MOOC sobre Hacking ético de MONDRAGON UNIBERTSITATEA - #moocHackingMU

Miguel Fernández, Iñaki Arenaza, Iñaki Garitano, Jesús Lizarraga, Mikel Iturbe
Departamento de Electrónica e Informática, Escuela Politécnica Superior - MONDRAGON UNIBERTSITATEA
Goiru Kalea, 2. 20500 Arrasate - Mondragón
mfernandez, iarenaza, igaritano, jlizarraga, miturbe @mondragon.edu

Abstract- **En este artículo se presenta el Curso Online Abierto y Masivo sobre Hacking Ético que MONDRAGON UNIBERTSITATEA ha organizado en este curso 2015/16. Ha sido la primera experiencia con este tipo de cursos en nuestra universidad y ha supuesto un notable éxito de participación, con casi 6000 inscritos. Hemos elegido la temática del hacking ético (conocer las técnicas que usan los hackers para atacar los sistemas y las redes corporativas y usar este conocimiento para mejorar nuestras medidas de protección) para enseñar a los participantes conceptos fundamentales de la seguridad informática. En este curso hemos optado por un enfoque conectivista, basado en la interacción entre los participantes y en el aprendizaje colaborativo, y por incluir técnicas de gamificación y de storytelling en el desarrollo del mismo, con el desarrollo de un reto por equipos basado en los juegos del tipo "Capture the Flag".**

***Index Terms*- jornadas, ciberseguridad, formación, innovación, MOOC, hacking ético.**

Tipo de contribución: *Formación innovación*.

I. Introducción

Desde hace un tiempo en MONDRAGON UNIBERTSITATEA estábamos expectantes con (y preocupados por) los Cursos Abiertos Online y Masivos (MOOC [1] por sus siglas en inglés: "Massive Open Online Courses"). Nos planteábamos cómo podemos aprovechar este tipo de formación no reglada o informal en nuestra universidad, y cómo están impactando plataformas como Coursera (https://es.coursera.org), edX (https://www.edx.org) o Miríada X (https://miriadax.net) en la educación superior, en lo que también se conoce como "educación disruptiva" [2]. Así que en este curso 2015/16 se decidió lanzar una plataforma propia de MOOCs (https://mooc.mondragon.edu) para conocer de primera mano este entorno. Como resultado, el primer MOOC que se ha ofertado desde MONDRAGON UNIBERTSITATEA ha sido la primera edición del MOOC sobre hacking ético.

Pensamos que este curso es innovador desde dos puntos de vista que están relacionados: por un lado, el enfoque conectivista basado en la interacción entre los participantes del curso y en el aprendizaje colaborativo y, por otro lado, la incorporación de la gamificación en el proceso de aprendizaje, que ha supuesto el desarrollo de un reto en el que hemos conseguido implicar a más de 600 personas agrupadas en 80 equipos, atacándose mutuamente durante una semana en la parte final del curso, utilizando una mecánica de juego basada en el concepto "capture the flag" o "atrapa la bandera".

El MOOC sobre Hacking Ético de MONDRAGON UNIBERTSITATEA es un curso abierto, masivo y online que introduce a los participantes en el mundo de la seguridad informática.

En este curso usamos la perspectiva del hacking ético: conocer las técnicas que usan los hackers para atacar los sistemas y las redes corporativas y usar este conocimiento para mejorar nuestras medidas de protección. Hemos elegido esta perspectiva porque pensábamos que podía ser más atractiva para las personas interesadas en formarse en temáticas relacionadas con la seguridad informática.

Ya existen algunas iniciativas de este tipo relacionadas con la seguridad informática como, por ejemplo, los cursos que ofrece CriptoRed desde su Aula Virtual de Criptografía y Seguridad de la Información Crypt4you (http://www.criptored.upm.es/crypt4you/portada.html). Sin embargo, no hemos encontrado ningún MOOC dedicado de manera específica al hacking ético. Sí que existen cursos online sobre esta temática, pero no con la filosofía de un MOOC.

II. Trabajos relacionados

Desde su creación y proliferación a principios de la década de 2010, los MOOC han sido de objeto de estudio por la comunidad científica, especialmente la relacionada con las ciencias de la educación y más aún desde que 2012 fuese considerado el "año del MOOC" [1].

Son varios los estudios que analizan el fenómeno de los MOOC. Liyanagunawardena y otros [3] y Chiappe-Laverde y otros [4] analizan la literatura relativa a este tipo de cursos.

Algunos trabajos se centran en el punto de vista del grado de terminación de estos cursos. En este sentido es especialmente relevante el trabajo de Jordan [5], que analiza el grado de atrición de los cursos y cifra la tasa media de terminación en un 6,5%.

Otros trabajos se han centrado en el tema de la accesibilidad a la educación que proporcionan los MOOC. Emanuel [6] argumenta que los MOOC, aunque online y masivos, no facilitan el acceso a la educación, ya que la gran mayoría de los participantes ya cuenta con estudios superiores.

Respecto a los casos de estudio, la experiencia más relevante y conocida es el primer MOOC a gran escala ofrecido por parte de una institución superior: el curso de la universidad de Stanford sobre inteligencia artificial [7]. En el caso de MOOCs de habla hispana, el primer MOOC reconocido como tal es Crypt4you [8] también de temática relacionada con la seguridad informática. A nivel latinoamericano, Gómez Porras y otros [9] analizan el impacto del primer MOOC del subcontinente.

III. Objetivos del curso

El primer objetivo que nos planteamos a la hora de lanzar este MOOC era aprender sobre este tipo de cursos. Este MOOC ha sido la primera iniciativa de este tipo que se ha abordado desde MONDRAGON UNIBERTSITATEA. Durante el curso 2014/15 el rectorado de la Universidad decidió apostar por este tipo de cursos y esta apuesta se tradujo en el lanzamiento de 3 cursos en el curso 2015/16: el curso sobre "Hacking ético" sobre el que trata este artículo y dos cursos más relacionados con el cooperativismo.[1]

También pretendíamos ganar visibilidad como una universidad especializada en la formación en el ámbito de la seguridad informática. Tenemos la percepción de que nuestra universidad sí está bien posicionada en nuestro entorno como grupo de investigación en los temas relativos a la seguridad, pero no tanto en el ámbito de la formación.

Por último, nos planteamos el MOOC como una herramienta para captar alumnos para los cursos de formación reglada de la universidad relacionados con la seguridad. Debido a este motivo, programamos el Máster en Seguridad Informática y el Curso Experto en Seguridad Informática a continuación del MOOC, con el objetivo de que los alumnos del MOOC pudieran continuar con su formación. Este es el objetivo más relacionado con la rentabilidad económica del MOOC.

IV. Estructura del curso

El curso está dividido en 4 unidades, cada una con una semana de duración. En cada unidad, los participantes disponen de un vídeo de presentación, una serie de contenidos y tareas propuestas. El curso se ha planteado con un carácter conectivista [10], dando una importancia crítica a la interacción entre los participantes. Es decir, es un MOOC en el que prima el aprendizaje colaborativo. Los contenidos son importantes, pero damos mayor importantica a que el curso proporcione herramientas de interacción entre los participantes y fomente el aprendizaje colaborativo. Por tanto, uno de los objetivos del curso es que los participantes se apoyen entre ellos en el proceso de aprendizaje. Para ello, nos hemos apoyado en las redes sociales, fundamentalmente Facebook y Twitter, además de en el foro disponible en la plataforma del curso. Sin ninguna duda, Facebook ha sido la plataforma en la que los participantes más han interactuado.

En la segunda parte del curso, los participantes se han enfrentado entre si, agrupados en equipos, en un reto que les hemos propuesto. Con este reto pretendíamos introducir la gamificación en el proceso de aprendizaje y fomentar la colaboración entre los participantes. El reto ha tenido una gran aceptación entre los participantes y pensamos que es uno de los diferenciales principales de este curso.

Relacionado con el tema de la gamificación, hemos optado por dar una línea argumental al curso basada en "Star Wars", para poder lograr un tono más informal que en los cursos tradicionales. De hecho, los alumnos que han logrado completar el curso han recibido, en función de sus logros individuales y grupales, las insignias "Padawan", "Jedi" y "Sith". El diseño gráfico de los elementos del curso también han seguido esta línea.

V. Desarrollo del curso

La concepción inicial del curso se realizó en el segundo semestre del curso 2014/15, partiendo de una idea de Urko Zurutuza (profesor del área de Telemática y coordinador de la línea de investigación sobre seguridad informática) y la preparación del curso (planificación, adaptación de contenidos, puesta en marcha de la plataforma, etc.) comenzó en mayo de 2015.

Para crear parte de los contenidos del MOOC hemos adaptado contenidos del curso experto en seguridad informática del que ya hemos ofrecido varias ediciones. Inicialmente, realizamos un análisis del syllabus del curso experto para la elaboración de la propuesta de contenidos para el MOOC, y adaptamos contenidos y actividades ya existentes, sobre todo para las dos primeras unidades del MOOC, que son las más tradicionales (basadas en contenidos y tareas individuales)

La primera edición ha tenido lugar en este curso 2015/16. Comenzó el 22 de septiembre de 2015 y tuvo una duración de 4 semanas. El curso terminó concretamente el 27 de octubre con un hangout en directo en el que se anunciaron los equipos ganadores en la fase del reto. El curso es gratuito y está dirigido a cualquier persona de habla hispana interesada en la seguridad informática, ya sea para conocer en más profundidad este tema o bien para iniciar un proceso de reorientación profesional. Está recomendado especialmente a titulados universitarios en Informática o Telecomunicaciones, si bien está abierto a la participación de cualquiera que tenga un conocimiento básico sobre Redes, ya sea adquirido de manera formal como informalmente.

Aunque esperábamos un gran número de participantes, hemos tenido un éxito de convocatoria que nos ha sorprendido, con 5868 inscritos, muchos de ellos procedentes de Latinoamérica. Un 47% de los inscritos son latinoamericanos, un 46% procede de España y el resto vienen de Estados Unidos y países del resto de Europa.

Como hemos comentado, las dos primeras unidades del MOOC son más tradicionales: se ofrecen contenidos y actividades desde la plataforma. Cada unidad sigue la misma estructura: un vídeo de presentación, objetivos de la unidad y contenidos, tareas, indicaciones y otros recursos. En la Fig. 1se puede observar la plataforma sobre la que se sirve el curso.

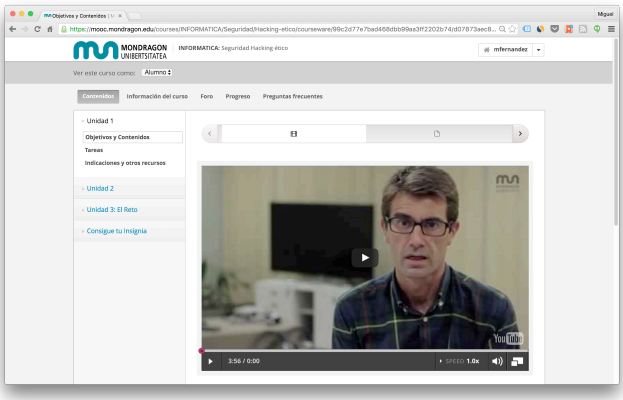

Fig. 1: Plataforma del curso sobre Open edX.

[1] MONDRAGON UNIBERTSITATEA es una universidad constituida como cooperativa de trabajo, que pertenece a MONDRAGON (http://www.mondragon-corporation.com), un grupo empresarial que engloba a 260 cooperativas y empresas.

Los objetivos de aprendizaje específicos que nos planteamos para estas dos primeras unidades son:

- Conocer el concepto de cibercrimen y poner en contexto los delitos informáticos.
- Conocer el proceso habitual que sigue un hacker para realizar un ataque.
- Comprender y ejecutar algunas técnicas básicas de hacking.
- Aprender a obtener información a partir de capturas de tráfico de Internet, utilizando sniffers o analizadores de protocolos.
- Conocer algunos ejemplos de ataques que se apoyan en debilidades de programación de las aplicaciones.
- Debatir sobre la ética del Hacker.

Al término de la segunda unidad, planteamos a los participantes un enigma criptográfico sencillo, relacionado con una tarea que ya habían realizado. Al resolverlo, concedíamos acceso a un grupo secreto en Facebook, donde los participantes accedían a información sobre el reto con unos días de antelación respecto al resto de participantes.

Uno de lo elementos diferenciales de este MOOC es el uso del concepto de gamificación. Como hemos comentado, en la segunda mitad del curso (durante dos semanas) se propuso un reto a los participantes, que permitiera al alumnado poner en práctica lo aprendido y trabajar en equipo. Dadas las características del curso y de los participantes se decidió avanzar en la gamificación incorporando una narrativa que sirviera de elemento motivador y de hilo conductor del reto, adoptando el concepto de "storytelling" como recurso educativo. Para ello se optó por usar los personajes y el argumento de la saga de Star Wars, desarrollándose no sólo una narrativa ex profeso para darle sentido al reto del curso, sino que también se diseñaron elementos gráficos (empezando por los badges o insignias del curso) para dar mayor credibilidad a la historia. El diseño de las insignias se puede ver en la Fig. 2.

Asimismo se jugó con los espacios sociales, cambiando la interfaz de la cuenta de Twitter durante el Reto y añadiendo un nuevo grupo en Facebook (Consejo Jedi), que tenía una finalidad específica en el desarrollo del reto. Más adelante comentaremos la presencia del MOOC en redes sociales.

En el reto, los participantes se agrupaban en equipos de 8 personas. A cada grupo se le asignaba un servidor público en Internet, con una configuración idéntica para todos los grupos. Durante la primera semana del reto, los equipos se dedicaban a securizar sus servidores. Después, hicimos públicas las direcciones IP de todos los servidores, y los equipos se dedicaban durante otra semana a atacar los servidores del resto de equipos, con el objetivo de conseguir 3 archivos de cada servidor.

Fig. 2: Insignias del MOOC.

Tabla 1

VULNERABILIDADES PRESENTES EN LOS SERVIDORES PUESTOS A DISPOSICIÓN DE LOS EQUIPOS.

Vulnerabilidad	Grado de dificultad
Servidor FTP anónimo habilitado por defecto. Uno de los archivos a conseguir está en la zona de acceso público (/srv/ftp)	Bajo
Los servidores tienen instalado el software gitlist (http://gitlist.org/), en concreto la versión 0.4.0, que tiene (entre otras) la vulnerabilidad CVE-2014-4511. Si se consultan los detalles de dicho CVE se pueden obtener las URLs de al menos dos exploits	Medio
Se instala una versión antigua vulnerable del paquete Debian de Cacti, que tiene (entre otras) las vulnerabilidades CVE-2015-4634, CVE-2015-4454, CVE-2015-4342 y CVE-2015-0916 que permiten hacer ataques de SQL Injection de diferentes formas.	Alto

Para conseguir cada archivo, los equipos debían explotar determinadas vulnerabilidades presentes en los servidores. En la Tabla 1 hemos listado una breve descripción de estas vulnerabilidades.

Para la evaluación del reto, hemos tenido en cuenta los archivos conseguidos por cada grupo. Al finalizar el MOOC, hemos premiado a los participantes con 3 insignias, en función de sus logros: la insignia Padawan (individual), la insignia Jedi (grupal, que permia a los equipos que mejor han defendido sus servidores) y la insignia Sith (grupal, que premia a los equipos han demostrado mayor destreza en el ataque al resto de servidores).

Para la evaluación individual de los alumnos y la obtención de las insignias Padawan, les solicitamos desde el comienzo del curso que mantuvieran un blog personal como diario del curso, en el que mostraran evidencias de su trabajo. Mediante estos blogs de los participantes, ellos mismos han realizado una evaluación entre pares [11] a través de un procedimiento disponible en la plataforma del curso. Aunque nosotros no hemos podido leer todos los blogs de los alumnos, sí que hemos detectado algunos muy interesantes que pueden servir de apoyo en las próximas ediciones. Incluso, pensamos que es interesante contar con algunos de los alumnos de esta edición como prescriptores y colaboradores de próximas ediciones.

La evaluación entre pares tiene como finalidad evaluar las evidencias del trabajo que se ha realizado, y no la capacidad o habilidades de quienes realizaron dicho trabajo. Los participantes han tenido que evaluar dos tipos de atributos, unos para valorar la presentación de las distintas tareas propuestas durante el curso, y otros sobre las evidencias de aprendizaje, en función de si la tarea presentada incluye o no evidencias.

El número de insignias emitidas se puede observar en la Tabla 2.

Tabla 2

NÚMERO Y TIPO DE INSIGNIAS EMITIDAS

Insignia	Número de insignias emitidas
Padawan	59
Jedi	36
Sith	24

Estas insignias son compatibles con las insignias o *badges* del proyecto de Mozilla "Open Badges" (http://openbadges.org), que tiene como uno de sus objetivos la acreditación del aprendizaje no formal en el currículum de los alumnos. Así, los alumnos del MOOC que hayan obtenido insignias las pueden incluir en su mochila digital. Pensamos que es importante que en este tipo de cursos los alumnos pueden disponer de una certificación de este tipo, además de un certificado emitido por la universidad.

La plataforma elegida para el MOOC ha sido Open edX. Esta elección ya venía impuesta por el rectorado, debido a que se quería mantener un control estricto sobre la plataforma. También se valoró la posibilidad de integrar el MOOC en plataformas públicas ya existentes, pero finalmente se desestimó esta opción.

Aunque la plataforma ha funcionado bien, uno de los aspectos mejorables es el foro que proporciona, que con el alto número de participantes se ha convertido en una herramienta ingobernable. Nuestra recomendación durante el curso ha sido orientar a los participantes hacia los espacios sociales para interactuar (Facebook y Twitter, fundamentalmente), pero tenemos que tener en cuenta que hay personas reacias a usar este tipo de herramientas y así lo han manifestado.

Open edX también nos ha permitido lanzar una newsletter semanal con la que conseguíamos informar de las novedades a los participantes den el curso.

VI. Presencia en Redes Sociales

Como hemos comentado, el enfoque conectivista del curso ha hecho que nos hayamos apoyado en las redes sociales para que los participantes pudieran interactuar y aprender de manera colaborativa. Este ha sido un punto muy importante durante el desarrollo del curso, al que hemos dedicado una atención especial.

Fig. 3: Página en Facebook del MOOC.

Los meses anteriores a la celebración del curso (desde julio de 2015) hemos utilizado una página de seguidores de Facebook (https://www.facebook.com/moochackingetico), que se muestra en la Fig. 3 y un perfil en Twitter (https://twitter.com/moocHackingMU) (Fig. 4) para promocionar el curso.

Fig. 4: Perfil en Twitter del MOOC.

Estos perfiles estaban activos unos meses antes del comienzo del MOOC, publicando contenido interesante relacionado con la seguridad informática, y su objetivo era ganar visibilidad para conseguir participantes. Además, creamos el hashtag en Twitter "#MoocHackingMU" para que se utilizara en las conversaciones sobre el curso. Este hashtag ha tenido una gran repercusión durante el curso y ha sido muy usado por los participantes activos en Twitter.

El perfil en Twitter, durante el reto, se convirtió en una herramienta a la que podían acudir los equipos en busca de ayuda, a través de mensajes privados. Cada vez que usaban esta posibilidad, eran penalizados en la puntuación final del reto.

Pero donde realmente los participantes han interactuado ha sido en los grupos que hemos creado en Facebook. El grupo principal es la "Comunidad de #moocHackingMU" (https://www.facebook.com/groups/moochackingmu), un grupo público que cuenta con 1019 miembros y que mantiene actividad de los participantes que publican información sobre seguridad, hacking, etc. Este grupo (Fig. 5) ha sido el principal espacio de interacción.

Además, como apoyo para el reto, creamos un grupo cerrado en Facebook llamado "Consejo Jedi" (Fig. 6) (https://www.facebook.com/groups/consejojedimu) al que los participantes solo podían accede tras resolver un enigma. En este grupo, los miembros obtenían información privilegiada relativa al reto unos días antes que el resto de participantes. Ambos grupos siguen manteniendo actividad actualmente.

Fig. 5: grupo en Facebook "Comunidad #moocHackingMU".

Fig. 6: Grupo cerrado en Facebook "Consejo Jedi".

Para el desarrollo del curso también hemos contado con un blog (http://mukom.mondragon.edu/mooc-hacking-etico), que se muestra en la Fig. 7, integrado en la plataforma de blogs de la universidad. Este blog ha sido un complemento para anunciar eventos importantes del curso.

Fig. 7: el blog del curso.

En el canal de YouTube de MONDRAGON UNIBERTSITATEA están disponibles los vídeos del MOOC: un vídeo de presentación del curso y los vídeos con los que introducíamos las unidades. Además, el curso se cerró con un hangout en el que comunicamos los equipos que se habían hecho acreedores de las insignias Jedi y Sith, así cómo el equipo ganador del reto.

En la Tabla 3 se muestran los datos de reproducciones y porcentaje medio reproducido de cada vídeo.

Tabla 3:

REPRODUCCIONES Y PORCENTAJE MEDIO REPRODUCIDO EN YOUTUBE

Vídeo	Reproducciones	Porcentaje medio reproducido
Presentación del curso	1234	51%
Unidad 1	3419	71%
Unidad 2	1133	76%
El reto	1187	68%
Final del curso	326	68%
Anuncio de los ganadores del reto	388	40%

VII. LECCIONES APRENDIDAS

En este MOOC hemos participado profesores del área de telemática y seguridad de la Escuela Politécnica de MONDRAGON UNIBERTSITATEA , además de personal de sistemas y de administración. Ha sido una experiencia muy enriquecedora y gratificante, y también muy intensa. En consonancia con los objetivos previamente definidos para este curso, durante este MOOC hemos aprendido mucho sobre este tipo de cursos, hemos logrado conectar con una comunidad de personas muy interesadas en el mundo de la seguridad informática (de hecho, algunos de los participantes en el curso se han matriculado en el Máster online en Seguridad de la universidad) y hemos colaborado en dar visibilidad a MONDRAGON UNIBERTSITATEA en el ámbito de la seguridad.

En un primer momento, el éxito de audiencia del MOOC nos generó cierta preocupación, pero hemos aprendido que los participantes en este tipo de cursos tienen, en su mayoría,

experiencia en otros MOOCs y conocen qué pueden esperar de los profesores, en el sentido de que no es curso online al uso en el que los profesores podemos dedicar tiempo a cada alumnos para tutorías, resolver dudas, intervenir en el foro, etc.

Este tipo de cursos requiere una alta implicación del equipo docente, tanto en la preparación y adecuación de contenidos como en la dinamización del curso. Aunque este MOOC emplea un enfoque conectivista y fomenta el aprendizaje colaborativo, la tarea de los profesores en el día a día se basa en ofrecer contenidos interesantes y complementarios a través de los canales habilitados para ello y en resolver cuestiones relacionadas con la gestión del curso. En nuestro caso y hablando de recursos, hemos dedicado una persona a dedicación completa durante el desarrollo del curso, aunque este rol estaba soportado por los 4 profesores del equipo docente.

Por último, con un número alto de participantes inscritos como el de este curso, es muy importante automatizar todas las tareas que sean posibles. En nuestro caso, las tareas de asignación de servidores y la evaluación del reto a través de los archivos capturados por los distintos grupos, por ejemplo, nos han supuesto una carga de trabajo que no teníamos contemplada.

VIII. Conclusiones y líneas futuras

En primer lugar, pensamos que el grado de consecución de los objetivos que nos planteábamos con el MOOC ha sido alto. Como ya hemos comentado en el apartado sobre las "lecciones aprendidas", hemos conseguido un conocimiento alto sobre los MOOC: su planteamiento, organización, dinamización, evaluación, etc. Además, hemos conseguido vencer ciertas reticencias internas que existían sobre este tipo de cursos.

Hemos conseguido ganar visibilidad como entidad formadora en el ámbito de la seguridad informática. En este sentido, la presencia del MOOC en los medios ha sido importante: entrevistas en radio y televisión en EITB (la radio-televisión pública vasca), prensa escrita y digital. Nos hemos aprovechado tanto del concepto MOOC como un concepto todavía novedoso para los medios, como de la temática del curso, el hacking ético, que resulta atractiva también para los medios.

En cuanto a posicionamiento online, hemos conseguido a través del MOOC estar posicionados, por ejemplo, en Google España en el primer lugar de los resultados de búsqueda para la búsqueda "curso hacking ético" (Fig. 8), en segundo lugar para el término más genérico "hacking ético" y en tercer lugar para el término "mooc seguridad informática", lo que nos permite decir que la plataforma elegida desde la universidad (edX) es una buena herramienta para ganar visibilidad frente a los buscadores, combinado con un trabajo de consecución de enlaces entrantes.

La presencia en YouTube a través de los vídeos del curso también nos ha permitido estar bien posicionados para los términos descritos tanto para búsquedas en YouTube como para búsquedas en Google.

El último de los objetivos que nos planteábamos implicaba conseguir alumnos para los cursos de formación reglada de la universidad. En este sentido, ocho de los participantes en el MOOC se han matriculado en la presente edición del Máster Online en Seguridad Informática han participado en el MOOC.

Todos estos datos han sido valorados de manera muy positiva desde el rectorado de la universidad, que ha confirmado la continuidad de este curso y la apuesta por los MOOC.

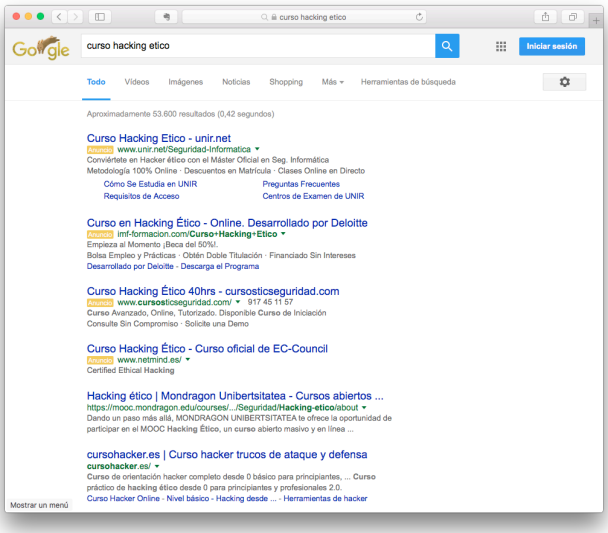

Fig. 8. Posicionamiento en google.es para el término "curso hacking ético".

En cuanto a la participación en el curso, además del número de participantes que han conseguido insignias, alrededor de unas 640 personas (un 11% de las personas inicialmente matriculadas) se mantenían activas en la fase final del curso, el reto, con 80 equipos atacándose mutuamente. Estamos satisfechos con estos datos (que superan los datos globales de participación encontrados en la literatura sobe MOOCs [5][12]), aunque nuestra intención es mejorarlo en próximas ediciones.

Otra conclusión que hemos extraído del curso es que este curso ha sido posible gracias a la colaboración de una empresa externa a la universidad y con mucha experiencia en MOOCs. En nuestro caso, la empresa elegida para guiarnos en este proceso nuevo para nosotros fue Conecta13 (http://conecta13.com), y la elección ha sido un completo acierto. David Álvarez y su equipo nos han transmitido su conocimiento y nos ayudado en la concepción, preparación y dinamización del curso. Por tanto, vemos que es clave para las universidades que quieran experimentar con los MOOC que consigan un buen aliado, ya que es un concepto de formación muy distinto a los entornos de formación reglada a los que estamos acostumbrados.

Es muy importante que el equipo de personas que se vayan a ocupar de la impartición del MOOC reciban formación específica sobre lo qué supone gestionar y dinamizar este tipo de cursos, ya que, sobre todo con el enfoque conectivista que se ha aplicado en el MOOC sobre hacking ético, las diferencias con los cursos online tradicionales son grandes. Como ya hemos comentado, hay que trabajar en la dinamización del curso tanto o más que en la gestión de contenidos tradicional.

Hemos conseguido crear una comunidad de personas a las que les interesa el mundo de la seguridad informática y del hacking ético, y que siguen interactuando en las comunidades

virtuales del MOOC, aún después de la finalización del curso [13]. Aunque éste no era un fin en si mismo del MOOC, creemos que las personas que han vivido una buena experiencia en el desarrollo de un curso de este tipo, establecen una ligazón con la comunidad que les ha acompañado en el proceso y con la universidad responsable del mismo, y esto puede ser aprovechable en el futuro por la universidad, si mantenemos esta comunidad viva.

Hemos visto que este MOOC ha funcionado muy bien para detectar a participantes con gran talento en el mundo de la seguridad informática. Sin haberlo pretendido inicialmente, hemos visto que un MOOC de este tipo, en el que se juega con conceptos como la gamificación y los desafíos, pueden servir para la captación de talento, y puede ser una muy buena opción de cara a las empresas, a la hora de encontrar determinados perfiles profesionales interesantes. Es una vía que estamos explorando desde la universidad con algunas asociaciones empresariales.

Por último, creemos que puede ser interesante encontrar empresas patrocinadoras que aporten más relevancia y visibilidad al curso y que nos ayuden a mantener un curso de este tipo en constante contacto con al realidad tecnológica y empresarial en un mundo tan cambiante como el de la seguridad informática.

AGRADECIMIENTOS

Además de las personas mencionadas en el artículo, este curso no hubiera sido posible sin el apoyo y la colaboración de Edurne Galindez (Coordinadora de eLearning), Gentzane Aldekoa (Coordinadora de Formación Continua) y Eduardo Sánchez (Sistemas de Información).

REFERENCIAS

[1] L. Pappano, «The Year of the MOOC,» 2 Noviembre 2012. http://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html?_r=0.

[2] P. Hyman, «In the year of disruptive education,» *Communications of the ACM,* vol. 55, nº 12, pp. 20-22, 2012.

[3] Liyanagunawardena, T. R., Adams, A. A., & Williams, S. A. (2013). MOOCs: A systematic study of the published literature 2008-2012. The International Review of Research in Open and Distributed Learning, 14(3), 202-227.

[4] Chiappe-Laverde, A., Hine, N., & Martínez-Silva, J. A. (2015). Literatura y práctica: una revisión crítica acerca de los MOOC - Literature and Practice: A Critical Review of MOOCs. Comunicar, 22(44), 09-18.

[5] Jordan, K. (2014). Initial trends in enrolment and completion of massive open online courses. The International Review of Research in Open and Distributed Learning, 15(1).

[6] Emanuel, E. J. (2013). Online education: MOOCs taken by educated few. Nature, 503(7476), 342-342.

[7] Rodriguez, C. O. (2012). MOOCs and the AI-Stanford like courses: Two successful and distinct course formats for massive open online courses. European Journal of Open, Distance and E-Learning, 15(2).

[8] Muñoz, A. M., & Ramió, J. (2013). Crypt4you y la utilidad de los MOOCs en la formación online en lengua española. Innovación educativa, (23).

[9] Porras, M. D. L. G., Ramirez, R. C., & Montoya, M. S. R. (2014). Diseño de autoestudios multimedia para competencias digitales: Caso del primer MOOC latinoamericano. Edutec. Revista Electrónica de Tecnología Educativa, (47).

[10] Á. Fidalgo Blanco, M. L. Sein-Echaluce Lacleta y F. J. García Peñalvo, «MOOC cooperativo. Una integración entre cMOOC y xMOOC,» de *II Congreso Internacional sobre Aprendizaje, Innovación y Competitividad (CINAIC 2013)*, Madrid, 2013.

[11] P. Sánchez y C. Blanco, «Una Metodología para fomentar el aprendizaje mediante sistemas de evaluación entre pares,» de *Jornadas de Enseñanza Universitaria de la Informática (JENUI)*, Castellón de la Plana, 2013.

[12] J. Cabero Almenara, M. d. C. Llorente Cejudo y A. I. Vázquez Martínez, «Las tipologías de MOOC: su diseño e implicaciones educativas,» *Profesorado. Revista de Curriculum y Formación del Profesorado,* vol. 18, nº 1, pp. 13-26, 2014.

[13] D. Torres Mancera y D. Gago Saldaña, «Los MOOC y su papel en la creación de comunidades de aprendizaje y participación,» *RIED. Revista Iberoamericana de Educación a Distancia,* vol. 17, nº 1, pp. 13-34, 2014.