda del título presentaba valores muy bajos (ver Tabla I). Como se observa en la Tabla I la tasa de matriculación se situó por debajo del 25 % en los dos primeros cursos. Si se tiene en cuenta que, de acuerdo al informe realizado en 2013 por la Conferencia de Directores y Decanos de Ingeniería Informática (CODDII) [3], la empleabilidad media de los titulados en el Grado en Ingeniería Informática es elevada (se situó en el 94,3 % en 2013) y que las clases

del máster durante estos dos primeros cursos se impartieron en horario de mañana se puede deducir que los alumnos difícilmente podían compaginar su trabajo con los horarios del máster.

Para el curso 2016-2017 en el plan de mejora de este título se propuso cambiar el horario de mañana por uno de tarde, lo cual tuvo el efecto esperado al incrementarse el número de matriculados en los dos siguientes cursos; así, la tasa de matriculación se incrementó alcanzando el 46,6 % en el curso 2017-2018 (ver Tabla I). Aunque estos datos mejoraron significativamente, ya que este nuevo horario permitía a los alumnos compaginar mejor su trabajo con los estudios del máster, en el curso 2018-2019 la ETSII afrontó el reto de actualizar este máster y ofertarlo totalmente a distancia.

En este trabajo se va a presentar cómo se ha renovado la asignatura "Gestión de Riesgos y Seguridad en Red" para su adaptación a la nueva modalidad no presencial. Asimismo, se van a presentar las principales dificultades encontradas y cómo se han solventado.

La estructura de este trabajo es la siguiente: tras una pequeña introducción que explica las características del Máster Universitario en Ingeniería Informática en su modalidad presencial, expuesta en la sección I, en la sección II se procede a la descripción de todas las acciones llevadas a cabo para impartir la asignatura comentada siguiendo una modalidad totalmente a distancia. Posteriormente, en la sección III se expondrán los principales resultados así como las dificultades que se han observado durante la ejecución de la asignatura durante el curso 2018-2019. Finalmente, en la sección IV se proporcionarán las conclusiones más importantes que se pueden extraer de este trabajo.

II. Estructura del MII no presencial

El Máster Universitario en Ingeniería Informática en su modalidad no presencial comenzó a impartirse en el curso 2018-2019, y al igual que en la versión presencial su carga lectiva es de 90 créditos que se imparten en dos cursos académicos. Asimismo, la organización de las asignaturas también se mantuvo, impartiéndose de dos en dos a lo largo de todo el curso. Esto se debió a que la experiencia en el máster presencial fue muy positiva, ya que esta distribución permite a los alumnos centrarse en exclusiva en las dos asignaturas que se están impartiendo en un momento determinado y a los profesores concentrar todo su esfuerzo durante las semanas que se imparte su asignatura.

La asignatura "Gestión de Riesgos y Seguridad en Red" es una asignatura de primer curso con una carga lectiva de 4,5 créditos y fue el resultado de dividir en dos la asignatura impartida previamente en el máster presencial. De acuerdo a dicha carga la asignatura tiene asignada cuatro semanas, en las cuales debe impartirse completamente, es decir, deben abordarse todos los contenidos y realizarse su evaluación.

Tabla I
Tasa de matriculación.

Curso	Nº de matriculados	Tasa*(%)
2014-2015	7	23,3
2015-2016	5	16,7
2016-2017	10	33,3
2017-2018	14	46,6

*la oferta fue de 30 plazas.

Tabla II
Estructuración en módulos de los contenidos de la asignatura.

Semana 1	
Módulo	**Título**
1	Introducción y objetivos
2	Fundamentos de la seguridad en redes
3	Ataques contra la seguridad en redes
Semana 2	
Módulo	**Título**
4	Introducción a la seguridad perimetral
5	Cortafuegos
6	Redes Privadas Virtuales
Semana 3	
Módulo	**Título**
7	Introducción al proceso de gestión de riesgos
8	Análisis de riesgos
9	Tratamiento y gestión de riesgos
Semana 4	
Entrega y evaluación de los proyectos	

II-A. Contenidos y metodologías aplicadas

Dentro de la Universidad de Sevilla ya se contaba con experiencia en la puesta en marcha y desarrollo de un máster a distancia [4]. Según los autores de esta experiencia, al ser el Máster de Microelectrónica impartido a distancia, las metodologías docentes son las propias y exclusivas de procesos de e-learning, estando basada la enseñanza en el uso de una plataforma de enseñanza virtual que facilita el acceso a todas las herramientas de gestión de cursos, inclusión de materiales, desarrollo de contenidos, evaluación, comunicación, foros, tutorías, etc. En base a esta experiencia, a continuación se van a presentar todos los aspectos concretos implementados para la adaptación de la asignatura "Gestión de Riesgos y Seguridad en Red" a la modalidad a distancia.

En relación con los contenidos y las metodologías aplicadas para impartirlos se optó principalmente por una metodología basada en proyectos (ABP). La opción del trabajo colaborativo fue descartada ya que al desconocer los horarios de trabajo de cada alumno se consideró más adecuado que cada uno se organizará libremente en lugar de obligarlos a reunirse de manera remota en un mismo horario para repartirse y completar las diferentes tareas. En este sentido, los contenidos de esta asignatura se han estructurado en diferentes módulos que se imparten durante las tres primeras semanas (ver Tabla II), dedicando la última semana a la entrega y evaluación de los proyectos planteados en cada módulo.

Cuando se aplica una metodología basada en proyectos en clases donde los alumnos asisten presencialmente, generalmente los profesores exponen en primer lugar los contenidos teóricos que se van a tratar y a continuación los alumnos tienen que realizar ejercicios o actividades prácticas relacionados

con dichos contenidos. Además, los alumnos cuentan con la ayuda del profesor, si es necesaria, durante el transcurso del proyecto. En este aspecto, cuando se aplica esta metodología en un modelo de clases no presenciales el profesor no está disponible, o al menos no cuando el alumno lo necesita. Para suplir esta carencia del profesor se han propuesto las siguientes acciones:

1. Elaboración de vídeos con los contenidos teóricos de cada módulo. Antes de abordar los proyectos el alumno debe visualizar los vídeos explicativos de ese módulo y completar una autoevaluación. Aunque esta autoevaluación no cuenta para la nota final es necesario que los alumnos obtengan como mínimo un 70 % de respuestas acertadas para desbloquear los contenidos del siguiente módulo. La duración de cada vídeo es corta, oscilando entre los 5 y los 10 minutos.
2. El documento que expone el proyecto a realizar es autocontenido. Este documento no sólo incluye la descripción del proyecto sino que se aporta material de apoyo y bibliográfico con toda la información necesaria para su correcta realización.
3. Se han habilitado diferentes formas para contactar con los profesores. Así, dentro de la plataforma de Enseñanza Virtual, basada en *Blackboard* [5], se han habilitado foros donde los alumnos pueden realizar consultas; además, se dispone de la herramienta *Blackboard Collaborate* que permite habilitar un salón de clases virtuales. Fuera de esta plataforma se ha empleado la herramienta *Microsoft Teams* [6] que pone a disposición de los alumnos y profesores salas de conversación públicas y privadas y permite hacer vídeos, compartir ficheros y acceder a diferentes recursos como bloc de notas, Powerpoint, etc.

Como se ha mostrado en la Tabla II esta asignatura se ha dividido en un total de 9 módulos. Así, en el primer módulo de la primera semana, mediante un conjunto de vídeos, se presenta la información de la asignatura: conocimientos previos necesarios, índice detallado de los contenidos, recomendaciones y objetivos. A continuación, en el segundo módulo se exponen los fundamentos de la seguridad en redes: definición y enfoques de la seguridad, definición de conceptos y principios de criptografía. Finalmente, en el tercer módulo de esta primera semana se explican los ataques contra la seguridad en redes: escaneo de puertos, *sniffing*, *spoofing*, denegación de servicio (DoS), etc. Una vez finalizados estos tres módulos los alumnos pueden realizar la autoevaluación y los proyectos planteados para esta primera semana (ver Tabla III).

Dada la naturaleza técnica de la asignatura que se presenta en este trabajo resulta imprescindible el uso de un laboratorio de redes para la realización de los proyectos, tal y como ocurría en la modalidad presencial del máster. Asimismo, en el caso de otras asignaturas del máster que precisan manejar hardware (placas basadas en procesador, microcontroladores, etc.) existe la opción de proporcionar este material a los alumnos por correo o que el propio alumno lo adquiera,

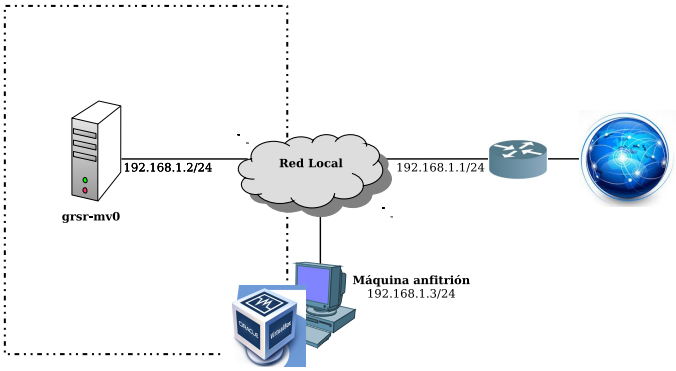

Figura 1. Topología de red para los primeros proyectos realizados.

facilitando para ello la lista de dispositivos que se van a utilizar. En el caso concreto de la asignatura descrita en este trabajo, el problema de los laboratorios de redes se ha solventado mediante el despliegue de un laboratorio de redes virtual. Para ello, la herramienta de virtualización seleccionada ha sido *VirtualBox* [7]. Un aspecto importante es que se ha proporcionado a los alumnos una imagen de una máquina virtual preinstalada, que incluye una instalación mínima de una máquina Linux (distribución Debian), y son los propios alumnos los que deben realizar la importación y configuración de las diferentes máquinas virtuales que componen el laboratorio de redes virtual. Para ello, también se les ha proporcionado material audiovisual y manuales explicando todo el proceso.

Para los proyectos 1 y 2 se comienza con una topología de red básica (Fig. 1). Sobre la máquina virtual disponible, denominada *grsr-mv0*, los alumnos deben crear una pareja de claves pública y privada y completar un conjunto de actividades: cifrado y descifrado de mensajes, comprobación de la firma digital y envío de correo electrónico seguro, donde se debe realizar un intercambio de mensajes de correo electrónico con el profesor, que deben ir correctamente firmados y cifrados. Dado que son los primeros proyectos y el nivel de dificultad es medio, el peso de la nota final asignado a cada uno ha sido del 10 % (Tabla III).

El tercer proyecto requiere un escenario más complejo, de-

Tabla III
PROYECTOS REALIZADOS Y PESOS DE LA NOTA FINAL ASIGNADOS A CADA UNO.

Semana 1		
Proyecto	**Título**	**Peso**
1	OpenPGP	10 %
2	Correo electrónico seguro	10 %
3	Seguridad de la capa de transporte (SSL/TLS)	20 %
Semana 2		
Proyecto	**Título**	**Peso**
4	Filtrado de paquetes con *Netfilter*	30 %
5	Redes Privadas Virtuales basadas en TINC	10 %
Semana 3		
Proyecto	**Título**	**Peso**
6	Aplicación del proceso de gestión de riesgos a un sistema de información	20 %

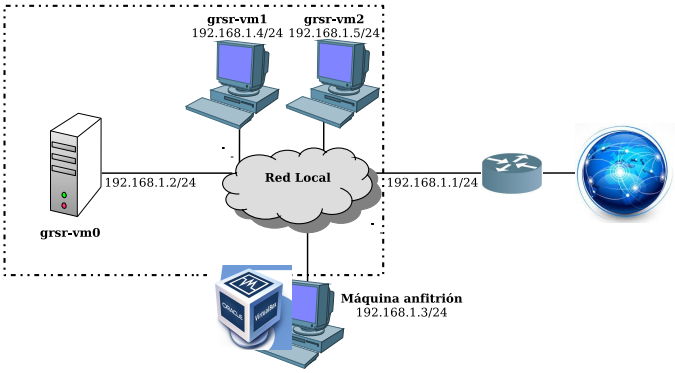

Figura 2. Topología de red para el tercer proyecto realizado.

biendo los alumnos añadir y configurar dos máquinas virtuales adicionales (Fig. 2). En este proyecto se introduce el protocolo *Secure Sockets Layer* (SSL) y su versión mejorada *Transport Layer Security* (TLS). Estos protocolos son empleados por las aplicaciones (servidores web, de correo electrónico, etc.) ya que dotan de seguridad al nivel de transporte. Así, tras la descripción del protocolo, se propone a los alumnos configurar dos servicios de red seguros, un servidor web y un servidor del protocolo de transferencia de ficheros FTP (File Transfer Protocol), en las máquinas virtuales 1 y 2 respectivamente. Las pruebas de funcionamiento de los servidores deben ser realizadas desde la máquina virtual 0. Como resultado de este proyecto los alumnos deben entregar un documento donde se relacionan todas las acciones y configuraciones que hay que realizar para aportar seguridad a dichos servicios. Al ser el nivel de esta actividad elevado se le ha asignado un peso del 20 %.

La segunda semana se compone de 3 módulos dedicados a introducir la seguridad perimetral y profundizar luego en los dos elementos principales de la misma: los cortafuegos (*firewalls*) y las Redes Privadas Virtuales (*Virtual Private Networks* - VPN). Al igual que en la primera semana tras visualizar todos los vídeos explicativos de estos módulos los alumnos pueden realizar la autoevaluación y los proyectos planteados para esta segunda semana (ver Tabla III).

El proyecto 4 requiere desplegar la topología de red mostrada en la Fig. 3. Para ello, también se proporciona a los alumnos un documento que explica detalladamente cómo adaptar la configuración de red de las máquinas virtuales para establecer un perímetro de seguridad en el laboratorio de redes virtual. En la Fig. 3 se observa cómo las tres máquinas virtuales están conectadas a una red virtual interna (192.168.2.0/24) que engloba el perímetro de seguridad. Además, la máquina virtual 0 también se conecta a la red externa (zona de riesgo) haciendo de puerta de enlace de la red interna. Con este proyecto se pretende que las dos máquinas que ofrecen servicios de red (servidor web y FTP) estén dentro del perímetro protegido y sobre la última máquina, que hace de puerta de enlace (*gateway*), se configure el *firewall* que protege el perímetro (red interna). Para ello, este proyecto se divide en dos actividades. En la primera, se proporciona al alumno un manual de *Netfilter*, que consiste en un módulo del núcleo de Linux que permite el filtrado de paquetes, la traducción de direcciones y puertos y otras manipulaciones del datagrama IP (*packet mangling*). El propósito general de esta primera actividad es introducir todos los aspectos necesarios para realizar la configuración de un cortafuegos para el sistema operativo Linux. En la segunda, se persigue el objetivo especificado anteriormente, es decir, la configuración de un *firewall* en la máquina virtual 0, que es la que separa la zona protegida de la zona de riesgo.

La configuración de este *firewall* abarca diferentes tareas que se resumen a continuación:

1. Configurar la máquina virtual 0 como *gateway* (activar el reenvío de paquetes).
2. Permitir a los dispositivos de la red interna (zona protegida) el acceso a la zona de riesgo (compartir la conexión a Internet).
3. Establecer la política por defecto (se optará por una política prohibitiva).
4. Habilitar los servicios que pueden usar los dispositivos de la zona protegida (resolución de nombres, acceso web, etc.).
5. Denegar el acceso a determinados servicios y contenidos.
6. Permitir el acceso a los servicios de la zona protegida desde la zona de riesgo.
7. Registrar los sucesos que van teniendo lugar en el *gateway* (necesario para asegurar la trazabilidad).
8. Hacer persistente la configuración del *firewall*.

Al ser el nivel de esta actividad elevado se le ha asignado un peso del 30 % tal y como se muestra en la Tabla III.

En la segunda semana también se realiza otro proyecto cuya finalidad es configurar sobre la máquina virtual 0 una red privada virtual basada en TINC [8]. TINC es una solución *Open Source* basada en SSL que permite unir mediante túneles seguros un conjunto de nodos remotos, es decir, distribuidos por la red. Una vez configurada la VPN se plantea a los alumnos el escaneo de la red privada virtual con el objetivo de buscar los dispositivos conectados en la misma. Dado que los alumnos se pueden conectar a la VPN de manera intermitente, se ha configurado un nodo que se mantendrá conectado permanentemente. Una vez localizado este dispositivo, los alumnos deben afinar el escaneo y proporcionar información detallada sobre él y en especial sobre los servicios de red que tiene activos. La dificultad de este proyecto se ha considerado media por lo que de acuerdo a la Tabla III se le ha asignado un peso de la nota final del 10 %.

Continuando con la tercera semana, los contenidos tratados versan sobre el proceso de gestión de riesgos. Se han desarrollado tres módulos donde se introduce este proceso y cómo realizar el análisis y posterior tratamiento de los riesgos de un sistema de información empleando MAGERIT [9]. MAGERIT es una metodología de análisis y gestión de riesgos promovida por el Gobierno Español y enfocada a las Administraciones Públicas. Como en semanas anteriores tras visualizar todos

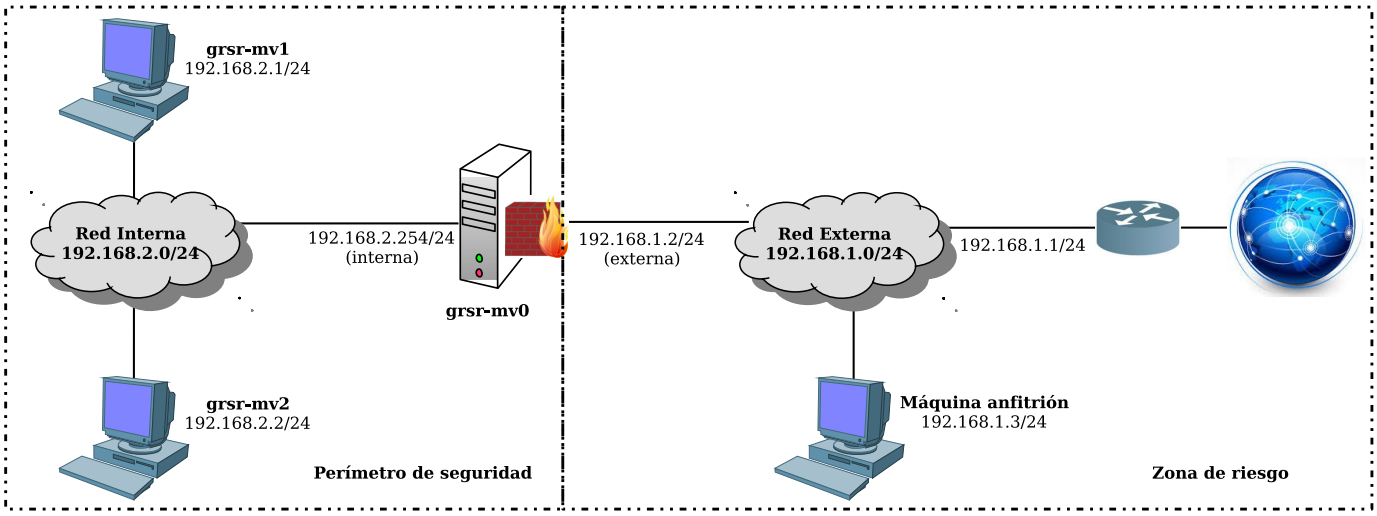

Figura 3. Topología de red para el cuarto proyecto realizado.

los vídeos y completar la autoevaluación los alumnos pueden proceder a realizar los proyectos.

Como se observa en la Tabla III para esta semana sólo está programado un proyecto. Esto se debe a que el análisis y tratamiento de riesgos no es un proceso complejo pero sí muy laborioso, donde hay que desarrollar diferentes tareas en diferentes etapas, lo cual requiere mucho tiempo. Para este proyecto se plantea un caso práctico donde se especifica un sistema de información que presenta algunos riesgos y los alumnos deben estimar el estado del riesgo y a continuación proceder a su tratamiento. Tras la toma de decisiones deben repetir el análisis y comprobar que las medidas tomadas contra las amenazas detectadas tienen el efecto esperado. Al ser un proyecto con un nivel alto se le ha asignado un peso del 20 %.

Finalmente, como se ha comentado previamente, la cuarta semana está dedicada a la evaluación. Este aspecto será tratado con detalle en el siguiente apartado.

II-B. Evaluación de los proyectos

En relación con la evaluación es preciso aclarar en primer lugar que se realiza completamente a distancia, es decir, no se requiere que los alumnos asistan presencialmente a ninguna prueba. Sin embargo, esto no quiere decir que no se exija la defensa de alguno de los proyectos a través de otras vías: videoconferencia, salas de conversación de *MS Teams*, etc., en caso de que los profesores lo estimen oportuno.

Tanto la realización de las autoevaluaciones como la entrega de la documentación requerida para la evaluación de cada proyecto se efectúa empleando la plataforma de Enseñanza Virtual (*Blackboard*). Para comprobar la identidad del estudiante en estos procesos se ha utilizado el sistema SMOWL [10]. SMOWL es un sistema continuo de autenticación de la identidad del estudiante online, que utiliza un algoritmo de reconocimiento facial automático para verificar la identidad del usuario y detectar comportamientos incorrectos a través de todo el proceso de aprendizaje.

Desde el comienzo de la primera semana todos los proyectos están disponibles para su realización. Además, se proporciona un calendario a los alumnos con una planificación por semanas. En esta planificación se incluyen las fechas de entrega recomendadas, en función del tiempo que los profesores estiman que deben dedicar a cada proyecto. No obstante, no es obligatorio entregar las actividades en la fecha recomendada sino que pueden hacerlo en cualquier momento durante el transcurso de las cuatro semanas de duración de la asignatura.

Una vez entregada la actividad se procede a su evaluación desde el centro de calificaciones proporcionado por *Blackboard* y se emite una calificación, que consiste en una nota numérica de 0 a 10 puntos. Además, se proporcionan un conjunto de comentarios sobre los errores o deficiencias detectadas. A partir de estos comentarios los alumnos pueden mejorar la resolución de su proyecto y volver a entregar de nuevo la actividad. La calificación obtenida en este segundo intento será la definitiva para el proyecto en cuestión. Para este proceso de mejora es importante que los alumnos dispongan de un tiempo adicional, de ahí que en la cuarta semana no se proponga ningún proyecto y se destine completamente a la evaluación.

Finalmente, una vez entregados y evaluados todos los proyectos la nota final se calcula aplicando los pesos indicados en la Tabla III a la calificación obtenida en cada actividad.

III. Resultados obtenidos y problemas encontrados

Según la información ofrecida por la Universidad de Sevilla [11], los datos de demanda del MII a distancia son muy alentadores, puesto que ésta ha aumentado significativamente (ver Tabla IV). Como se observa en esta tabla en el curso 2018-2019 hubo una demanda total de 69 (47 de primera preferencia y 22 de segunda y tercera) y de 87 en el curso 2019-2020 (64 de primera preferencia y 23 de segunda y tercera), ocupándose todas las plazas ofertadas (30 plazas). Si se comparan estos resultados con los del máster presencial, donde no se llegaron

a cubrir todas las plazas ofertadas en ninguno de los cursos en los que se impartió, se puede deducir que este incremento se debe a que:

1. La oferta del máster se ha extendido a un conjunto mucho mayor de estudiantes. Al eliminar la obligatoriedad de asistencia presencial cualquier alumno, sin importar su lugar de residencia actual, puede cursar el máster.
2. Esta modalidad a distancia permite que muchos estudiantes puedan compaginar en mayor medida sus trabajos y vidas personales con los estudios del máster.

En relación con los resultados académicos, en la Tabla V se observa cómo la tasa de aprobados es muy elevada en los cursos impartidos con la modalidad presencial, donde el peor resultado se encuentra en el curso 2015-2016 (80 %). Este resultado se debió a la enfermedad de uno de los alumnos que motivó que no pudiera asistir a clase y completar los proyectos. En el resto de los cursos de la modalidad presencial los resultados superaron siempre el 90 %. Esto se debe al hecho de que los alumnos, además de tener una alta motivación, aprovecharon todas las ventajas que ofrece cursar las asignaturas de forma presencial: tras la explicación del profesor los proyectos se abordan en el horario de clase, los alumnos cuentan con el apoyo inmediato del profesor ante las dudas que surgen durante la realización de los proyectos, se utilizan los recursos e infraestructuras disponibles en el centro donde se imparte la titulación, etc. En relación con los resultados obtenidos en el curso 2018-2019 (modalidad a distancia) se observa cómo la tasa de aprobados se ha situado en el 63,3 %. Este resultado es coherente ya que está demostrado que la tasa de abandono en estudios a distancia es aún más elevada que en los formatos presenciales [12]. Efectivamente, los 11 alumnos no aprobados ni siquiera accedieron a los contenidos, e incluso 4 de ellos abandonaron al comenzar el máster.

García-Aretio [12] realiza un análisis exhaustivo de las principales causas de abandono en estudios a distancias. De todas las señaladas, en el caso de este máster, se considera que las dos que han tenido más influencia son:

1. La falta de tiempo para dedicar a los estudios.
2. La falta de diálogo del estudiante con la institución, los docentes y el resto de compañeros.

La falta de tiempo puede estar ligada a razones laborales, al tratar de compaginar el estudio con un determinado trabajo que puede restar horas, por lo que las obligaciones laborales de los estudiantes a distancia exigen a éstos una adecuada gestión del tiempo. Pero también es cierto que esa percepción de falta de tiempo pudiera deberse realmente a una organización

Tabla IV
OFERTA Y DEMANDA DE PLAZAS DEL MII EN SU MODALIDAD A DISTANCIA.

		Demanda	
Curso	**Oferta**	**1ª Preferencia**	**2ª y 3ª Preferencia**
2018-2019	30	47	22
2019-2020	30	64	23

Tabla V
RESULTADOS ACADÉMICOS OBTENIDOS EN EL MII DESDE SU COMIENZO PARA LA ASIGNATURA DE SEGURIDAD EN REDES IMPARTIDA.

Curso	**Nº Alumnos**	**Nº Aprobados**	**Tasa (%)**
2014-2015	7	7	100
2015-2016	5	4	80
2016-2017	10	10	100
2017-2018	14	13	92,8
2018-2019	30	19	63,3

institucional y docente deficiente respecto a los programas y cursos o de la propia orientación al estudiante para ayudarle en esa gestión del tiempo. En este sentido, si se tiene en cuenta que el 100 % de los estudiantes que comenzaron el máster estaban trabajando un aspecto muy importante es medir adecuadamente la carga de trabajo y no exigir a los alumnos proyectos de tal magnitud que sean inabordables en el tiempo de duración de la asignatura, que en el caso de este trabajo, es de cuatro semanas. La percepción de los profesores que han impartido esta asignatura es que la carga de trabajo fue adecuada. Sin embargo, el problema encontrado fue que ésta se impartió en el último bloque de forma que los alumnos ya habían desistido antes de que diera comienzo.

También puede considerarse, ante esa falta de tiempo, el problema de la frustración del estudiante en línea, ante el cúmulo de dificultades, sobre todo si es nuevo en estos escenarios, y que puede llevar al abandono. De ahí que la segunda causa más influyente que se ha considerado es la falta de diálogo. Según apunta García-Aretio si ese diálogo no es de calidad, no es eficaz, sea por déficit del estudiante, o sea por rupturas con la institución (causas institucionales), con los docentes o con los recursos (causas académicas), o con los propios pares, la deserción podrá estar más cerca. En consecuencia, desde la institución y desde la actividad docente, han de implementarse medidas y acciones concretas para restablecer esos diálogos débiles o rotos y aumentar la retención, tales como: propiciar líneas para que los estudiantes aprendan a autorregular el estudio; potenciar los servicios tecnológicos de apoyo a la docencia y el aprendizaje; impulsar una docencia de calidad adaptada a los sistemas digitales de enseñanza y aprendizaje, con diseños rigurosos, gestión eficaz de la docencia en línea y activando diferentes formas y modelos de evaluación formativa.

Finalmente, también se ha observado otro problema relacionado con la evaluación. Mientras que en una docencia presencial el profesor puede realizar un seguimiento durante las clases y garantizar que los alumnos han realizado los proyectos y las evaluaciones, en el caso de la docencia a distancia no existen tantas garantías de que esto ocurra así. El uso de SMOWL garantiza que los alumnos han realizado las autoevaluaciones y las entregas de la documentación de los proyectos pero no que dicha documentación haya sido realizada por los mismos, es decir, que los alumnos hayan recibido ayuda. Para solventar este problema resulta conveniente combinar SMOWL con otro conjunto de acciones, entre

las que destaca la defensa de los proyectos ante el profesor empleando los medios digitales disponibles. Sólo de esta forma se podrá determinar con veracidad si el alumno ha realizado el trabajo propuesto y ha adquirido realmente los conocimientos que se exigen.

IV. Conclusiones

El Máster de Ingeniería Informática en su modalidad presencial presentaba buenos resultados de rendimiento y éxito pero sin embargo el problema radicaba en su baja demanda. Así, durante los cuatro cursos en los que se impartió esta modalidad la tasa de matriculación no superó el 50 %.

Este hecho motivó que la ETSII decidiera afrontar el reto de ofrecer esta titulación en una modalidad completamente a distancia. Esta nueva modalidad comenzó a impartirse en el curso 2018-2019 siendo los resultados obtenidos muy alentadores al superar la demanda las espectativas iniciales y cubrirse todas las plazas ofertadas.

Esto nos hace pensar que la decisión de la ETSII de ofrecer este máster a distancia ha conseguido su principal objetivo, es decir, facilitar a los alumnos la realización de estos estudios y poderlos compaginar tanto con su vida laboral como familiar. Esto se ha conseguido mediante la generación de material de estudio en formato audiovisual y el uso de plataformas digitales. No obstante, esta propuesta también presenta un conjunto de problemas. Por un lado, el uso de los laboratorios es casi imprescindible dada la naturaleza técnica de la asignatura que se presenta en este trabajo. Por otro lado, la evaluación también debe realizarse totalmente a distancia. Finalmente, la tasa de abandono en este tipo de educación a distancia se sitúa en niveles superiores a los encontrados en estudios presenciales. Los dos primeros problemas se han solventado mediante el despliegue de un laboratorio de redes virtual y la utilización de herramientas como SMOWL que permiten la monitorización e identificación continua de los estudiantes. En relación con el tercero es necesario potenciar el diálogo con los alumnos a diferentes niveles para intentar evitar su abandono.

Acknowledgment

Este trabajo ha sido parcialmente financiado por el Ministerio de Industria y Competitividad del Gobierno de España a través del proyecto TIN2017-89951-P (BootTimeIoT) y por el Fondo Europeo de Desarrollo Regional (FEDER).

Referencias

[1] J. Bará, J. Domingo, and M. Valero. (2011) Técnicas de Aprendizaje Cooperativo y Aprendizaje Basado en Proyectos. [Online]. Available: https://ice.unizar.es/sites/ice.unizar.es/files/users/leteo/materiales/ac_pbl.pdf

[2] Autoinforme Global de Acreditación de Títulos. [Online]. Available: http://webapps.us.es/fichape/Doc/AUTOSEG/IG/2017_M147_ autoglobal.pdf

[3] E. Vendrel, "Empleabilidad 2013. Segundo informe sobre la empleabilidad de los egresados en las diferentes titulaciones en Ingeniería e Ingeniería Técnica Informática," Conferencia de Directores y Decanos de Ingeniería Informática, Tech. Rep. 2, Jun. 2015.

[4] A. J. Acosta, A. Barriga, B. Perez, and J. L. Huertas, "Experiencia de puesta en marcha y desarrollo de un máster on-line en microelectrónica," in *Actas XII Congreso de Tecnologia, Aprendizaje y Enseñanza de la Electronica (TAEE 2016)*, Sevilla, España, Jun. 2016, pp. 97–103.

[5] Página web oficial de Blackboard. [Online]. Available: https://www.blackboard.com/es-es

[6] Página web oficial de Microsoft Teams. [Online]. Available: https://products.office.com/es-es/microsoft-teams/group-chat-software

[7] Página web oficial de VirtualBox. [Online]. Available: https://www.virtualbox.org/

[8] Página web oficial de TINC VPN. [Online]. Available: https://www.tinc-vpn.org/

[9] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[10] Página web oficial de SMOWL. [Online]. Available: https://smowl.net/es/

[11] Página web oficial del Máster Universitario en Ingeniería Informática. [Online]. Available: https://www.us.es/estudiar/que-estudiar/oferta-de-masteres/master-universitario-en-ingenieria-informatica

[12] L. Garcia, "El problema del abandono en estudios a distancia. Respuestas desde el Diálogo Didáctico Mediado," *RIED. Revista Iberoamericana de Educación a Distancia*, vol. 22, no. 1, pp. 245–270, 2019. [Online]. Available: http://revistas.uned.es/index.php/ried/article/view/22433