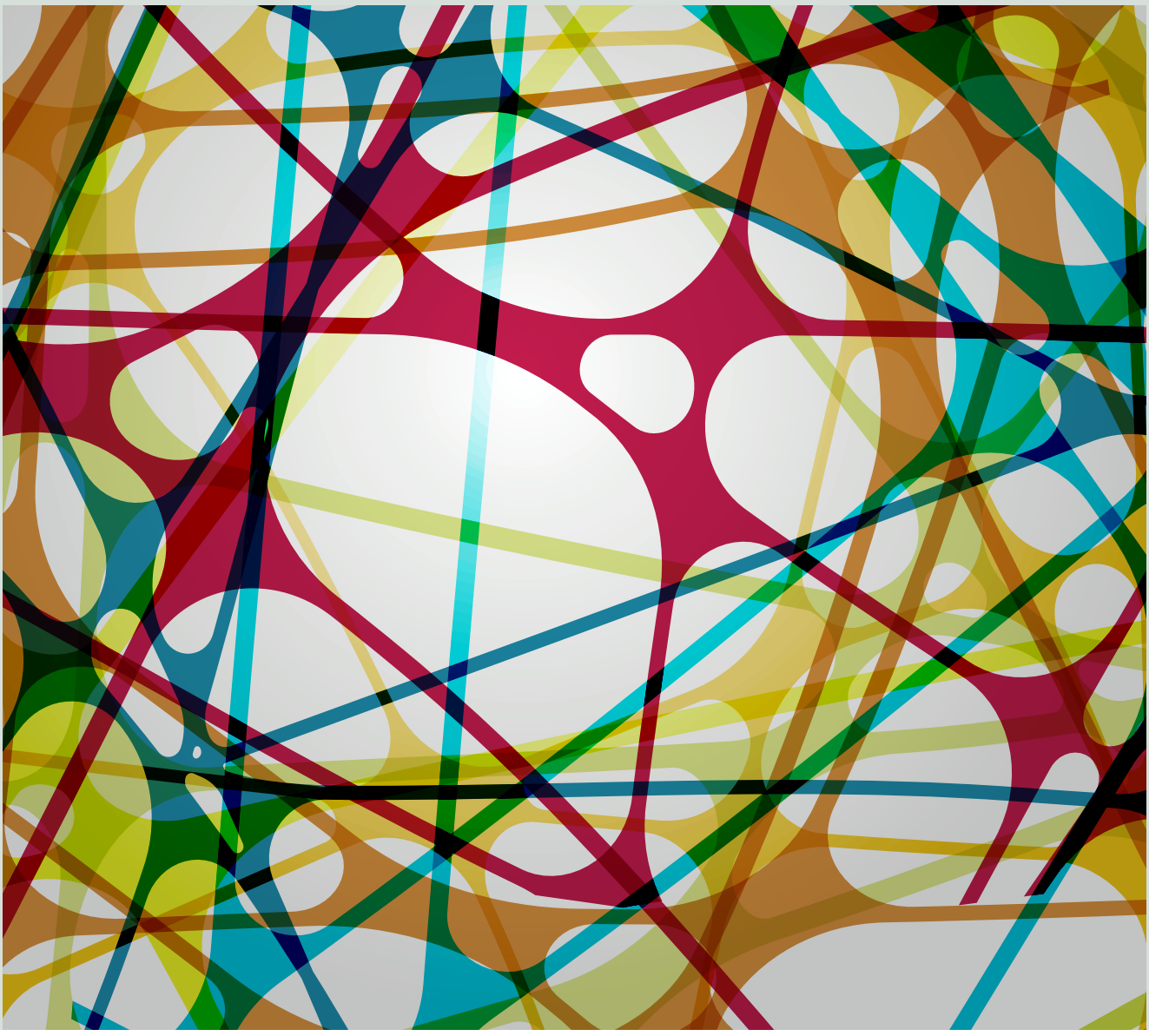
Universitat d'Alacant
Universidad de Alicante

I³CE

Memòries del Programa de Xarxes-I3CE de qualitat, innovació i investigació en docència universitària. Convocatòria 2019-20

Memorias del Programa de Redes-I³CE de calidad, innovación e investigación en docencia universitaria. Convocatoria 2019-20



Rosabel Roig Vila, R. (Coord.)
Jordi M. Antolí Martínez, Rocío Díez Ros, Neus Pellín Buades (Eds.)

UA | UNIVERSITAT D'ALACANT
ICE Institut de Ciències de l'Educació
Instituto de Ciencias de la Educación

Memòries del Programa de Xarxes-I3CE de qualitat, innovació i investigació en docència universitària. Convocatòria 2019-20

Memorias del Programa de Redes-I3CE de calidad, innovación e investigación en docencia universitaria.Convocatoria 2019-20

Rosabel Roig-Vila (Coord.),
Jordi M. Antolí Martínez, Rocío Díez Ros & Neus Pellín Buades (Eds.)

UA | UNIVERSITAT D'ALACANT
UNIVERSIDAD DE ALICANTE
ICE Institut de Ciències de l'Educació
Instituto de Ciencias de la Educación

2020

Memòries de les xarxes d'investigació en docència universitària pertanyent al ProgramaXarxes-I3CE d'Investigació en docència universitària del curs 2019-20 / *Memorias de las redes de investigación en docencia universatira que pertence al Programa Redes -I3CE de investigación en docencia universitaria del curso 2019-20*

Organització: Institut de Ciències de l'Educació (Vicerectorat de Qualitat i Innovació Educativa) de la Universitat d'Alacant/ *Organización: Instituto de Ciencias de la Educación (Vicerrectorado de Calidad e Innovación Educativa) de la Universidad de Alicante*

Edició / Edición: Rosabel Roig-Vila (Coord.), Jordi M. Antolí Martínez, Rocío Díez Ros & Neus Pellín Buades (Eds.)

Comité tècnic / Comité técnico: Neus Pellín Buades

Revisió i maquetació: ICE de la Universitat d'Alacant/ Revisión y maquetación: ICE de la Universidad de Alicante

Primera edició: / *Primera edición*:

ice@ua.es

ISBN: 978-84-09-24478-2

Producció: Institut de Ciències de l'Educació (ICE) de la Universitat d'Alacant / Producción: Instituto de Ciencias de la Educación (ICE) de la Universidad de Alicante

EDITORIAL: Les opinions i continguts dels textos publicats en aquesta obra són de responsabilitat exclusiva dels autors. / *Las opiniones y contenidos de los textos publicados en esta obra son de responsabilidad exclusiva de los autores.*

22. Acción educativa transversal entre grado de ingeniería multimedia y máster en Ciberseguridad para la mejora de competencias en ciberseguridad

J.V. Berná Martínez; F. Maciá Pérez; I. Lorenzo Fonseca; J.A. Gil Martínez-Abarca; D. Gil Méndez; F.J. Mora Gimeno; G. Candela Romero; M. Marco Such; M.P. Escobar Esteban; M.D. Sáez Fernández;

jvberna@ua.es, pmacia@dtic.ua.es, iren.fonseca@ua.es, gil@eps.ua.e, dgil@dtic.ua.es, fjmora@dtic.ua.es
Departamento de Tecnología Informática y Computación
Universidad de Alicante
gcandela@ua.es, marco.such@ua.es, mpilar.escobar@ua.es, md.saez@ua.es
Departamento de Lenguajes y Sistemas Informáticos
Universidad de Alicante

RESUMEN

Este trabajo expone el planteamiento y los resultados de una acción innovadora en la que se propuso un trabajo en el que colaboran alumnos de distintas titulaciones y nivel académico. Esta colaboración tiene el objetivo de proponer una práctica en la cual alumnos del Máster en Ciberseguridad y del 4º curso Grado en Ingeniería Multimedia se necesitan para llevar a cabo una práctica, ya que los resultados de unos sirven de entrada a los otros. Esta práctica persigue ofrecer un escenario dónde los alumnos encuentren mayor realismo y paralelismo con el mundo laboral en que desempeñarán sus funciones y así mejorar las competencias relacionadas en este caso con la ciberseguridad. Para los alumnos de máster permitió realizar análisis de penetración, auditoría y generación de planes de seguridad sobre sistemas web complejos, reales y diversos producidos por los alumnos de grado y practicar la intervención para la resolución de incidentes. A los alumnos de grado les permitió conocer como es una auditoría de ciberseguridad, que fallos habían cometido en el desarrollo de sus sistemas y la forma de solucionarlos. Esta colaboración sería la que se realizaría en el mundo real y ha permitido a todos poner en prácticas sus competencias.

Palabras clave: competencias, ciberseguridad, prácticas realistas

ISBN: 978-84-09-24478-2

1. INTRODUCCIÓN

En la Universidad de Alicante, las carreras relacionadas con tecnologías desarrollan al menos el 50% de su carga docente mediante clases prácticas en las cuales los alumnos han de desarrollar, mediante supuestos cercanos a su profesión, las competencias a tratar en cada asignatura. Esto supone que el profesorado tiene que preparar entornos artificiales que simulan casos mediante cuya resolución los alumnos exhiben y practican sus habilidades y conocimientos. Esta hace que se busquen mediante diferentes estratégicas la forma de desarrollar estos escenarios, muchos de ellos virtualizados precisamente para poder ofrecer una realidad "virtual" al alumno cercana a lo que será el propio desarrollo de su labor profesional (Castaño Garrido et al., 2008). La preparación de estos entornos artificiales no es tarea sencilla, sobre todo si queremos lograr una alta efectividad en el entrenamiento (García Martínez et al. 2015), lo que implica a los profesores un gran esfuerzo para prepararlos y así logra entornos que ofrezcan los restos adecuados a los alumnos, protegerlos frente a mal uso o copia, dotarlos de elementos que los hagan atractivos y motivadores y en general lograr una educación integral e integradora (Maciá Pérez et al., 2014)

En nuestra universidad de imparten el Máster en Ciberseguridad (Ciberseguridad, 2020) y el Grado en Ingeniería Multimedia (Multimedia, 2020) y varios profesores imparten docencia en ambos títulos. Esto ha hecho que conozcan las necesidades que tienen ambas titulaciones en cuestión de preparar los entornos de prácticas. En ciberseguridad, para varias asignaturas, a los alumnos se les proporcionaba entornos profesionales de código abierto donde los alumnos realizan las prácticas. En multimedia sin embargo, las competencias en ciberseguridad apenas se trabajan porque no están explícitamente en los temarios. Sin embargo en multimedia, en 4º, se utiliza el aprendizaje basado en proyectos (Berná Martinez et al., 2017) mediante el cual todas las asignaturas se unen para que los alumnos trabajen a lo largo de un único proyecto, que en este caso produce una aplicación web profesional de calado. Esta situación hizo que los profesores planteasen la idea de utilizar los trabajos de Multimedia como entradas para los análisis de Ciberseguridad y a su vez, los resultados producidos por estos alimentaran de nuevo los proyectos de Multimedia para mejorar las características de seguridad. La figura 1 muestra un esquema de este planteamiento y las asignaturas implicadas. Las imágenes que aparecen en el lado izquierdo la figura son capturas de las 7 aplicaciones desarrolladas por los alumnos de multimedia y que han sido presentadas en el evento UAContenidos del curso 2019-2020 (UAcontenidos, 2020), un evento online donde se exhiben los proyectos públicamente.

Figura 1. Escenario de prácticas donde los resultados de multimedia son usados por los alumnos de ciberseguridad y los resultados de ciberseguridad por los alumnos de multimedia

Mediante este planteamiento se podrían cubrir todos los objetivos de todas las asignaturas y a la vez hacerlo de una forma más enriquecedora a la par de útil y realista.

2. OBJETIVOS

El objetivo de esta acción es la creación de escenarios de prácticas realistas para lo cual se utilizará el propio trabajo de los alumnos de una titulación como recurso para ser usado por los otros. Para ello el objetivo principal se divide en dos sub-objetivos:

En el caso de Ciberseguridad el sub-objetivo es crear entornos de aplicaciones complejas y realistas para quedan ser sometidas a los procesos de análisis y auditoría que los profesionales de este sector realizan y cuyas competencia se desarrollan a lo largo del máster.

En el caso de Multimedia el objetivo es proporcionar a los alumnos un análisis sobre ciberseguridad de sus proyectos que les permita conocer los puntos débiles de sus desarrollos y la forma de solucionarlos.

3. MÉTODO

3.1. Descripción del contexto y de los participantes

En el Máster de Ciberseguridad, con una media de 20 alumnos anuales, entre otras se imparten las asignaturas de Sistemas de Gestión de la Seguridad (SGS), en el primer semestre, y Hacking Ético y Contramedidas (HEC), en el segundo.

Para el desarrollo de las competencias de la asignatura SGS a los alumnos se les proporciona unos supuestos de sistemas sobre los cuales han de realizar una auditoría de seguridad. Para crear estos supuestos el profesorado desarrolla sobre papel todos los contenidos referentes a una empresa ficticia donde se enuncian las infraestructuras y recursos físicos que dicha empresa posee, el personal y las características del mismo, las instalaciones físicas donde se desarrolla una actividad por parte de la empresa y en general se describe con detalle todos los aspectos que los alumnos de SGS van a necesitar para desarrollar sus prácticas de auditoría. Estas prácticas tienen como objetivos detectar las amenazas más importantes a las que está sometido el supuesto planteado y crear los planes de seguridad que permitirían evitarlos.

Por otro lado, para el desarrollo de las competencias de la asignatura HEC también se crean diversos escenarios donde los alumnos han de poner en práctica sus hacer ataques de penetración de ciberseguridad, buscando los puntos débiles que poseen, encontrando la forma de explotarlos y una vez más proponiendo solución.

Ambas asignaturas plantean sistemas virtuales o supuestos teóricos sobre los que los alumnos trabajan. Para poder realizar prácticas útiles y efectivas estos escenarios han de ser muy realistas, a la vez que se controla que posean los elementos (en este caso los fallos de seguridad que los alumnos han de detectar) para que se puedan practicar las habilidades de los alumnos. Cada año se cambian estos escenarios para hacerlos más sofisticados, enriquecerlos, evitar copias de años anteriores a la vez que mantener alto el ánimo de los alumnos por presentarles retos nuevos en cada curso. Y todo este trabajo exige una gran inversión temporal del profesorado.

Por otro lado, en Ingeniería Multimedia, en 4º, los alumnos siguiendo una metodología ABP que

ISBN: 978-84-09-24478-2

integra a todas las asignaturas de último curso han de producir una aplicación web que tiene el tamaño, características y tipología de una aplicación comercial como la que podría suministrar cualquier empresa. Las asignaturas 7 que forman 4º de multimedia son Proyectos Multimedia (PM), Técnicas Avanzadas de Gráficos (TAG), Servicios Multimedia Basados en Internet (SMBI), Sistemas de Difusión Multimedia (SM), E-Learning (EL), Servicios Multimedia Avanzados (SMA) y Negocio Multimedia (NM). Durante el desarrollo del curso, una de las competencias que no se trabaja directamente es la de la ciberseguridad, ya que no hay ninguna asignatura que la incluya directamente, pero sin embargo es necesario abordarla porque este es un aspecto esencial en cualquier aplicación. Para ello se trabaja un tema durante el curso en la asignatura de SMBI u otro en SMA y además se hace una revisión final de los proyecto, pero dado el calado que tiene cada proyecto (aplicaciones web con miles de líneas de código y centenares de funcionalidades) solo se puede hacer una revisión superficial sobre ciberseguridad del proyecto.

Los participantes por tanto son algunos de los profesores de ambas titulaciones, algunos los cuales imparten docencia tanto en el máster como en el grado, los 20 alumnos que han formado el curso del máster en ciberseguridad y los 38 alumnos que han formado el itinerario de gestión de contenidos del grado de multimedia.

3.2. Descripción del instrumento utilizado para la investigación o la evaluación de la innovación educativa

Para realizar la evaluación de la innovación educativa se ha seleccionado el procedimiento de encuestas, mediante la cual conocer el grado de satisfacción y de percepción de utilidad por parte de los alumnos. Se han diseñado dos cuestionarios diferentes, uno para cada titulación. La encuesta del máster está orientada a conocer el grado de utilidad de los escenarios. La encuesta del grado se orienta a conocer cuánto mejoran las competencias en ciberseguridad.

3.3. Procedimiento

Las fases para el diseño y la puesta en marcha de esta actividad ha sido las siguientes:

Fase 1. Puesta en común.

Reunión con los profesores que imparten asignaturas en 4º de multimedia y en ciberseguridad (asignaturas de SGS y HEC), puesta en común de necesidades para los alumnos y objetivos a cumplir. También se definieron ciertos requerimientos software que era necesario que los sistemas de multimedia tengan para que los alumnos de ciberseguridad pudiesen poner en práctica sus competencias.

Fase 2. Elaboración de enunciado de la práctica.

Se redactó un documento que se enunciaba la práctica y que sería entregado a todos los estudiantes implicados, máster y grado, en el cual se redactaba las tareas de cada uno de los grupos de alumnos y se indicaban os resultados esperados por cada titulación y el trabajo a realizar en torno a ese resultado.

Fase 3. Planificación y diseño de encuestas.

Se planificaron las fechas en las cuales cada grupo de alumnos tendría que llevar a cabo s parte y además los mecanismos mediante los cuales se comunicarían y trasladarían los recursos de unos a otros.

También se diseñaron dos encuestas, una para los alumnos de cada titulación con objetivos dirigidos a los intereses de cada grupo.

Fase 4. Ejecución.

Se lanzaron las prácticas a los alumnos junto a la planificación para que fuesen ejecutadas.

Fase 5. Encuestas.

Se suministraron las encuestas a los grupos de alumnos y se recogieron sus valoraciones sobre la actividad.

4. RESULTADOS

Los resultados obtenidos a través de los cuestionarios realizados por los alumnos son de tipo cualitativo y ofrecen las siguientes conclusiones.

El primero cuestionario es el de los alumnos del máster en ciberseguridad, en el cual se han recogido aspectos como la complejidad percibida de los entornos a analizar, el tiempo que han requerido para el desarrollo de las prácticas, si les han gustado las propuestas y cómo de útiles les han resultado para desarrollar sus competencias. De este cuestionario se ha extraído que en general a los alumnos les ha parecido muy interesante poder practicar con aplicaciones desarrolladas por otros estudiantes completamente ajenos al máster y que prefieren este tipo de aplicaciones a otras que simular los problemas, ya que los incidentes de seguridad analizados y resueltos son más diversos, más difíciles de localizar y ha exigido profundizar más, pero que al ser sobre sistemas reales en producción se han sentido muy motivados y más cercanos a su realidad laboral.

El segundo es el de los alumnos del grado de ingeniería multimedia, donde se les ha preguntado por los informes que han sido presentados sobre sus herramientas, el tiempo que han requerido para la corrección de los problemas (o su no corrección si era imposible), sobre si les ha parecido interesante haber sido sometidos a una auditoría externa, si los resultados ofrecidos tenían la calidad esperada y de si este ejercicio ha influido positivamente o negativamente en sus competencias sobre ciberseguridad. En general los alumnos han percibido esta actividad como muy valiosa, ya que han podido mejorar notablemente sus sistemas. Todos han coincidido en que han mejorado sus competencias en ciberseguridad, ya que los reportes que han recibido trataban aspectos desde muchas aristas de la ciberseguridad que desde el grado no se pueden tratar y que al menos de una forma superficial han podido ver. Además al conocer que iban a ser auditados han mostrado más cuidado y esfuerzo en la parte de seguridad y al recibir los resultados han podido profundizar en competencias que en la carrera ni se ven y que mejoran sus capacidades profesionales.

5. CONCLUSIONES

La principal que extraemos de este trabajo es que la interrelación de los profesores de entre distintas titulaciones y niveles académicos puede proporcionar unos recursos valiosos para mejorar nuestra docencia. Muchas veces los profesores estamos absortos en nuestra propia docencia y reinventamos la rueda una y otra vez. Sin embargo tras analizar el trabajo que se realizan en otras asignaturas y titulaciones, hemos podido comprobar que podemos utilizar las salidas de unas como entradas para otras y viceversa. Otra de las conclusiones a las que hemos llegado es que a los alumnos les inquieta mucho en un principio compartir su trabajo, pero que una vez que asumen que esto un ejercicio cotidiano, se sienten muy motivados (por no decir orgullosos) de poder mostrar su trabajo a otros alumnos y cuando reciben críticas constructivas de estos otros alumnos lo perciben más como una colaboración que como una corrección (que sería lo que percibirían si fuese un profesor el que les proporciona el feedbak). Esta corrección

ISBN: 978-84-09-24478-2

por pares entre titulaciones además se ve reforzada porque los alumnos de multimedia perciben a los de máster como expertos en ciberseguridad y por tanto valoran su criterio más que el de cualquier otro compañero, por lo menos en el sentido de la ciberseguridad. A los alumno del máster por su lado les ha ocurrido algo similar, al encontrarse con aplicaciones extraordinariamente grandes mucho más allá de las tradicionales prácticas acotadas y predecibles, donde no se conocía el resultado a priori, y donde han podido dar lo mejor de sí sin límites, lo han percibido como un reto más que como una trabajo e incluso han agradecido poder interactuar con los alumnos de multimedia, igual que si ayudaran a un cliente a solucionar sus problemas de ciberseguridad.

Como conclusión final extraemos que al brindan a los alumnos escenarios de prácticas realistas, pero conservando el hecho de que no es real (son trabajas de otros alumnos), los alumnos se sienten más motivados, realizan más trabajo y perciben que su trabajo tiene más sentido. El hecho de no utilizar empresas reales asegura que en ningún caso se vería afectado un negocio, por eso no saltar al mundo real y utilizar siempre productos realistas pero no reales.

Como trabajo futuro nos queda seguir ampliando este planteamiento a otras asignaturas, ya que hemos vistos como asignaturas de 3º de multimedia podrían utilizarse también para hacer este tipo de colaboraciones cruzadas con 4º en este caso.

6. TAREAS DESARROLLADAS EN LA RED

Aunque el trabajo ha sido global, cada miembro de la red ha sido responsable de un área de trabajo para facilitar así la definición de los sistemas que los alumnos de multimedia debían analizar y que sirviesen a los propósitos de ciberseguridad.

PARTICIPANTE DE LA RED	TAREAS QUE DESARROLLA
José Vicente Berná Martínez	Coordinación de la Red.
Francisco Maciá Pérez	Definición de requerimientos software en sistemas distribuidos
Iren Lorenzo Fonseca	Definición de requerimientos de ciberseguridad en componentes software
Juan Antonio Gil Martínez-Abarca	Diseño de auditoría ciberseguridad de servicios e infraestructuras
David Gil Méndez	Definición de indicadores de ciberseguridad para aplicaciones Web
Francisco José Mora Giménez	Diseño de pruebas de hacking ético y contramedida para aplicaciones web
Gustavo Candela Romero	Diseño de interfaces para aplicaciones y especificación para la práctica
Manuel Marco Such	Definición de requerimientos de calidad
María Pilar Escobar Esteban	Diseño de la especificación funcional de las aplicaciones web

María dolores Sáez Fernández	Diseño de cuestionarios para recogida de resultdos

7. REFERENCIAS BIBLIOGRÁFICAS

Castaño Garrido, C. M., Maiz Olazabalaga, I., Palacio Arco, G. J., & Villarroel Villamor, J. D. (2008). Prácticas educativas en entornos Web 2.0. Madrid: Síntesis, 2008.

García Martínez, A., Guerrero Proenza, R. S., & Granados Romero, J. M. (2015). Buenas prácticas en los entornos virtuales de enseñanza-aprendizaje. Revista Cubana de Educación Superior, 34(3), 76-88.

Maciá Pérez, F., Berná Martínez, J. V., Lorenzo Fonseca, I., Rodríguez Jaume, M. J., Fuster Guilló, A., & Mañas Viejo, V. (2014). Estrategia MOOC en la Universidad de Alicante para la Educación Digital del Futuro. UA| edf. Jornadas de Enseñanza Universitaria de la Informática (20es: 2014: Oviedo).

Ciberseguridad, Máster (2020). Información online sobre el Máster en Ciberseguridad oficial de la Universidad de Alicante. https://cvnet.cpd.ua.es/webcvnet/PlanEstudio/planEstudioND.aspx?plan=D104

Multimedia, Grado (2020). Información online sobre el Grado en Ingeniería Multimedia oficial de la Universidad de Alicante. https://web.ua.es/es/grados/grado-en-ingenieria-multimedia/plan-de-estudios.html

Berná Martínez, J. V. , Martínez-Abarca, J. A. G., Méndez, D. G., Escamez, P. M., Villagrá-Arnedo, C. J., Carmona, R. M., ... & Such, M. M. (2017). Organización docente, coordinación y desarrollo de Metodología Transversal ABP en 4º grado de Ingeniería Multimedia: Itinerario de Gestión de Contenidos. In Memorias del Programa de Redes-I3CE de calidad, innovación e investigación en docencia universitaria: convocatoria 2016-17 (pp. 108-119). Instituto de Ciencias de la Educación.

UAcontenidos (2020). Evento de presentación de proyectos de gestión de contenidos del curso 2019-2020, retransmisión a través del canal de Youtube de la UA disponible online en https://www.youtube.com/watch?v=jmMcccXBc7w

ISBN: 978-84-09-24478-2