IX Congreso iberoamericano
de seguridad informática
Universidad de Buenos Aires
Ciudad Autónoma de Buenos Aires, Argentina
1 al 3 de noviembre de 2017

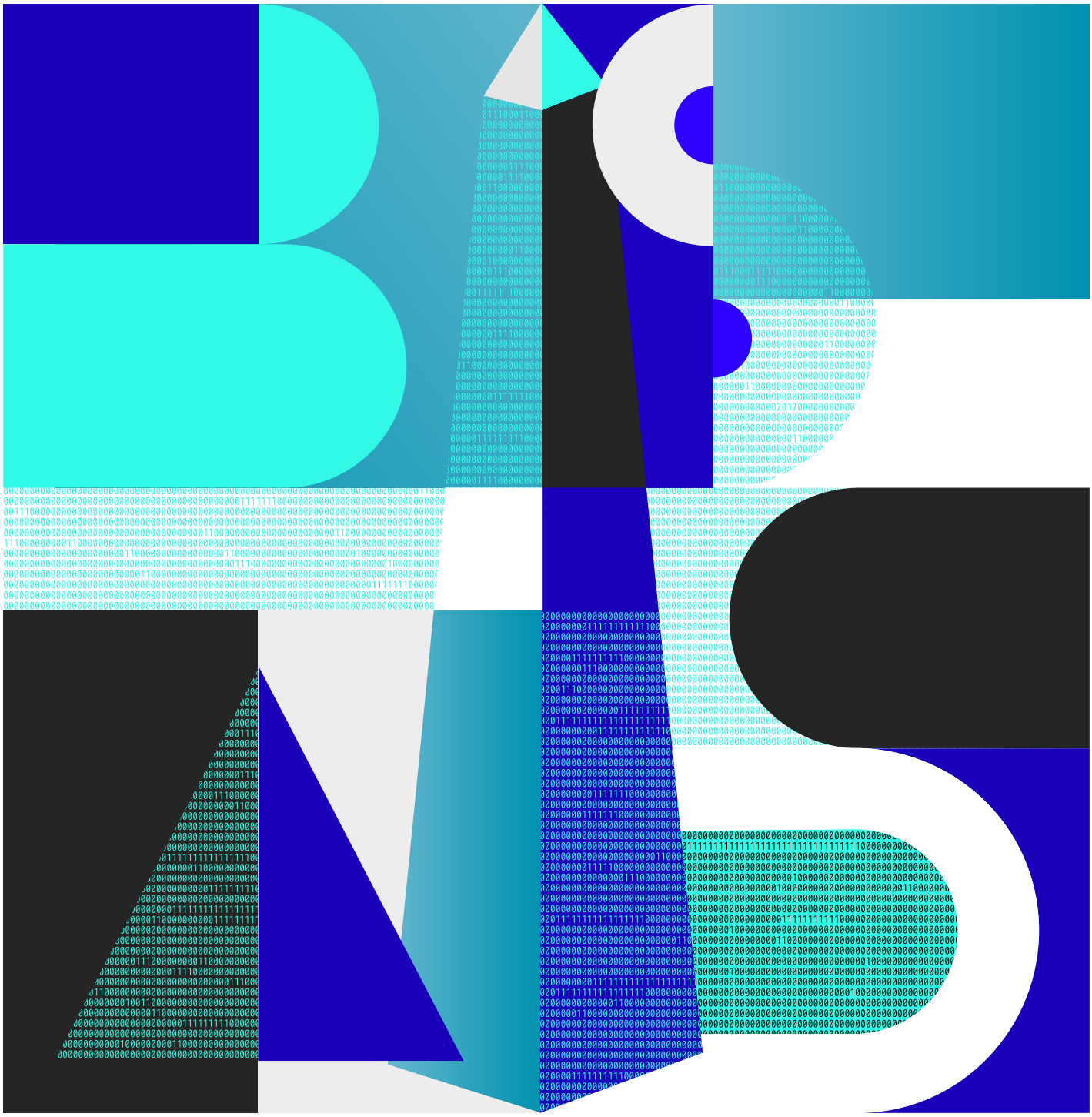
CIBSI

EU DE BA

PSI
POSGRADO EN SEGURIDAD INFORMATICA

CRIPTORED

Libro de Actas



Actas del IX Congreso Iberoamericano de Seguridad Informática
CIBSI2017, Buenos Aires, Argentina, 1 al 3 de Noviembre de 2017

Editores
Alberto E. Dams
Hugo A. Pagola
Luis E. Sánchez Crespo
Jorge Ramió Aguirre

Diseño de Tapas
Federico Dams

ISBN: en trámite

Prefacio

Del 1 al 3 de Noviembre se celebrará en la Universidad de Buenos Aires el IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017. El congreso está organizado por la Maestría en Seguridad Informática de la UBA en colaboración con la Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored.

Este espacio permitirá a las empresas, entidades públicas, entornos militares, de defensa, centros académicos y de investigación exponer sus avances y servicios vinculados con la seguridad, facilitando el intercambio de conocimientos y la formación de redes de colaboración en este ámbito.

El congreso contará con la presencia de especialistas de Latinoamérica y de Europa entre otros de Argentina, Brasil, Colombia, Ecuador, México, Perú, Uruguay, España y Francia. Estamos muy satisfechos por el nivel de los artículos que se presentarán y el de los invitados especiales que tendremos. En esta novena edición del CIBSI, se destacan las presencias de referentes internacionales en la materia como Hugo Scolnik director de la Maestría en seguridad Informática de la UBA y Hugo Krawczyk Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center.

Organización de la Conferencia

Comité Organizador

Hugo Pagola, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Alberto Dams, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España
Luis E. Sánchez Crespo, Universidad de Castilla La Mancha, España

Comité Local

Facundo Caram, FIUBA, Argentina
Luis Catanzariti, UTNfrba, Argentina
Marcia Maggiore, MUBA, Argentina
Patricia Prandini, MUBA, Argentina

Comisión de Posgrado Maestría en Seguridad Informática UBA

Mg Ing Alberto Dams, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Pedro Hecht, Maestria en Seguridad Informatica UBA, Argentina
Ing Hugo Pagola, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Ricardo Rivas, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Raul Saroka, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Hugo Scolnik, Maestria en Seguridad Informatica UBA, FCEN-UBA Argentina

Comité del Programa

Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp, Brasil
Javier Areitio	Universidad de Deusto, España
Rodolfo Baader	Universidad de Buenos Aires, Argentina
Gustavo Betarte	Facultad de Ingeniería, Universidad de la República, Uruguay
Carlos Blanco Bueno	Universidad de Cantabria, España
Joan Borrell	Universitat Autònoma de Barcelona, España
Pino Caballero-Gil	DEIOC, Universidad de La Laguna, España
Jeimy Cano	Universidad de los Andes, Colombia
Eduardo Carozo	Universidad de Montevideo, Uruguay
Joan-Josep Climent	Universitat d'Alacant, España
Roger Clotet	Universidad Simón Bolívar, Venezuela
Alberto Dams	Universidad de Buenos Aires, Argentina
José María De Fuentes	Universidad Carlos III de Madrid, España
Josep Domingo-Ferrer	Universitat Rovira i Virgili, España
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, España
Angelica Florez Abril	Universidad Pontificia Bolivariana, Colombia
Walter Fuertes	Universidad de las Fuerzas Armadas ESPE, Ecuador
Amparo Fuster-Sabater	Institute of Applied Physics, Madrid, España
Giovana Garrido	Universidad Tecnologica de Panama
Lorena González Manzano	Universidad Carlos III de Madrid, España
Juan Pedro Hecht	Universidad de Buenos Aires, Argentina

Luis Hernandez Encinas	Institute of Physical and Information Tecnologies, España
Emilio Hernández	Universidad Simón Bolívar, Venezuela
Leobardo Hernández	Universidad Nacional Autónoma de México
Jordi Herrera	Universitat Autònoma de Barcelona, España
Monica Karel Huerta	Universidad Politécnica Salesiana, Ecuador
Angel Martin Del Rey	Universidad de Salamanca, España
Maria Vanina Martinez	Universidad Nacional del Sur in Bahia Blanca, Argentina
Vincenzo Mendillo	Universidad Central de Venezuela
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María, Chile
Karel Huerta Monica	Universidad Politécnica Salesiana, Ecuador
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados, Mexico
Alfonso Muñoz	Criptored, España
Hugo Pagola	UBA - Facultad de Ingenieria, Argentina
Graciela Pataro	Universidad de Buenos Aires, Argentina
Alberto Peinado	Universidad de Malaga, España
Jose Pirrone	Universidad Catolica Andres Bello, Venezuela
Gustavo Presman	Universidad de Buenos Aires, Argentina
Jorge Ramio	Universidad Politécnica de Madrid, España
Ricardo Rivas	Universidad de Buenos Aires, Argentina
David Rosado	University of Castilla-La Mancha, España
Luis Enrique Sanchez Crespo	Universidad de Castilla La Mancha, España
Antonio Santos-Olmo Parra	Sicaman Nuevas Tecnologías
Raul Saroka	Universidad de Buenos Aires, Argentina
Hugo Scolnik	Universidad de Buenos Aires, Argentina
Pablo Silberfich	Universidad de Buenos Aires, Argentina
Jenny Torres	Escuela Politécnica Nacional, Ecuador
Urko Zurutuza	Mondragon University, España

eMarisma: Aplicación Práctica en la Asignatura de Seguridad de Sistemas Software

D.G. Rosado, L. E. Sánchez, A. Santos-Olmo, I. Caballero, E. Fernandez-Medina

***Abstract* — We currently live in a world that is increasingly requesting a greater link between universities and enterprises. The concept of technology transference is becoming of vital importance for the engineers in Europe and Latin America, since it comprises a mechanism by which to adapt to a constantly changing world led by new technologies. The objective of this paper is to show the results obtained during research into Cyber Security carried out in conjunction by the GSyA group from the University College of the University of Castilla-La Mancha and the Sicman Nuevas Tecnologías company, whose objective was the development of a product denominated as eMARISMA and its subsequent introduction into the subject of Software Systems Security, which is taught as an intensification of Software Engineering. The introduction of the product has enabled us to analyze the students' perception and use of it, thus allowing us to obtain relevant results for our research.**

***Index Terms* — Technology Transfer, Degree in Computer Engineering, MARISMA, Risk Analysis.**

I. Introducción

Actualmente, Europa se encuentra inmersa en el proceso de convergencia de la educación superior, que es fundamental para el futuro de algunas carreras, y por ello es muy importante ser capaces de adaptar los nuevos planes de estudio a las necesidades reales del mercado en este sector. En el caso de la Ingeniería Informática, las empresas y los profesionales están demandando perfiles cada vez más especializados y que se adapten a una o varias certificaciones profesionales internacionales. Además, estos profesionales deben haber trabajado con herramientas reales del mercado que les hayan acercado lo máximo posible a la realidad de la empresa. Por lo tanto, es muy importante que los nuevos estudios estén muy enfocados a las necesidades profesionales sin perder el rigor científico exigible en una ingeniería, y para conseguir este objetivo es fundamental que estos nuevos planes de estudio tengan una orientación que facilite la transferencia tecnológica entre la Universidad y la Empresa.

Para lograr el objetivo propuesto se alinearon los intereses del Grupo de Investigación GSyA, especializado en Seguridad Informática, y la empresa Sicaman Nuevas Tecnologías, especializada en el mismo campo y con capacidad de validar los resultados de la investigación en clientes. Durante los últimos 15 años ambas entidades han trabajado en desarrollar una metodología para gestión de seguridad y análisis de riesgos denominada MARISMA [1, 2], que ha ido evolucionando mediante la aplicación de dos técnicas de investigación muy utilizadas en el campo de la Ingeniería del Software denominadas “Revisión Sistemática de la Literatura” e “Investigación en Acción” [3-7]. Esta metodología ha sido completada con una herramienta que da soporte a la misma llamada eMARISMA [8], accesible en modelo SaaS.

En el año 2017 y después de más de una década de validación en el sector privado se ha decidido dar un paso más y comenzar su implantación dentro del sistema universitario, de forma que los alumnos puedan disponer de una herramienta con la que practicar y enfrentarse a casos reales. Una herramienta nacida del alineamiento entre la Universidad y la Empresa y con una clara orientación práctica, pero manteniendo siempre el rigor científico. Está herramienta adicionalmente presenta funcionalidades que permiten asociar riesgos entre diferentes análisis de riesgos, con lo que a futuro se tiene la posibilidad de realizar prácticas más complejas, asociando resultados de diferentes grupos, o incluso entre diferentes universidades.

En este artículo se presentan algunos de los resultados obtenidos por los alumnos al utilizar eMARISMA en la asignatura Seguridad de Sistemas Software, la cual forma parte de la intensificación de Ingeniería del Software impartida en la Escuela Superior de Ingeniería Informática del Campus de Ciudad (Universidad de Castilla-la Mancha). Esta investigación ha supuesto la creación de equipos docentes multidisciplinares, con experiencia académica pero también con experiencia profesional.

El artículo estará formado por ocho secciones: En la segunda sección ponemos en contexto la importancia del momento actual de creación de planes de estudio y de la transferencia tecnológica. En la tercera sección se analizará la estructura general del plan de estudios para la Ingeniería Informática propuesta en la Universidad de Castilla-la Mancha. En la cuarta sección se analizará la asignatura que se ha utilizada para investigación. En la quinta sección se introducirá la metodología MARISMA y la herramienta que la soporta. En la sexta sección se plantea la práctica que los alumnos deben acometer. En la séptima sección se analizarán algunos de los resultados obtenidos durante la investigación. Finalmente, en la última sección describiremos las principales conclusiones obtenidas hasta el momento y los siguientes pasos.

D. G. Rosado, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, David.Garcia@uclm.es

L. E. Sánchez, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Luisenrique@sanchezcrespo.org

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, asolmo@sicaman-nt.com

I. Caballero, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real España, Ismael.Caballero@uclm.es

E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

II. Estado del Arte

El Espacio Europeo de Educación Superior (EEES) se inicia con la Declaración de la Sorbona de 1998, que destacó el papel de las Universidades en el desarrollo de la dimensión cultural y de la Europa del conocimiento, y se amplía con las Declaraciones de Bolonia (Junio de 1999), de Praga (2001) y de Berlín (Septiembre de 2003) y Bergen (Mayo de 2005). En ellas se acordó promover y desarrollar en los países participantes la reforma de la estructura y la organización de las enseñanzas universitarias para estimular la construcción de un Espacio Europeo de Educación Superior con el objetivo de favorecer la movilidad y las oportunidades de empleo, y además hacer que estos nuevos planes de estudio y su implantación se adaptasen a las demandas de las empresas [9], de forma que sirvan para hacer que los nuevos profesionales aumenten la productividad del tejido empresarial Europeo [10].

Actualmente, la mayor parte de los grados ya se han definido, pero gran parte de las Universidades Europeas se encuentran en pleno proceso de implantación de los nuevos planes de estudio del Grado en Ingeniería Informática, basándose para ello en las intensificaciones propuestas por la ACM [11], las cuales están muy orientadas a competencias excesivamente complejas y difusas, y que en algunos casos ya están siendo revisadas por otros investigadores [12-14].

En el caso del grado en ingeniería informática, los nuevos planes se han orientado a la existencia de un grado único con cinco especialidades o intensificaciones. Estas cinco intensificaciones se corresponden con las Tecnologías Específicas de la Resolución de 8 de junio de 2009 de la Secretaría General de Universidades, por la que se da publicidad al Acuerdo del Consejo de Universidades que establece recomendaciones para la propuesta por las Universidades de memorias de solicitud de títulos oficiales del ámbito de la Ingeniería Técnica Informática (BOE Num. 187 del 4/8/2009), y las propuestas por la ACM [11], y que son: Ciencias de la Computación [15], Ingeniería del Software [16], Ingeniería de Computadores [17], Sistemas de Información [18] y Tecnologías de la Información [19].

Actualmente, muchas instituciones e investigadores están trabajando para unificar y complementar el grado de ingeniería informática, tomando como base el modelo USA [20] o el modelo Europeo [21]. Algunas investigaciones han considerado que el problema no estaba tanto en el contenido de los dominios como en el mecanismo de aprendizaje, centrándose en buscar metodologías de enseñanza ágiles [22] que permitan la transferencia de conocimiento útil a los alumnos para su incorporación en el mundo laboral.

Es decir, se considera crítico en esta nueva etapa de las universidades conseguir hacer más prácticas las ingenierías, y hacer que los conocimientos aportados sean útiles para los alumnos y los acerquen a sus futuros puestos de trabajo.

III. Grado de Ingeniería Informática en la UCLM

En el caso de la UCLM (Universidad de Castilla-la Mancha), la nueva propuesta del plan de estudios (ver Figura 1) está dividida en un conjunto de bloques orientados a la obtención de un título que, por una parte, se centrará en aspectos generalistas, haciendo que el estudiante adquiera al menos las competencias transversales de formación básica comunes a la rama de informática y, por otra parte, las competencias de al menos una de las especializaciones recomendadas por la ACM (de las 4 ofertadas en la UCLM).

ECTS	Estructura del Título				Mod
12	Trabajo fin de grado				
24	Optatividad				
48	Ing. Del Software	Tecnologías de la Información	Ing. De Computadores	Computación	
36	Formación complementaria para la rama de Ingeniería Informática				3
60	Formación común para la rama de Ingeniería Informática				2
60	Formación básica para la Ingeniería				1

Figura 1. Estructura del Título de Ingeniero en Informática de la UCLM

Desde el punto de vista metodológico, el diseño del Plan de Estudios se basó en un análisis descendente, partiendo de las competencias hasta llegar a las asignaturas. Las unidades de enseñanza-aprendizaje se agruparon temáticamente por materias y cada materia se dividió en una o varias asignaturas afines desde un punto de vista temático.

La investigación realizada se centró principalmente en la intensificación de Ingeniería del Software propuesta para el nuevo grado en ingeniería informática, que está basada en la "Guía para la creación del Cuerpo de Ingeniería de Software para el Conocimiento" (SWEBOK)" [23-26], donde se definen las competencias y conocimientos que, según el IEEE, un Ingeniero del Software debería haber obtenido al finalizar los estudios (ej.: proyectos de Ingeniería del Software, Seguridad y Auditoría, cubriendo todos los aspectos del ciclo de vida relacionados con ellos...). El principal problema detectado en estas competencias es que son complejas y difusas a la hora de poder aplicarlas, tanto para los alumnos como para las empresas [27, 28], y tampoco permiten responder a preguntas como: ¿Los conocimientos asociados con estas competencias han sido realmente obtenidos por el alumno? ¿En qué medida han sido obtenidos? ¿Son las competencias obtenidas las que necesitan realmente las empresas?

Y es en este proceso de cambio, definición e implantación de los nuevos planes de estudio donde está el punto crítico para el futuro de algunos estudios tan nuevos, tan cambiantes y de los que depende tanto el progreso de la sociedad como es el caso de la Ingeniería Informática [29]. Por lo tanto, es muy importante ser capaces de adaptar los nuevos planes de estudio a las necesidades reales del mercado [30, 31], siendo capaces de implantarlos de una forma correcta que permita alinearlos con las competencias a las que se orientan y a las necesidades de las empresas. En el caso de la Ingeniería Informática, las empresas y los profesionales están demandando perfiles cada vez más especializados [32], por lo que es muy importante que los nuevos estudios estén muy enfocados a poder obtener una

serie de competencias objetivas y medibles, y que éstas estén alineadas con las necesidades profesionales [33], sin perder el rigor científico exigible en una ingeniería.

Para conseguir este objetivo es fundamental que la implantación de estos nuevos planes de estudio tenga una orientación que facilite su alineamiento con las necesidades reales de las empresas. Es crítico que exista una comunicación continua entre la Universidad y la Empresa, y que la primera sea capaz de desarrollar proyectos y herramientas en conjunción con la segunda que puedan ser aplicadas en las asignaturas de la carrera con el objetivo de facilitar la posterior incorporación de los alumnos al mundo laboral, ya que esto puede suponer una importante ventaja competitiva para ellos, ayudándoles a decidir el mejor puesto de trabajo que pueden ocupar en el futuro.

No debemos olvidar que estas técnicas y herramientas que permiten al alumno tomar una mejor orientación laboral al finalizar sus estudios se traducen en una mejora de la productividad de la empresa al poder contratar a los alumnos más adecuados para las competencias buscadas, lo que se traduce a su vez en mejoras salariales que pueden superar el 10% [34].

IV. Asignatura de Seguridad de Sistemas Software

Dentro de la intensificación o mención de Ingeniería del Software, analizada en el apartado anterior, existe una asignatura, que es el caso que estudiamos, denominada Seguridad de Sistemas Software de 6 créditos ECTS cuya descripción detallada se explica a continuación.

A. Contenido

El contenido (o descriptores) que se ha definido para esta asignatura y que ha dado lugar a la división por temas es el siguiente:

- Fundamentos de seguridad.
- Seguridad organizativa.
- Requisitos de seguridad.
- Seguridad en desarrollo de software.
- Seguridad de sistemas de información.
- Riesgos de seguridad.
- Servicios de seguridad.
- Gestión de seguridad.
- Certificación, normas y estándares para la seguridad.

B. Competencias

Las competencias propias de la asignatura que se han definido son las siguientes:

- Capacidad de análisis, síntesis y evaluación.
- Capacidad de organización y planificación.
- Capacidad de gestión de la información.
- Capacidad de resolución de problemas aplicando técnicas de ingeniería.
- Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.
- Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
- Capacidad de trabajo en equipo.
- Capacidad de trabajo en equipo interdisciplinar.
- Capacidad de relación interpersonal.
- Reconocimiento a la diversidad, la igualdad y la multiculturalidad.
- Razonamiento crítico.
- Aprendizaje autónomo.
- Adaptación a nuevas situaciones.
- Creatividad.
- Capacidad de liderazgo.
- Capacidad de iniciativa y espíritu emprendedor.
- Tener motivación por la calidad.

C. Objetivos que se persiguen

Los objetivos que se persiguen en esta asignatura se centran en que el alumno sea capaz de:

- Identificar, modelar e integrar los requisitos de seguridad del software en el proceso de su desarrollo.
- Conocer las principales técnicas y servicios de seguridad del software.
- Conocer las normas, estándares y legislación más relevante sobre seguridad del software.

D. Práctica relacionada con eMARISMA

La práctica que se ha planteado a los alumnos coincidiendo con el tema de Gestión de seguridad y Riesgos, así como con la correspondencia directa con la competencia de la capacidad de identificar, evaluar y gestionar los riesgos potenciales, y otras muchas de forma indirecta, consiste en realizar un análisis de riesgos de un sistema de información utilizando los servicios y funciones que nos ofrece eMARISMA. Los detalles de la práctica se explican más adelante.

La práctica está acorde a las competencias y contenidos de la asignatura y, además, el uso de una herramienta real les acercará más al mundo empresarial y facilitará la labor del docente a la hora de explicar y analizar los contenidos de la asignatura y los resultados obtenidos por los alumnos.

E. Alumnos

En el curso 2016-2017 se ha contado con 21 alumnos matriculados en la asignatura de Seguridad de Sistemas Software. La mayoría de estos alumnos estaba también matriculado del resto de asignaturas de la intensificación de Ingeniería del Software, lo que hizo más fácil disponer de la especificación y definición de un proyecto a corto plazo para un sistema de información realizado en otra asignatura denominada Gestión de Proyectos Software (GPS). A los pocos alumnos que no estaban matriculados en GPS se les asignó a un grupo que tenían dicho proyecto para que pudieran trabajar juntos.

V. MARISMA

Fruto de 15 años de investigación realizada entre GSyA y Sicaman dentro del campo de la Gestión de la Seguridad nació la metodología MARISMA, con el objetivo de solucionar los problemas detectados en el análisis y gestión del riesgo y en los Sistemas de Gestión de Seguridad de la Información de las PYMES. La idea era desarrollar un mecanismo de análisis de riesgos basado en patrones reutilizables, de bajo coste y dinámicos.

MARISMA acomete todos los aspectos relacionados con la gestión de la seguridad y el análisis de riesgos [6, 7], y se crea bajo la premisa de que cualquier sistemas de Análisis de Riesgos valido para las PYMES también será extrapolable a grandes compañías.

Esta metodología asocia el análisis y la gestión del riesgo a los controles necesarios para la gestión de la seguridad y consta de tres procesos muy importantes:

- *Proceso 1 – Generación de Esquemas para el Análisis de Riesgos (GEAR):* Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgos y los controles necesarios para gestionar la seguridad. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada esquema para ser reutilizado con posterioridad, reduciendo los costes de generación de este proceso [35].
- *Proceso 2 – Generación del Análisis y Gestión del Riesgo (GAGR):* Mediante la selección del esquema más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo).
- *Proceso 3 – Mantenimiento Dinámico del Análisis de Riesgos (MDAR):* Mediante la utilización de las matrices generadas, las cuáles interconectan los diferentes artefactos, el sistema irá recalculando el análisis de riesgos según se produzcan incidentes de seguridad, fallen las métricas definidas o los auditores detecten "no conformidades" en los controles.

En la Figura 2 se pueden ver de forma resumida los tres procesos que componen la metodología MARISMA, y cómo intercambian información entre ellos. La información generada en el proceso GEAR será utilizada por los otros dos procesos. De igual forma, la información generada en el proceso GAGR será necesaria para el proceso MDAR. Esto no implica que siempre se deban ejecutar los tres procesos para obtener un resultado, sino que debe existir un Esquema generado previamente por el proceso GEAR para que se pueda ejecutar el GAGR.

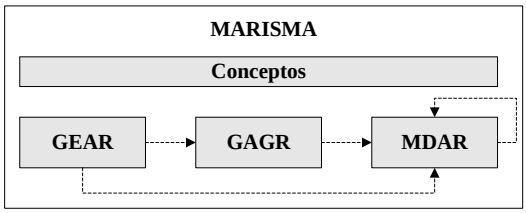


Figura 2. Esquema de procesos de MARISMA

Este apartado se divide a su vez en dos sub-apartados. En el primero de ellos exponemos una definiciones que permitirán entender la metodología (sólo se exponen las definiciones que están dentro del alcance de la práctica), y en el segundo nos centramos en la herramienta eMARISMA que da soporte a la metodología, y que es la que ha sido utilizada por los alumnos para realizar la práctica.

A. *Definiciones previas.*

A continuación, se describen los principales conceptos, que intervienen en la metodología:

- *Patrón:* Estructura formada por los principales elementos de un SGSI y las relaciones entre ellos, que puede ser reutilizado por un conjunto de compañías con características comunes (mismo sector y tamaño) a partir del conocimiento adquirido con la implantación de la metodología MARISMA y posteriores refinamientos [36].
- *Análisis de riesgos:* Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización [37]. La metodología MARISMA incluye un sencillo método para estimar el riesgo a partir de un conjunto básico de activos.
- *Activo:* Recursos del sistema de información, o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- *Activo de grano grueso:* La metodología MARISMA funciona bajo activos de grano grueso, que son aquellos que agrupan activos que están sometidos a las mismas amenazas, mismos criterios de riesgo, mismas vulnerabilidades y mismo valor estratégico. Dado que, por lo tanto, activarían los mismos riesgos y controles se tratan de forma unificada dentro del análisis de riesgos.
- *Activo de grano fino:* Son los activos de valor para la compañía al nivel más bajo de agregación.
- *Controles:* Mecanismos que nos permiten proteger los activos de las amenazas que intentan aprovechar las vulnerabilidades en estos para producir un impacto sobre algún criterio de riesgo de nuestros activos de valor.
- *Sub-controles:* Divisiones a mayor detalle de los controles. En ocasiones los controles son demasiado difusos, o intentan abordar demasiada información para permitir que el usuario dé una respuesta coherente sobre el nivel de cumplimiento (Si/Parcialmente/No).

- *Amenaza:* Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- *Vulnerabilidad:* Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema que presenta la citada debilidad. En el caso de MARISMA, las vulnerabilidades se calculan como la ausencia o debilidad de un control en la lista de controles base, que en el esquema seleccionado para la investigación está basada en controles y sub-controles derivados de la ISO27001:2013.
- *Criterios de riesgo:* Criterios que permiten estimar el grado de exposición a que una amenaza se materialice sobre uno o más dimensiones valorables de los activos causando daños o perjuicios a la organización.
- *Matriz Amenazas x Tipos de Activos:* Es una matriz que nos permite relacionar qué amenazas afectan a las diferentes familias de activos.
- *Matriz Amenazas x Controles:* Es una matriz que permite relacionar qué controles permiten proteger a los activos frente a cada amenaza. Dado que no se ha encontrado ninguna normativa que tuviera esta matriz, se ha tenido que extraer en base a la experiencia (Know-How) de los consultores involucrados en el proceso, aplicando la metodología científica Investigación en Acción.

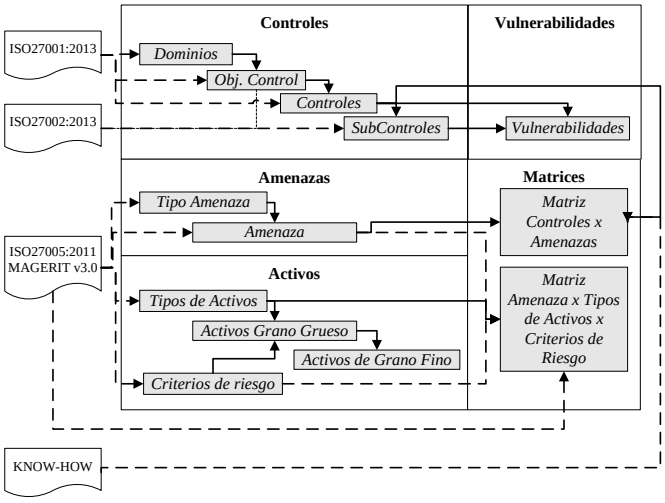


Figura 3. Elementos que componen el sistema base y sus relaciones.

En el esquema de la Figura 3 se puede ver cómo todos elementos se interrelacionan unos con otros y el origen que se ha utilizado para generar el esquema base que se está utilizando actualmente, y que básicamente parte de cuatro fuentes (ISO27001:2013, ISO27002:2013, ISO27005:2011, MAGERIT v3.0) y la Experiencia adquirida mediante la técnica de Investigación en Acción.

B. *eMARISMA.*

Con el objetivo de dar soporte a la metodología creada, el equipo formado por Sicaman-GSyA creó la herramienta eMARISMA (www.eMarisma.com).

El objetivo de este sub-apartado es explicar a grandes rasgos el funcionamiento de la misma, centrándonos sólo en aquellas parte que están dentro del alcance de la práctica, la cuál se centró sólo en el proceso GAGR, quedando por lo tanto fuera del alcance de la misma los otros dos procesos (GEAR y MDAR).

Para la realización de la práctica, a los alumnos se les facilitó acceso a la herramienta, desarrollada en modelo SaaS, de forma que no suponga ningún problema de acceso para alumnos y profesores, y que además estos puedan realizar proyectos internacionales de cooperación. En la Figura 4 se puede ver la zona en la que el profesor (que en este caso toma la figura del consultor) crea los diferentes proyectos de los alumnos.

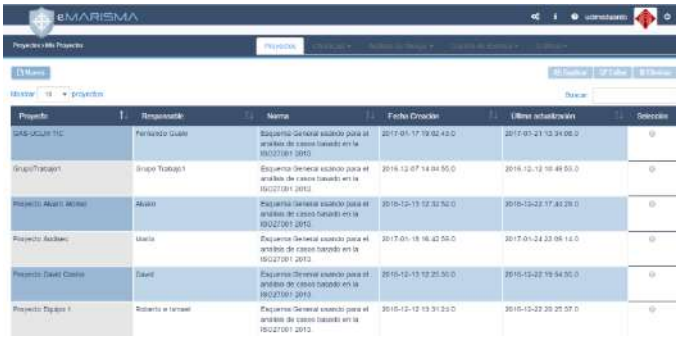


Figura 4. Proyectos creados por el profesor (consultor).

Para la creación de estos proyectos, el profesor previamente ha seleccionado el patrón que desea utilizar. En la Figura 5 podemos ver un patrón de MARISMA . En este caso concreto, el profesor ha seleccionado un patrón para análisis de riesgos basado en ISO27001:2013 y Magerit v3.0

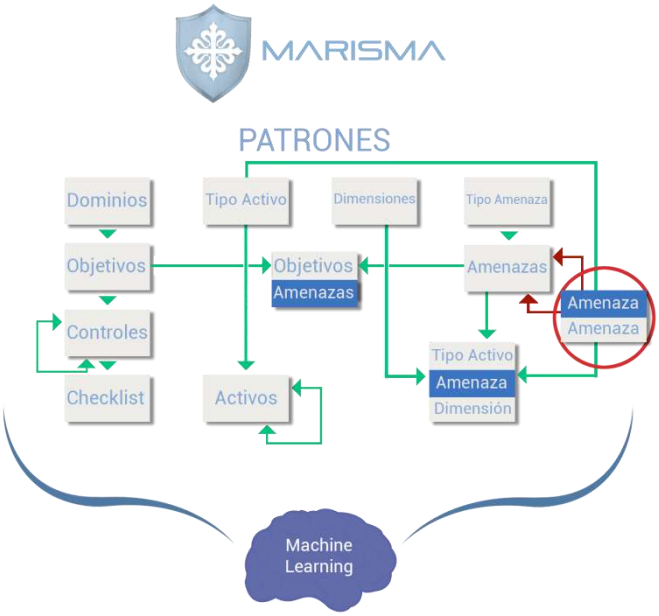


Figura 5. Visión de un patrón en eMARISMA.

Una vez que los alumnos tienen sus diferentes proyectos creados, pueden acceder a los mismos como si fueran los clientes y acometer sus análisis de riesgos. Para ello irán realizando los diferentes pasos que describimos a continuación:

- Paso 1º.- Creación de activos de grano grueso dentro del alcance de la auditoría (ver Figura 6).

Figura 6. Activos de Grano Grueso.

- Paso 2º.- Realización del Checklist para determinar el nivel de cumplimiento de controles (ver Figura 7).

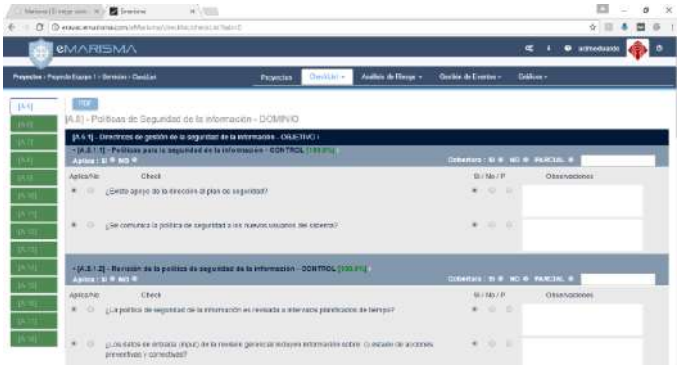


Figura 7. Checklist de nivel de cumplimiento de controles.

- Paso 3º.- Definición de las amenazas, determinando la probabilidad de ocurrencia de las mismas y el impacto en caso de que ocurra (ver Figura 8).

Figura 8. Listado de amenazas y características de las mismas.

- Paso 4º.- Generación de matriz de Activos x Amenazas: El sistema genera de forma automática dicha matriz (ver Figura 9).

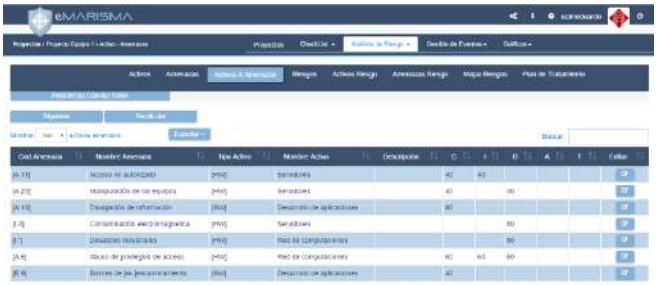


Figura 9. Matriz Activos x Amenazas.

- Paso 5º.- Generación del Análisis de Riesgos: Gracias al nivel de automatización de la herramienta al utilizar patrones, se puede generar de forma muy rápida un análisis de riesgos (ver Figura 10).

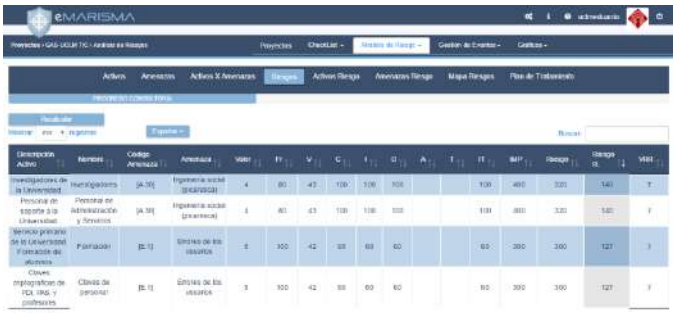


Figura 10. Generación Análisis de Riesgos.

- Paso 6º.- Generación del Plan de Tratamiento de Riesgos: Se genera de forma automática mediante un algoritmo recursivo de mejora continua (ver Figura 11).

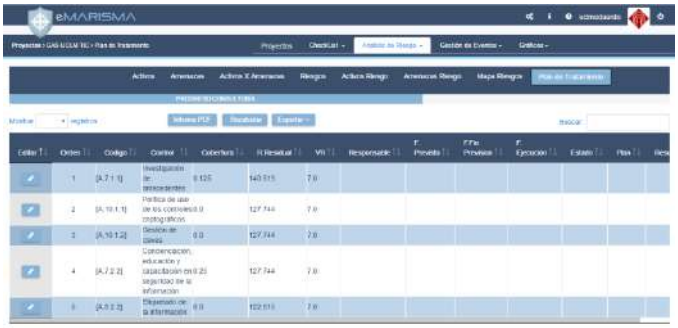


Figura 11. Plan de Tratamiento de Riesgos.

Por otro lado, en todo momento la herramienta permitirá al alumno tener una visualización grafica del estado de la compañía, mediante diagramas de Kiviat, mapas de riesgos, cuadros de mandos de controles, etc.

A continuación mostramos algunas de las opciones visuales de la herramienta:

- Cuadro de mandos para el seguimiento del nivel de cumplimiento de los controles (ver Figura 12).

Figura 12. Cuadro de Mandos de cumplimiento de Controles.

- Diagramas de Kiviat para el seguimiento del nivel de cumplimiento de los controles (ver Figura 13).

Figura 13. Diagrama de Kiviat de cumplimiento de Controles.

- Diagramas de Activos de granos grueso (ver Figura 14).

Figura 14. Diagrama de Activos.

- Gráfico de amenazas definidas (ver Figura 15).

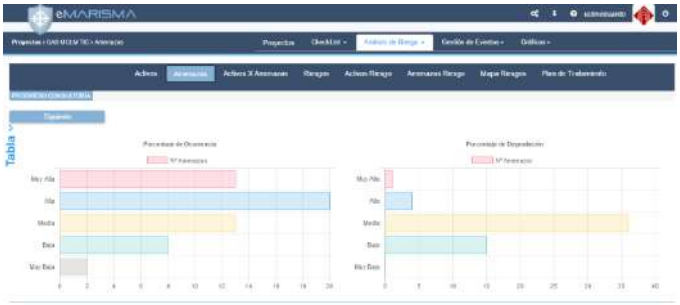


Figura 15. Gráfico de Amenazas.

- Mapa de Riesgos globales (ver Figura 16).

Figura 16. Mapa de Riesgos.

La herramienta tiene otras muchas opciones, pero se han dejado fuera al no estar contenidas dentro del alcance de la práctica definida para los alumnos.

VI. PRÁCTICA PLANTEADA A LOS ALUMNOS

La práctica que se planteó a los alumnos en la asignatura de Seguridad de Sistemas Software consistía en realizar un análisis de riesgos valorando los activos, identificando amenazas, definiendo la probabilidad y calculando el riesgo. Para la realización de la práctica se facilitó el uso de la herramienta eMARISMA para que los alumnos pudieran hacer todas las tareas planteadas, que fueron adaptadas a la herramienta para que pudieran obtener los resultados esperados de forma automática. Dichas tareas consistían en:

- Completar el Checklist de la compañía y generar un informe. (Servirá para guiar y recordar los puntos que deben ser inspeccionados en función de los conocimientos que se tienen sobre las características y riesgos).
- Identificar los Activos.
- Identificar las Amenazas con el porcentaje de probabilidad y degradación.
- Definir Activos por Amenazas teniendo en cuenta las dimensiones de seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
- Realizar el análisis de riesgos (“Matriz de riesgos”) y el plan de tratamiento.
- Generar los informes.
- Analizar los resultados gráficos obtenidos.
- Definir las conclusiones a partir de los resultados.

La asignatura tenía 21 alumnos matriculados en el curso 2016-2017, como se ha dicho anteriormente. Los alumnos se dividieron en equipos de entre 2 a 4 miembros, y cada equipo tenía un proyecto diferente que había definido y especificado en la asignatura GPS de la intensificación. Con ese proyecto pedimos a cada equipo que, por parejas o individualmente, realizaran el análisis de riesgos de su propio proyecto. De esta forma podemos obtener, en la mayoría de proyectos, más de un análisis de riesgos por proyecto para luego comparar los resultados obtenidos.

Por tanto, tenemos 7 proyectos diferentes, y para cada uno de ellos al menos un análisis de riesgos realizado con eMarisma. En la Tabla I podemos ver los proyectos

disponibles, los miembros por cada uno de ellos y el número de análisis que se hicieron para cada proyecto.

Tabla I. Proyectos de la práctica.

Proyecto	Análisis	Miembros	Total análisis
Proyecto A	Análisis 1	2	2
	Análisis 2	2	
Proyecto B	Análisis 1	2	3
	Análisis 2	2	
	Análisis 3	2	
Proyecto C	Análisis 1	1	3
	Análisis 2	2	
	Análisis 3	2	
Proyecto D	Análisis 1	2	2
	Análisis 2	2	
Proyecto E	Análisis 1	2	1

Los proyectos que nos interesan para su estudio son aquellos que han obtenido al menos dos análisis, ya que el objetivo de este artículo es analizar las diferencias o puntos en común que se pueden obtener al realizar un análisis de riesgos para un mismo proyecto hecho por diferentes equipos de personas. Como se puede ver en la Tabla I, los proyectos que vamos a estudiar son los proyectos A, B, C y D.

A continuación, vamos a describir brevemente en qué consisten los proyectos para que se puedan ver y entender los resultados generados en cada uno de ellos. Por ejemplo, los activos identificados, riesgos, amenazas, etc.

A. Proyecto A

Desarrollo de apps compatibles con los próximos dispositivos que salgan al mercado con una nueva versión de sistema operativo, tanto por parte de nuestra empresa como para los propios usuarios, bajo un determinado control de requisitos, que garantice la sincronización de dispositivos de forma sencilla. Por tanto, se facilita a los clientes o usuarios que desarrollen sus propias aplicaciones y puedan entrar a formar parte de la línea de desarrollo de la empresa si pasa los criterios y requisitos de calidad establecidos.

B. Proyecto B

Página web para mostrar vehículos y explicar todas sus ventajas. Además, la web contará con un configurador de vehículos donde se podrán seleccionar todos nuestros productos y configurarlos a su gusto, al igual que dar la oportunidad de generar un presupuesto online que llegará directamente a nuestro departamento. La web será amigable y muy usable para los usuarios. Además será adaptable a todo tipo de dispositivos. También tiene la opción de reserva de vehículos.

C. Proyecto C

Desarrollo de la web de una empresa para promocionar y vender productos de domótica, así como el diseño y desarrollo de una aplicación móvil para la utilización de una lavadora de acuerdo al paradigma IoT. También engloba la construcción del hardware y software necesario a incluir en la propia lavadora y que sea capaz de conectarse a la aplicación móvil.

D. Proyecto D

Integración de los videos de las distintas cámaras de una planta de fabricación de vino para crear un video promocional. Se instalaron cámaras para grabar a los trabajadores realizando sus tareas y se hicieron entrevistas personales. Para la elaboración de los videos se desarrollaron una serie de aplicaciones permitían editar y montar los videos. La publicación de los videos se ha hecho a través de las redes sociales y la página web, donde además se permite la venta de vinos.

VII. RESULTADOS DE LA INVESTIGACIÓN

El objetivo de este apartado es analizar los resultados obtenidos por cada alumno de los casos planteados y extraer algunas conclusiones que permitan mejorar la práctica para el siguiente año.

Los resultados se han analizado por cada equipo y en cuatro dimensiones de valoración:

- Activos identificados.
- Valoración de los controles.
- Valoración de las amenazas.
- Riesgos obtenidos.

El Equipo 4, perteneciente al proyecto C, se descarta finalmente porque no realiza la práctica, por lo que finalmente el proyecto C queda con dos sujetos de prueba.

A. Activos Identificados

Uno de los primeros pasos que un Consultor o un cliente debe realizar a la hora de valorar los riesgos es conocer cuáles son sus activos de valor asociados al Sistema de Información (activos InfSys).

Ante este trabajo surge la duda de si diferentes consultores ven de la misma forma los activos, y esta es la primera cuestión que pretendemos analizar con los resultados de la práctica: ¿Ante el mismo caso práctico los alumnos han identificado los mismos activos de información?

- Proyecto A (ver Figura 17): El Equipo 1 ha identificado 8 activos, mientras que el Equipo 9 ha identificado 7 activos.

Figura 17. Resultados Activos – Proyecto A (Equipos 1 y 9).

- Proyecto B (ver Figura 18): El Equipo 2 ha identificado 7 activos, mientras que el Equipo 7 ha

identificado 9 activos y el Equipo 8 ha identificado 4 activos.

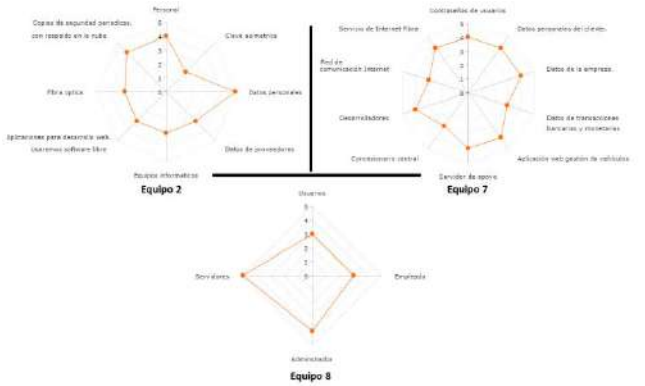


Figura 18. Resultados Activos – Proyecto B (Equipos 2, 7 y 8).

- Proyecto C (ver Figura 19): El Equipo 3 ha identificado 7 activos mientras el Equipo 10 ha identificado 7 activos. Existe una concordancia del 100% entre los activos identificados por ambos equipos de trabajo.

Figura 19. Resultados Activos – Proyecto C (Equipos 3 y 10).

- Proyecto D (ver Figura 20): El Equipo 5 ha identificado 11 activos y el Equipo 6 ha identificado 8 activos.

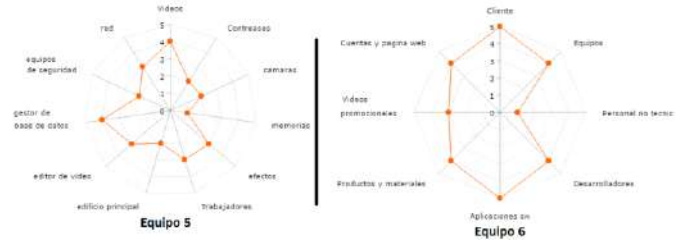


Figura 20. Resultados Activos – Proyecto D (Equipos 5 y 6).

Como conclusión de este primer análisis podemos ver cómo tan sólo en uno de los cuatro proyectos los alumnos han coincidido a la hora de identificar los activos.

Este es un resultado de valor y que coincide con una percepción de la empresa Sicaman, que detectó previamente que diferentes consultores sobre los mismos casos identificaban activos diferentes. Por lo tanto, nos encontramos ante un problema que tienen los análisis de riesgos en la actualidad en el mundo real y que hemos replicado en la universidad, con lo que nos encontramos que la aplicación de estos casos por parte de los alumnos nos puede ayudar a ir aplicando técnicas que permitan reducir el grado de error a la hora de identificar los activos de información de una compañía, que es algo de gran valor en el sector empresarial.

También de la comparación de los resultados se puede extraer que no sólo los activos identificados son diferentes, sino que también lo son las tipologías de los mismos.

Finalmente, desde el grupo de investigación GSyA se analizará si parte del error puede consistir en la necesidad de que los casos prácticos definidos deban acotarse mejor, con lo que encontramos otra ventaja del uso de la herramienta y es que permite identificar casos prácticos cuya descripción puede ser confusa para los alumnos.

B. Valoración de los Controles

En este apartado analizaremos los resultados obtenidos por los alumnos a partir de la entrevista realizada con el profesor sobre cada caso de estudio.

- Proyecto A (ver Figura 21): Los niveles de cumplimiento de los controles obtenidos por los dos equipos son totalmente diferentes para el mismo caso.

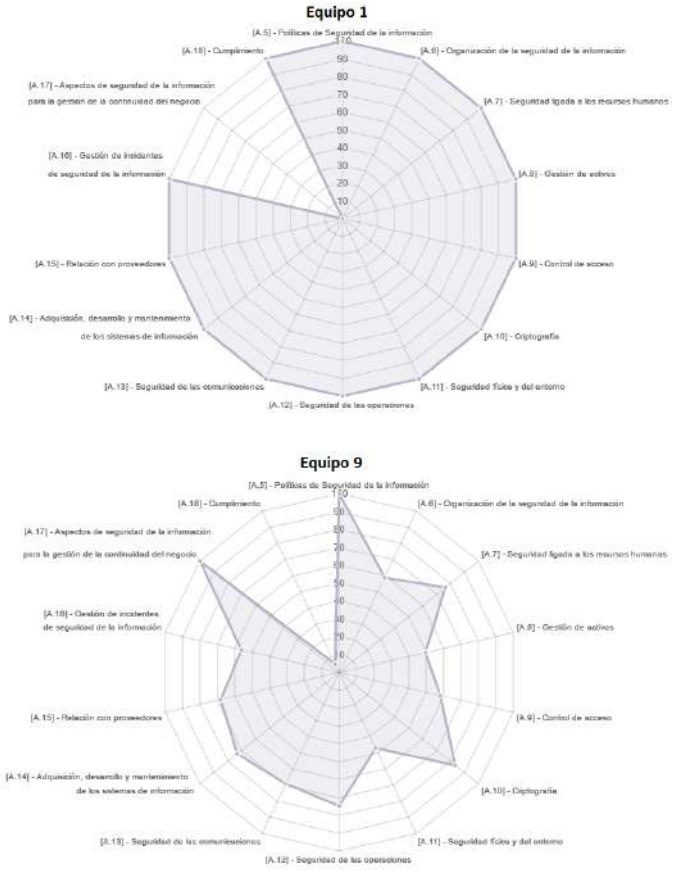


Figura 21. Resultados Controles – Proyecto A (Equipos 1 y 9).

- Proyecto B (ver Figura 22): Los niveles de cumplimiento de los controles obtenidos por los dos equipos son totalmente diferentes para el mismo caso.

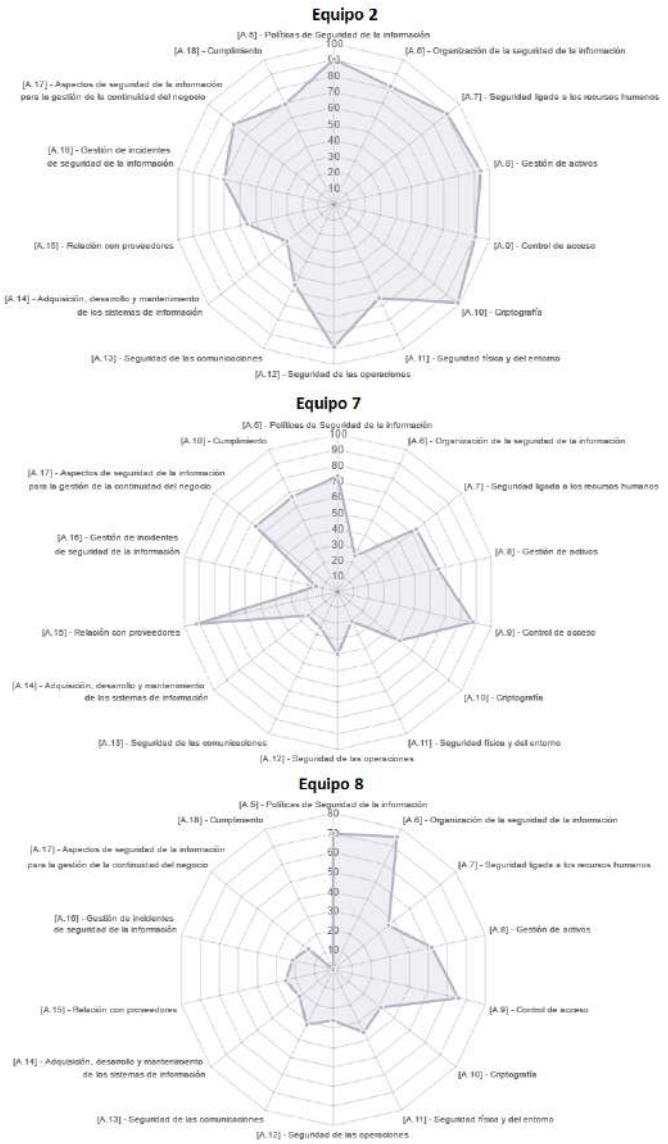


Figura 22. Resultados Controles – Proyecto B (Equipos 2, 7 y 8).

- Proyecto C (ver Figura 23): Los niveles de cumplimiento de los controles obtenidos por los dos equipos son diferentes para el mismo caso, aunque se aproximan en más del 50%.
- Proyecto D (ver Figura 24): Los niveles de cumplimiento de los controles obtenidos por los dos equipos son totalmente diferentes para el mismo caso.

Como vemos, a partir del análisis de los resultados podemos obtener algunas conclusiones claras:

- El proyecto C ha sido el que más similitudes ha obtenido.
- El resto de proyectos han obtenido resultados completamente diferentes de la entrevista.

Este resultado también coincide con otra de las problemáticas identificadas en las empresas clientes de Sicaman, y es que los resultados del nivel de cobertura de los controles son diferentes dependiendo de la percepción del entrevistador. Además cuando las entrevistas no son detalladas y se realizan de forma rápida como ha sido el caso de la práctica, el entrevistador toma muchas decisiones que pueden alterar los resultados.

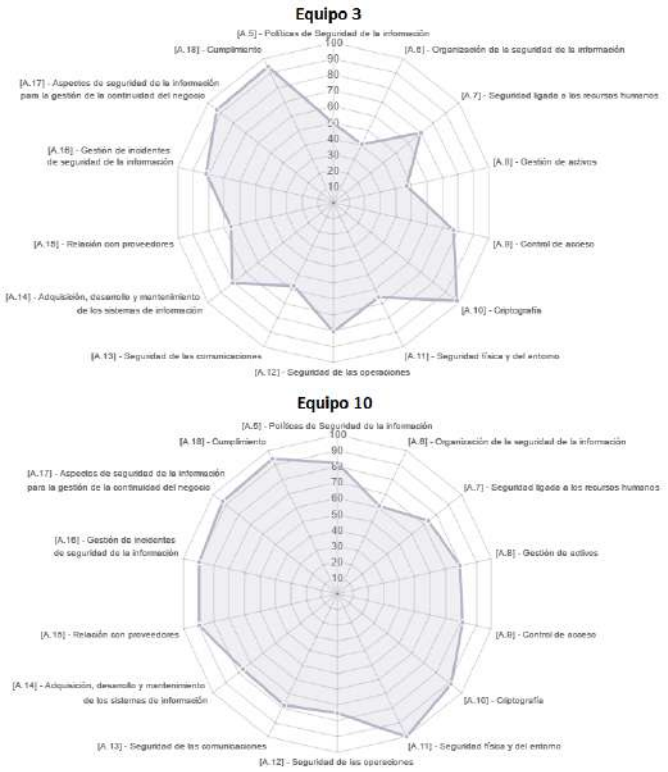


Figura 23. Resultados Controles – Proyecto C (Equipos 3 y 10).

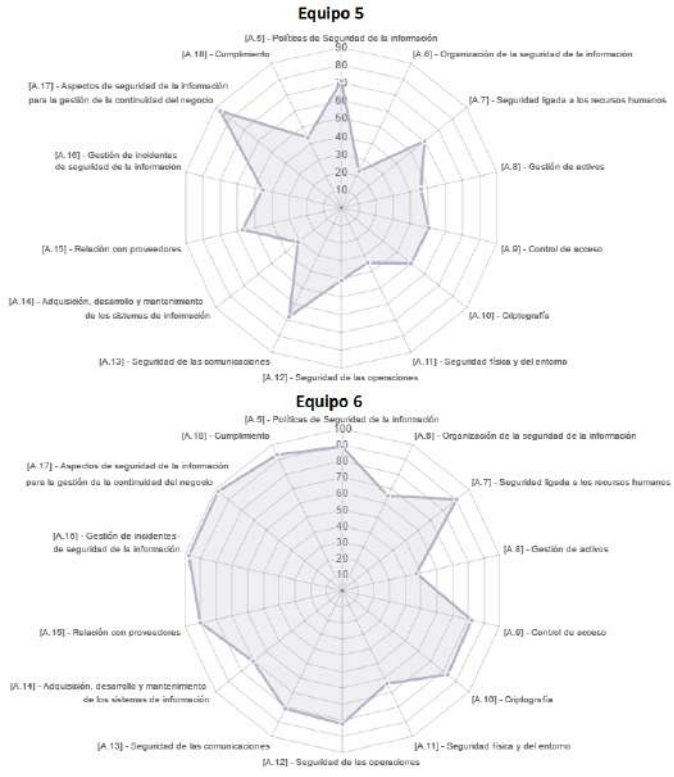


Figura 24. Resultados Controles – Proyecto D (Equipos 5 y 6).

De cara al año siguiente sería interesante analizar cómo reducir ese grado de incertidumbre, haciendo que la entrevista

sea mucho más detallada o incluso partiendo de proyectos con mucho más detalle respecto al nivel de cumplimiento de los controles.

C. Valoración de las Amenazas

En este apartado analizaremos cómo han valorado los alumnos las propiedades de "Probabilidad de Ocurrencia" y "Probabilidad de Degradación" frente a una lista de amenazas dadas.

- Proyecto A (ver Figura 25): La percepción de los dos equipos del "Porcentaje de Ocurrencia" y del "Porcentaje de Degradación" es totalmente diferente para el mismo caso.

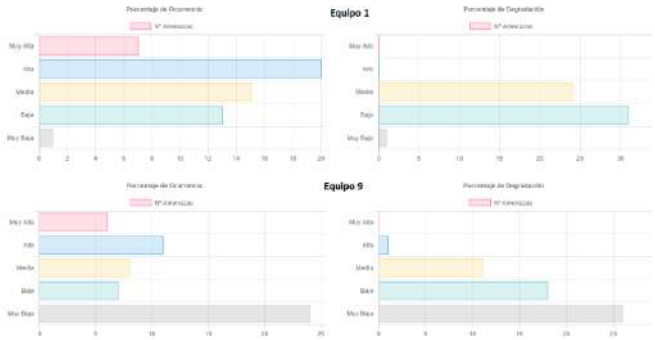


Figura 25. Resultados Amenazas – Proyecto A (Equipos 1 y 9).

- Proyecto B (ver Figura 26): La percepción de los dos equipos del "Porcentaje de Ocurrencia" y del "Porcentaje de Degradación" es totalmente diferente para el mismo caso.

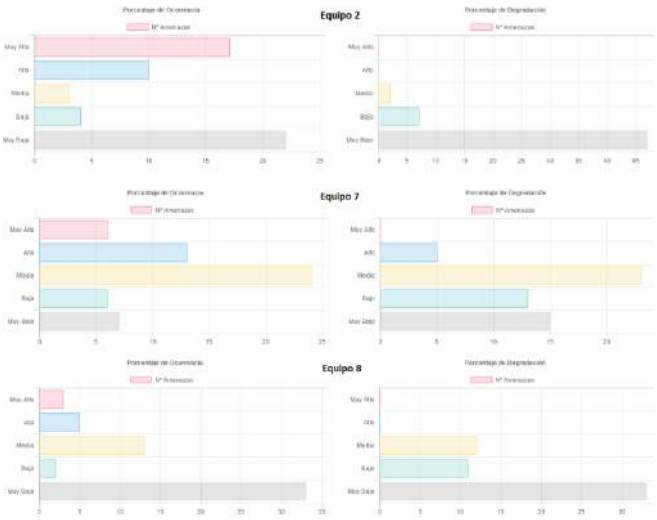


Figura 26. Resultados Amenazas – Proyecto B (Equipos 2, 7 y 8).

- Proyecto C (ver Figura 27): La percepción de los dos equipos del "Porcentaje de Ocurrencia" y del "Porcentaje de Degradación" es muy parecida, con una proximidad del 75%.

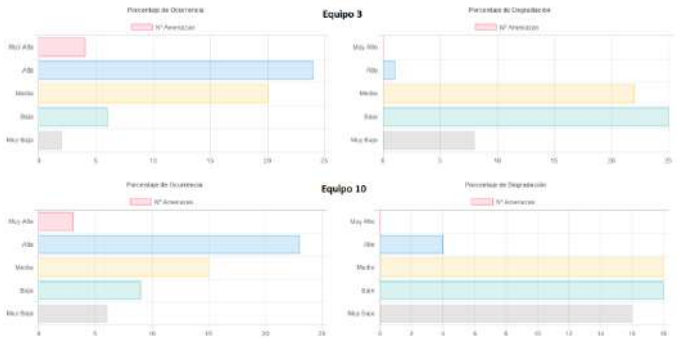


Figura 27. Resultados Amenazas – Proyecto C (Equipos 3 y 10).

- Proyecto D (ver Figura 28): La percepción de los dos equipos del "Porcentaje de Ocurrencia" y del "Porcentaje de Degradación" es totalmente diferente para el mismo caso.

Figura 28. Resultados Amenazas – Proyecto D (Equipos 5 y 6).

Como podemos ver, y al igual que en los dos casos anteriores, el Proyecto C ha sido el que ha obtenido resultados más aproximados. Sin embargo, los demás equipos han tomado decisiones totalmente diferentes para el mismo caso, lo que altera el resto de resultados del análisis de riesgos.

D. Riesgos Obtenidos

En este último apartado analizaremos el mapa de riesgos que se obtiene y que depende de las decisiones tomadas en cada uno de los tres apartados anteriores.

- Proyecto A (ver Figura 29): Los niveles de riesgos finales obtenidos por los dos equipos son totalmente diferentes para el mismo caso, con niveles de riesgo mucho más elevados en el segundo caso.
- Proyecto B (ver Figura 30): Los niveles de riesgos finales obtenidos por los dos equipos son diferentes para el mismo caso. Como podemos ver, el Equipo 2 no tiene riesgos relevantes mientras que en el Equipo 7 aparecen algunos. Aun así, ambos proyectos obtienen riesgos contenidos dentro de un margen de error aceptable. El resultado obtenido para el Equipo 8 es totalmente diferente a los dos anteriores.

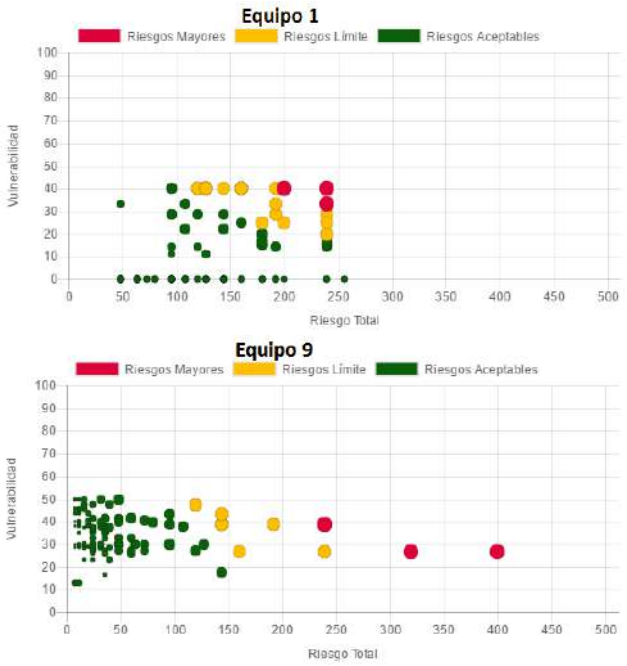


Figura 29. Resultados Mapa de Riesgos – Proyecto A (Equipos 1 y 9).

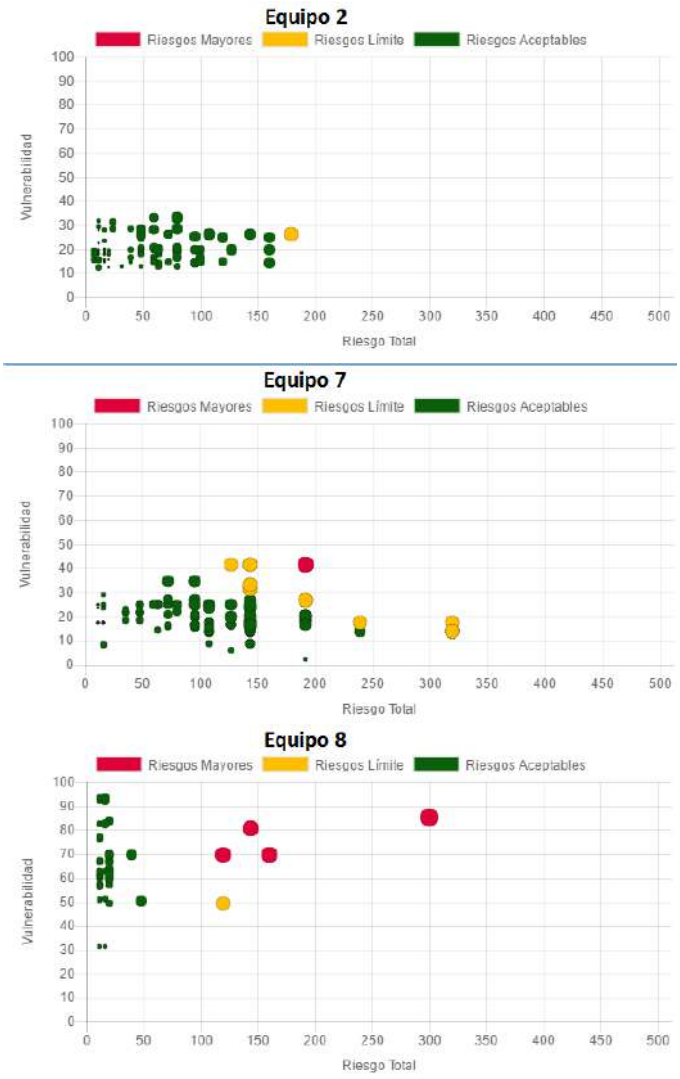


Figura 30. Resultados Mapa de Riesgos – Proyecto A (Equipos 2, 7 y 8).

- Proyecto C (ver Figura 31): Los niveles de riesgos finales obtenidos por los dos equipos son diferentes para el mismo caso, aunque se mantienen dentro de un rango aceptable de diferencia, con un riesgo total alrededor de 250 en ambos casos.

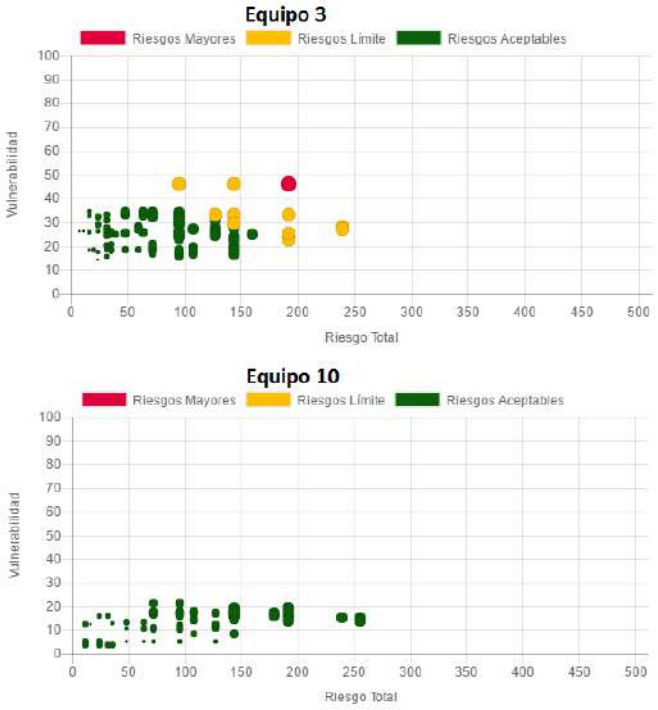


Figura 31. Resultados Mapa de Riesgos – Proyecto C (Equipos 3 y 10).

- Proyecto D (ver Figura 32): Los niveles de riesgos finales obtenidos por los dos equipos son totalmente diferentes para el mismo caso.

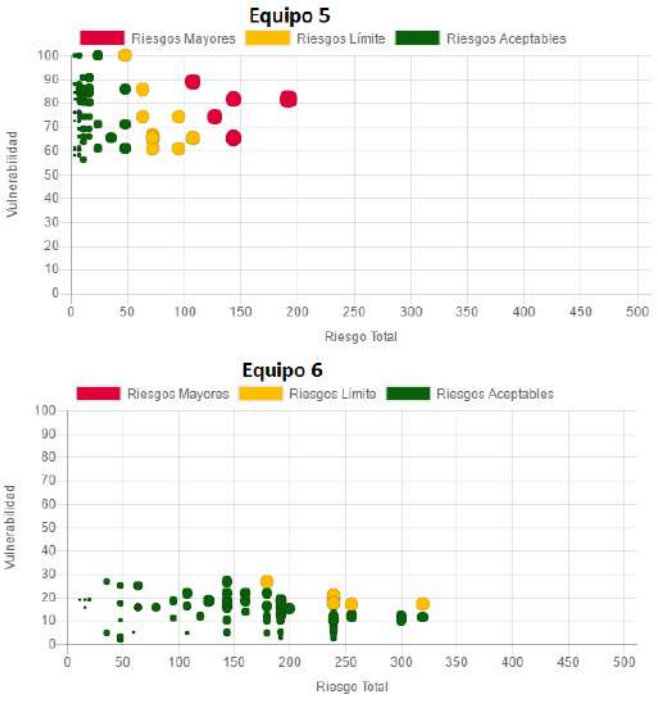


Figura 32. Resultados Mapa de Riesgos – Proyecto D (Equipos 5 y 6).

Como podemos ver, y al igual que en los casos anteriores, el Proyecto C ha sido el que ha obtenido resultados más aproximados. Sin embargo, en los demás proyectos los equipos han tomado decisiones totalmente diferentes para el mismo caso, lo que altera el resto de resultados del análisis de riesgos, dando en algunos casos mapas de riesgos totalmente diferentes (Ej: Proyecto D).

VIII. Conclusiones y trabajos futuros

La experiencia de haber abordado esta investigación ha supuesto un esfuerzo muy importante para todos los participantes, tanto del sector público (profesores y universidad) como del privado (empresas asociadas). Se debe destacar la buena disposición que todos los participantes del proyecto han mostrado en todo momento, aun cuando debían compaginar el proyecto con otras actividades cotidianas como la investigación y la docencia para la gente del sector público, y las tareas de dirección, gestión, etc., en el caso de los participantes del sector privado. Pero el esfuerzo realizado por todos ellos ha merecido la pena, ya que va a permitirles ofrecer un mejor valor.

En el caso de las empresas, ha permitido utilizar una herramienta que ha sido testada en casos reales y validar que las conclusiones y resultados obtenidos por los alumnos coincidían con los problemas que ellos también se estaban encontrando en la empresa.

En el caso de la Universidad, el uso de la herramienta ha permitido a los alumnos tener un acercamiento a casos reales y poder acceder a una herramienta que está siendo utilizada en el mundo empresarial. Además, ha supuesto el primer paso para contar con un laboratorio de investigación en el campo del análisis de riesgos de seguridad dentro de la universidad, al verificar que los resultados obtenidos por los alumnos son parecidos a los que se obtienen por las empresas consultoras, cometiendo los mismos errores que ellos y por lo tanto permitiendo que puedan ser verificadas las potenciales mejoras.

Otro de los aspectos importantes obtenidos es la capacidad de poder guardar y comparar los resultados de un año a otro, analizando cómo la práctica mejora y permitiendo ver la evolución de los alumnos.

También debemos destacar que esta tan solo ha sido una primera aproximación para utilizar el potencial de eMARISMA, y que el objetivo es ir mejorando la práctica en años posteriores para utilizar todo el potencial de la herramienta.

Uno de los objetivos perseguidos en los próximos años es que eMARISMA sea adoptado por más universidades y así aprovechar su capacidad de compartir riesgos para crear una macro-práctica entre varias universidades. Esto permitiría a los alumnos analizar cómo los riesgos de unos pueden afectar a activos asociados, creando una macro-red de riesgos asociativos y jerárquicos aprovechando la potencialidad de la herramienta a la hora de asociar y compartir activos. También permitiría aprovechar su capacidad para realizar análisis de riesgos dinámicos y multi-patrón, que son funcionalidades que han quedado fuera del alcance de la práctica actual.

AGRADECIMIENTOS

Esta investigación ha sido co-financiada por los proyectos *SEQUOIA – Security and Quality in Processes with Big Data and Analytics* (TIN2015-63502-C3-1-R) financiados por el "Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER", del proyecto ERAVAC ISO25000 (13/16/IN/4/014) financiados por la "Consejería de Economía, Empresas y Empleo" y del proyecto "Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad - Código: ESPE-2015-PIC-019" financiado por la ESPE y CEDIA (Ecuador), y ha contado con la participación de la empresa Sicaman Nuevas Tecnologías (www.sicaman-nt.com) que ha permitido validar los resultados.

Referencias

[1] Sánchez, L.E., et al. *SCMM-TOOL: Tool for computer automation of the* Information Security Management Systems. in 2nd International conference on Software and Data Technologies (ICSOFT'07). . 2007c. Barcelona-España Septiembre.

[2] Sánchez, L.E., et al. Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas. in International Conference on Security and Cryptography (SECRYPT'08). 2008. Porto–Portugal.

[3] Sánchez, L.E., et al. Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. in International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES. 2006. Viena (Austria).

[4] Sánchez, L.E., et al. MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. in 9th International Conference on Enterprise Information Systems (WOSIS'07). 2007b. Funchal, Madeira (Portugal). June.

[5] Sánchez, L.E., et al. Developing a model and a tool to manage the information security in Small and Medium Enterprises. in International Conference on Security and Cryptography (SECRYPT'07). 2007a. Barcelona. Spain.: Junio.

[6] Sánchez, L.E., et al., Managing Security and its Maturity in Small and Medium-sized Enterprises. J. UCS, 2009. 15(15): p. 3038-3058.

[7] Santos-Olmo, A., et al., A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs, in 9th International Workshop on Security in Information Systems (WOSIS12) In conjunction with 11th International Conference on Enterprise Information Systems (ICEIS12).2012: Wroclaw, Poland. p. 117 -124.

[8] Parra, A.S.O., et al., Methodology for Dynamic Analysis and Risk Management on ISO27001. IEEE Latin America Transactions, 2016. 14(6): p. 2897-2911.

[9] Pereira, C., et al. The European Computer Science Project: A Platform for Convergence of Learning and Teaching. in DLC&W 2006. 2006. Lisbon, Portugal: October 2006.

[10] Forbes, N.M., P, Computer science today in the European Union. Computing in Science & Engineering, 2002. 4(1): p. 10-14.

[11] ACM, Computer science curriculum 2008: An interim revision of CS 2001, in Review Task Force, R.f.t. Interim, Editor 2008, ACM.

[12] Sahami, M., et al., Computer science curriculum 2013: reviewing the strawman report from the ACM/IEEE-CS task force, in Proceedings of the 43rd ACM technical symposium on Computer Science Education2012, ACM: Raleigh, North Carolina, USA. p. 3-4.

[13] Milosz, M., et al., COMPARISON OF EXISTING COMPUTING CURRICULA AND THE NEW ACM-IEEE COMPUTING CURRICULA 2013. EDULEARN14 Proceedings, 2014: p. 5808-5818.

[14] Martinez, J.E.P., J. Garcia Martin, and A.S. Alonso. Teamwork competence and academic motivation in computer science

engineering studies. in Global Engineering Education Conference (EDUCON), 2014 IEEE. 2014.
[15] CC2001, Computing Curricula 2001. Computer Science, I.C.S.a.A.f.C. Machinery, Editor 2001.
[16] SE2004, Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering, I.C.S.A.f.C. Machinery, Editor 2004.
[17] CE2004, Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering, I.C.S.A.f.C. Machinery, Editor 2004.
[18] Gorgone, J., et al., MSIS 2006: Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems. Communications of AIS, 2006. 38(2): p. 121-196.
[19] Lunt, B., et al., Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, in Association for Computing Machinery (ACM), I.C. Society, Editor 2008.
[20] Pyster, A., et al., Master's Degrees in Software Engineering: An Analysis of 28 University Programs. IEEE Software, 2009: p. 95-101.
[21] Lago, P., et al. Towards a European Master Programme on Global Software Engineering. in 20th Conference on Software Engineering Education & Training (CSEET'07). 2007.
[22] Rico, D. and H. Sayani. Use of Agile Methods in Software Engineering Education. in Agile Conference, 2009. 2009. Chicago, USA.
[23] Lavrischeva, E.M. Classification of Software Engineering Disciplines. in Kibernetika i Sistemnyi Analiz. 2008.
[24] Society, I.C., P. Bourque, and R.E. Fairley, Guide to the Software Engineering Body of Knowledge (SWEBOK(R)): Version 3.02014: IEEE Computer Society Press. 346.
[25] Bourque, P. and R.E. Fairley, Guide to the software engineering body of knowledge (SWEBOK (R)): Version 3.02014: IEEE Computer Society Press.
[26] Alarifi, A., et al., SECDEP: Software engineering curricula development and evaluation process using SWEBOK. Information and Software Technology, 2016. 74: p. 114-126.
[27] Samarthyam, G., et al., FOCUS: an adaptation of a SWEBOK-based curriculum for industry requirements, in Proceedings of the 34th International Conference on Software Engineering2012, IEEE Press: Zurich, Switzerland. p. 1215-1224.
[28] Alarcón, A., N. Martinez, and J. Sandoval, Use of Learning Strategies of SWEBOK© Guide Proposed Knowledge Areas, in 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing, L. Uden, et al., Editors. 2013, Springer Berlin Heidelberg. p. 243-254.
[29] Lethbridge, T., et al. Improving software practice through education: Challenges and future trends. in Future of Software Engineering(FOSE'07). 2007.
[30] Thompson, J. Software Engineering Practice and Education An International View. in SEESE'08. 2008. Leipzig, Germany.
[31] Fairley, R.E.D., P. Bourque, and J. Keppler. The impact of SWEBOK Version 3 on software engineering education and training. in Software Engineering Education and Training (CSEE&T), 2014 IEEE 27th Conference on. 2014.
[32] García García, M.J. and L. Fernández Sanz, Opinión de los profesionales TIC acerca de la formación y las certificaciones personales, in Certificaciones profesionales en las TIC2007, mayo-junio 2007: Novática. p. 32-39.
[33] Seidman, S.B. Software Engineering Certification Schemes. in Computer, 2008. 2008.
[34] Willmer, D. Today's Most In-Demand Certifications. 2010 [cited 2010 26 July 2010].
[35] Sanchez, L.E., et al., ISMS Building for SMEs through the Reuse of Knowledge. Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications, 2013: p. 394.
[36] Sánchez, L.E., et al. Building ISMS Through Knowledge Reuse. in 7th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS'10). 2010. Bilbao, Spain.
[37] V3, M., Methodology for Information Systems Risk Analysis and Management (MAGERIT version 3), 2012, Ministerio de Administraciones Públicas (Spain).

David G. Rosado has an MSc and PhD. in Computer Science from the University of Málaga (Spain) and from the University of Castilla-La Mancha (Spain), respectively. His research activities are focused on security for Information Systems and Cloud Computing. He has published several papers in national and international conferences on these subjects, and he is co-editor of a book and chapter books. Author of several manuscripts in national and international journals (Information Software Technology, System Architecture, Network and Computer Applications, etc.). He is member of Program Committee of several conferences and workshops nationals and internationals such as ICEIS, ICCGI, CISIS, SBP, IAS, SDM, SECRYPT, COSE and international journals such as Internet Research, JNCA, KNOSYS, JKSU, and so on. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.

Luis Enrique Sánchez is PhD and MsC in Computer Science and is an Professor at the Universidad of Castilla-la Mancha (Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Ismael Caballero has an MSc and PhD in Computer Science from the Escuela Superior de Informa´tica of the Castilla-La Mancha University in Ciudad Real. He actually works as an assistant professor in the Department of Information Systems and Technologiesat the University of Castilla-La Mancha, and he has also been working in the R&D Department of Indra Sistemas since 2006. His research interests are focused on information quality management, information quality in SOA, and Global Software Development.

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in databases, datawarehouses, web services and information systems, and also in security metrics. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (DEXA, CAISE, UML, ER, etc.). Author of several manuscripts in national and international journals (Information Software Technology, Computers And Security, Information Systems Security, etc.), he is director of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain. He belongs to various professional and research associations (ATI, AEC, ISO, IFIP WG11.3 etc.).