Diseño de una e–actividad para Seguridad Informática

X. A. Vila, M. J. Lado, P. Cuesta, D. N. Olivieri
Departamento de Informática
Universidad de Vigo
Campus Universitario s/n
32004 Ourense
{anton,mrlado,pcuesta}@uvigo.es, dnolivieri@gmail.com

Resumen

En este artículo se presenta un estudio de caso, diseñado para ser utilizado en la materia Seguridad Informática o similar. Este tipo de actividad, también denominada método de caso, es un tipo de e–actividad que se caracteriza por utilizar una situación real sobre la que los alumnos trabajan y discuten para llegar a conclusiones. En este estudio concreto utilizaremos una noticia real sobre ataques de seguridad en Internet, para que los alumnos debatan sobre temas como la responsabilidad de una configuración segura, el papel de los proveedores de acceso o las consecuencias legales para los hackers. También se pedirá a los alumnos que elaboren una guía de configuración segura.

1. Introducción

Éste es el año de la adaptación real de la titulación de Ingeniería Informática, y de muchas otras titulaciones, a la normativa impuesta por el Espacio Europeo de Educación Superior (EEES). Algunas universidades dieron ya este paso en el curso 2008–09, la mayoría lo han hecho en el 2009–10, y algunas más lo han pospuesto hasta el curso 2010-11. Se trata de un paso importante en la educación superior en aspectos como el organizativo, la metodología docente, los objetivos pedagógicos, la homologación internacional, etc.

La implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en el ámbito docente ha sido escasa hasta hace pocos años. La introducción de los ordenadores en las aulas se ha producido en la última década [7], así como la habilitación de plataformas de teledocencia en diversas universidades [10].

Entre las metas buscadas con la implantación del EEES podríamos mencionar la eliminación de barreras geográficas que permitan la movilidad de profesores y alumnos, o la adecuación de la oferta docente universitaria al "aprendizaje a lo largo de toda la vida" (*long life learning*) [6]. Para conseguir estos objetivos es necesario flexibilizar la rigidez espacio–temporal de la docencia tradicional en el aula.

Hasta ahora, las plataformas de teledocencia y las herramientas que nos ofrece Internet eran utilizadas únicamente para archivar el material docente, realizar algún cuestionario o publicar las calificaciones, y esto no de modo generalizado. Ahora nos veremos obligados a aprovechar las posibilidades que la tecnología nos ofrece para diseñar nuevos tipos de actividades que permitan a los alumnos ejercitar nuevas habilidades, tales como el trabajo en grupo, la construcción colaborativa de conocimiento, o la realización de actividades síncronas con colectivos de alumnos geográficamente dispersos, o para avanzar en la personalización del aprendizaje [3].

No se trata de trasladar a dichas plataformas el mismo tipo de actividades que realizábamos hasta ahora, sino de diseñar nuevas actividades que aprovechen todas las posibilidades que nos ofrecen estos soportes; esto es, tenemos que diseñar "e–actividades".

En las dos secciones siguientes se profundiza un poco más en los conceptos de e–actividad y de método del caso, y se proporcionan las referencias necesarias para ampliar información y para que cualquiera pueda diseñar su propio estudio de caso. En la sección 4 se presenta el estudio de caso diseñado para la materia Seguridad Informática, perteneciente al Grado en Ingeniería Informática de la Universidad de Vigo. La información se presenta organizada en el mismo orden en el que se ha ido elaborando en la realidad. Esto facilitará el trabajo de aquellos que quieran diseñar su propio caso, al servirles de guía o plantilla. Finalizaremos el artículo con los apartados de conclusiones, agradecimientos y referencias.

2. E–actividades

Las "actividades educativas" son las diferentes acciones que los alumnos llevan a cabo en completa relación con los contenidos e informaciones que les han sido ofrecidos. Si estas actividades son presentadas, realizadas o transferidas a través de la red, entonces las podemos considerar e–actividades [1].

Según esta definición, cualquier actividad "presencial" puede transformarse en e–actividad simplemente haciendo uso de una plataforma de teledocencia para colgar el material o recibir los resultados. Sin embargo, de este modo no estaríamos aprovechando las nuevas funcionalidades que nos ofrecen Internet y las TIC. No se trata de duplicar actividades en la red, sino diseñar nueva actividades (e-actividades) que aprovechen todos estos recursos.

Por otra parte, el hecho de que estas actividades se desarrollen sin la presencia simultánea en tiempo y espacio de los actores (profesor y alumnos) presenta nuevos obstáculos que deben de ser tenidos en cuenta: falta de motivación, ausencia de lazos afectivos, falta de lenguaje gestual, desconocimiento del estado de ánimo del alumno, etc [8].

La variedad de e–actividades que pueden plantearse es grande. El profesor Cabero indica las siguientes posibilidades [1]:

- Proyectos de trabajo.
- Visitas a sitios Web.
- Análisis y reflexión de la información presentada.
- Realización de ejemplos presentados.
- Análisis de imágenes.
- Estudio de casos.
- Resolución de problemas.
- Lectura de documentos.

El ejemplo que describimos en este artículo pertenece a la categoría de estudio de casos o *método del caso*.

3. Método del caso

Este método pedagógico tuvo su origen aproximadamente en 1914 en la Facultad de Derecho de la Universidad de Harvard. El objetivo era que los estudiantes se enfrentasen a situaciones reales y que tuviesen que tomar decisiones y emitir juicios fundados [9]. Con el paso de los años se fue extendiendo a otros campos, y se ha convertido en una estrategia didáctica muy eficaz.

El método del caso es una técnica de aprendizaje activa, centrada en la investigación del estudiante sobre un tema real, el aprendizaje cooperativo y el diálogo democrático. Esta actividad entrena al alumno en la elaboración de soluciones válidas para los posibles problemas de carácter complejo que se presenten en la realidad futura [4]. El caso no proporciona soluciones, sino datos concretos para reflexionar, analizar y discutir en grupo las posibles salidas. Es además un recurso que fomenta la habilidad creativa y la capacidad de innovación, y representa un recurso para conectar la teoría con la práctica real.

Según [9] existen los siguientes tipos de casos:

- Casos centrados en el estudio de descripciones: los alumnos analizan, identifican y describen los puntos clave de una situación, para debatir y reflexionar con los compañeros las distintas perspectivas para abordar la situación.
- Casos de resolución de problemas: los alumnos, tras el análisis exhaustivo de la situación, valoran la decisión tomada por el protagonista del caso o justifican su propia decisión. Dentro de este grupo podemos distinguir tres subgrupos: casos centrados en el análisis crítico de tomas de decisiones descritas; casos centrados en generar propuestas de toma de decisones; y casos centrados en la simulación.

El ejemplo que presentamos en este artículo correspondería al primer grupo. La figura 1 muestra el proceso de desarrollo que un alumno debería de seguir para analizar estos casos.

El diseño de un método de caso debe plasmarse en una guía pedagógica que permita a un docente su correcta utilización. En la sección siguiente describiremos el proceso que hemos seguido para elaborar nuestro ejemplo, desde la idea inicial hasta la elaboración de dicha guía docente.

4. Ejemplo para Seguridad Informática

4.1. Selección del caso

La teoría dice que se deberían de seleccionar casos reales, que puedan suscitar algún debate, que permitan sostener posiciones encontradas, suscitar polémica. No es fácil encontrar este tipo de problemas

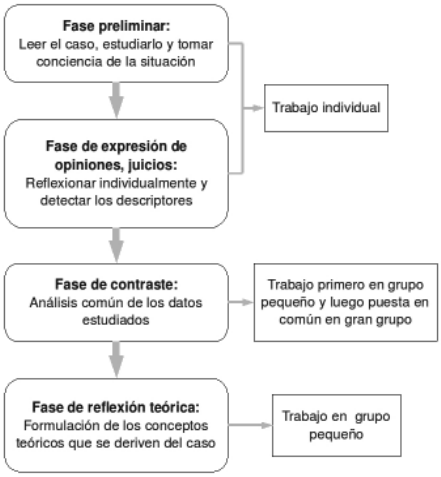

Figura 1: Fases de trabajo en el análisis de un caso centrado en el estudio de descripciones, tomada de [9].

Figura 2: Imagen de la página Web donde se describe el caso a analizar.

en Informática, una disciplina bastante reglada, como cualquier otra ingeniería.

Una vez que teníamos claro que queríamos buscar algún tema relacionado con la Segurida Informática, y más concretamente con la configuración segura de los ordenadores, nos pusimos a buscar en la red noticias reales relacionadas con este campo. Otra forma de obtener casos para trabajar sería entrevistar a expertos en el campo para que nos describan situaciones vividas por ellos [4].

Encontramos una noticia que nos pareció cumplir los requisitos pedidos en la siguiente dirección: `http://lavozdeljoven.blogspot.com/2009/11/cuidado-virus-informatico-que-dana.html` (figura 2).

4.2. Descripción y justificación

En esta noticia se describe la situación de una persona que vio atacado su ordenador por un hacker, que lo utilizó para almacenar y difundir pornografía. Como consecuencia del descubrimiento de dicho material, el protagonista perdió su trabajo, amigos y dinero.

Pensamos que podríamos utilizar ese material (hay otros similares) para fomentar el debate sobre la necesidad de mantener una configuración segura de nuestros ordenadores, y también de la obligación de hacerlo, de la responsabilidad que adquirimos cuando conectamos nuestro ordenador a la red. La actividad podría incluir una parte relativa a consejos o pautas para realizar dicha configuración.

Una vez comprobado que el caso era adecuado y que teníamos claros los objetivos y perfilados los puntos centrales del debate, procedimos a "formalizar la guía docente". Los cuatro apartados siguiente reproducen íntegramente el contenido de dicha guía.

4.3. Justificación pedagógica

Inserción en el plan docente: La actividad se enmarca dentro de la materia de Seguridad Informática, perteneciente al Plan de Estudios del Grado en Informática, del primer semestre del cuarto curso, cuando los alumnos disponen ya de las competencias mínimas requeridas para seguirla. Dichas competencias habrán sido adquiridas en las asignaturas de Redes y Sistemas Operativos.

En esta actividad se pretende que el alumno aprenda conceptos relacionados con la configuración segura de una computadora. Para ello, los estudiantes deben conocer los conceptos de seguridad informática, configuración de redes, así como aspectos básicos de *spyware* y virus entre otros, para los cuales harán actividades previas relacionadas con estos te-

mas.

Una vez realizada esta actividad, los alumnos estarán en condiciones de continuar con los siguientes contenidos y actividades de la materia, que consistirán en el desarrollo de una guía de configuración de seguridad básica para equipos de usuario, que pueda ser de cumplimiento obligado para cualquier ordenador conectado a Internet.

Explicitación del enfoque pedagógico: Se ha elegido un método constructivista, de tal forma que el estudiante vaya aprendiendo a medida que va interaccionando con los demás estudiantes, con sus opiniones, y con su entorno: búsqueda y estudio de los diferentes aspectos y documentos que se pueden relacionar con la lectura inicial propuesta. Será también una actividad colaborativa, ya que los estudiantes, partiendo de sus ideas y conocimientos individuales, deberán llegar a un solución final conjunta y completa para el problema propuesto: la seguridad de los equipos informáticos.
Objetivos de la actividad:

- Comprender la importancia de la protección de equipos frente a posibles ataques.
- Conocer las posibles soluciones a tomar frente a un ataque informático.
- Aplicar los conocimientos adquiridos a la construcción de una guía básica de seguridad.

Competencias en juego y a desarrollar:

- Competencias de partida: conocimientos previos de Sistemas Operativos y Redes; dominio del idioma inglés a nivel de documentos técnicos.
- Competencias específicas de la titulación: dependen de la guía docente concreta
- Competencias específicas de la materia: conocer la arquitectura de seguridad de los sistemas operativos actuales y saber configurarlos y administrarlos de un modo seguro; ...
- Competencias transversales: capacidad de análisis, síntesis y evaluación; capacidad de tomar decisiones; razonamiento crítico; ...

4.4. Elementos del caso

Introducción: Michael Fiola, ex investigador de la oficina del gobierno de Massachusetts, se vio involucrado en un escándalo de pornografía infantil a través de la red. Los jefes de Fiola detectaron un flujo anormal de datos en el ordenador del interesado, lo cual les llevó a realizar una tarea de investigación sobre el mismo, y encontraron en su equipo una gran cantidad de pornografía infantil. Por ello, fue despedido y juzgado, perdió amigos y trabajo, y tuvo también graves consecuencias personales.

Michael Fiola siempre se declaró inocente, y tras una dura lucha consiguió demostrar que un hacker se había introducido en su sistema, y era el responsable de todos los contenidos pornográficos alojados en su máquina.

Descripción general / análisis: Se trata de que los alumnos tomen conciencia de la importancia de mantener los equipos informáticos protegidos contra posibles ataques, así como de que sean capaces de buscar soluciones a la falta de seguridad, y se encuentren preparados para confeccionar una guía básica de seguridad para cualquier equipo conectado a Internet.

Para poder llevar a cabo la actividad, los alumnos deberán completar la documentación entregada por el profesor con material que ellos mismos deberán buscar y seleccionar, bien a través de Internet, bien mediante libros de consulta u otras fuentes que consideren apropiadas. Al finalizar el análisis y el debate entre ellos, deberán ser capaces, entre todos, de confeccionar la anteriormente citada guía básica.

Informe de situación: Se plantea un problema de seguridad informática que puede repercutir en gran manera en los usuarios implicados en él, de forma que puede llegar incluso a afectar en el aspecto profesional, económico y personal. El tema central del estudio consiste en las graves repercusiones que puede acarrear una falta de protección de nuestro equipo, cuando algún intruso se introduce en nuestro sistema y lo utiliza como almacén o repositorio de material ilegal: cuando éste es encontrado, es difícil demostrar la inocencia de los propietarios de los equipos y, aún en el caso de que esto se consiga, las consecuencias para dicho propietario pueden llegar a ser irreversibles.

Problemas concretos que deben resolver los alumnos: Entre las preguntas que podrían ser objeto de debate estarían:

- ¿Se respetó la presunción de inocencia en este caso?
- Aunque no son culpables del delito, ¿podrían

tener algun tipo de culpabilidad por no tener su ordenador protegido?
- ¿Qué nivel de protección sería exigible a los usuarios?
- Supongamos que el daño fuese monetario (ataque a las cuentas bancarias por ejemplo), ¿habría que devolverle el dinero a los usuarios si ellos no fueron los ladrones?
- ¿Podrían ser responsables las compañías de telecomunicaciones de los ordenadores conectados a las mismas?
- Pensando ahora en un hacker o en un fabricante de virus, ¿sería delito entrar en un ordenador ajeno sin causar daños?

Además, al finalizar el debate y clarificar los aspectos anteriores, deben poder:

- Proponer posibles medidas de seguridad para sus equipos.
- Ser capaces de detectar si están siendo víctimas de un ataque informático.
- Confeccionar una guía de seguridad básica.

Anexos: Se proporcionará al alumno la siguiente información y documentación:

- `http://lavozdeljoven.blogspot.com/2009/11/cuidado-virus-informatico-que-dana.html`
- `http://es.wikipedia.org/wiki/Seguridad_informatica`
- `http://www.criptored.upm.es/guiateoria/gt_m001a.htm`
- `http://www.educa.madrid.org/web/cp.seneca.madrid/webaprend_archivos/manualseguridad.pdf`

4.5. Guía docente: elementos

Sinopsis: Análisis de un problema de seguridad informática real, y estudio de los posibles efectos de los virus informáticos sobre una computadora, así como los problemas colaterales potenciales derivados de la falta de protección de nuestros equipos de usuario.

Objetivos pedagógicos:

- Comprender la importancia de la protección de equipos frente a posibles ataques.

Act.	Método	items
1	Ninguno	
2	Escala(0-3)	Entradas de información Réplicas a otras entradas Aportaciones originales
3	Escala(0-3)	Entradas personales Conclusiones del debate Réplicas a otras entradas
4	Escala(0-3)	Participación en hilos Aportaciones personales Comentarios a otros
5	Rúbrica	ver figura 3

Cuadro 1: Evaluación de las actividades

- Aprendizaje autónomo.
- Pensamiento crítico y responsabilidad.
- Ser capaz de tomar decisiones frente a problemas de seguridad de nuestra computadora.

Dinámica de trabajo:

1. Lectura del texto de partida para tomar conciencia del problema existente (individual).
2. Recopilación y ampliación de documentación mediante la recogida de casos similares (individual).
3. Debate/discusión acerca de las lecturas realizadas (grupo grande):
   - Aportaciones de los alumnos sobre los distintos casos encontrados (grupo grande).
4. Debate/discusión sobre las preguntas planteadas por el profesor (las ya mencionadas anteriormente).
5. Elaboración de guía de seguridad (grupo pequeño): cada grupo se ocuparía de uno de estos tres apartados: seguridad de red, acceso local, ataques "sociales".

Evaluación: De las 5 actividades descritas, la primera de ellas no será directamente evaluable, la última se evaluará mediante una rúbrica y las otras tres mediante escalas de valores [5]. La tabla 1 y la figura 3 recogen el contenido de dichas escalas y rúbricas.

Anexos: Portales sobre seguridad informática

- `http://www.kriptopolis.org/`
- `http://www.iec.csic.es/CRIPTonOMiCon/default2.html`

CATEGORY	Nada	Poco	Suficiente	Mucho
Presentación del documento escrito	Faltas de ortografía, estilos y tipos de letras, párrafos, sangrados.... demasiado heterogéneos Falta de índice y tabla de contenidos.	Algunas faltas de ortografía. Fallos de estilo. Falta de índice y tabla de contenidos.	Muy pocas faltas de ortografía. Algún fallo de estilo.	Sin faltas de ortografía. Con índice y tablas de contenido. Estilos bien definidos
Claridad y concisión	Redacción incoherente, demasiado extensa, poca concreción.	Algunas frases mal redactadas, falta de coherencia en varias partes del documento.	Redacción aceptable.	Completamente bien redactado. Sin redundancia informativa.
Contenido	Poco contenido o contenido poco relevante.	Contenido que cubre de manera escueta los principales puntos de la materia.	Contenido que desarrolla en gran medida los puntos fundamentales.	Contenido abundante, abarcando desde los mínimos a otros contenidos extra.
Bibliografía actualizada	Ausencia de bibliografía.	Bibliografía mínima o no actual.	Bibliografía aceptable en número o actualización, pero con algunos fallos.	Bibliografía extensa y actualizada.

Figura 3: Rúbrica para evaluar la actividad 5.

Libros

- Simson Garfinkel, “Web Security, Privacy & Commerc”, OReilly & Associates (2001).

Cuando hablamos de “grupo grande” y “grupo pequeño” estamos utilizando la terminología que se emplea en nuestra universidad para referirnos a “toda la clase” y a “grupos reducidos de 5-10 personas”.

4.6. Entorno de aprendizaje: herramientas

El desarrollo de la actividad requiere el empleo de varias herramientas de la Web 2.0. Podría realizarse con cualquier plataforma de teledocencia de que disponga el profesorado; en este caso, trabajaremos con Faitic, la plataforma de teledocencia de la universidad de Vigo, basada en Moodle [2].

La plataforma se utilizará para publicar el material necesario, y para que los alumnos hiciesen las correspondientes entregas. Las herramientas a utilizar, fase por fase serían:

1. Lectura del texto de partida para tomar conciencia del problema existente: Sección “Documentos” de Faitic.
2. Recopilación y ampliación de documentación mediante la recogida de casos similares o información que los alumnos consideren relevante: Sección “wiki” de Faitic para que los alumnos vayan subiendo la información que encuentran.
3. Debate/discusión acerca de las lecturas realizadas: Se realizará en clase. Los alumnos recogerán en la wiki las principales conclusiones a las que llegan.
4. Debate/discusión sobre las preguntas planteadas por el profesor: No se necesita herramienta, ya que se realizará en clase. Tras la discusión, se abrirán varios hilos en un foro para ir recogiendo las opiniones y respuestas de los alumnos.
5. Elaboración de guía de seguridad: Sección “wiki” de Faitic. Se pueden incorporar vídeos y presentaciones mediantes enlaces a Slideshare (`www.slideshare.net`). El resultado final debe subirse a la Wikipedia (`http://es.wikipedia.org/wiki/Wikipedia:Portada`)

5. Conclusiones

Este artículo fue escrito con una doble intencionalidad. Por una parte servir de “plantilla” para aquellos profesionales que deseen elaborar un estudio de caso para otra materia. Por ello, hemos puesto especial cuidado en describir el aspecto teórico de esta metodología, y hemos proporcionado referencias suficientes para completar dicha descripción.

Por otra parte, hemos querido aportar un recurso docente, listo para su utilización por parte de cualquier docente que imparta la materia “Seguridad Informática”. Para ello, hemos redactado los apartados 4.3, 4.4, 4.5 y 4.6 en un formato de “guía docente de la actividad”. Esta guía docente, podría ser directamente incorporada a cualquier repositorio de materiales educativos.

Hoy en día es posible encontrar en Internet recursos docente clásicos: apuntes en pdf, presentaciones, boletines de problemas, cuestionarios, etc. Sin embargo, es muy difícil encontrar guías docentes de actividades, y menos de e–actividades. Creemos que sería muy interesante que fuesen desarrollándose repositorios de guías docentes, similares a la presentada en este artículo.

Agradecimientos

El recurso docente presentado en este artículo fue creado durante la impartición de un curso organizado por el Vicerrectorado de Innovación Educativa de la Universidad de Vigo. Dicho curso fue impartido por los profesores Albert Sangrá, Lourdes Guardiá y

Marcelo Maina, de la Universidad Oberta de Cataluña. Nuestro más sincero agradecimiento a los tres.

Referencias

[1] Cabero, J., Román, P. *E-actividades. Un referente básico para la formación en Internet*. Editorial MAD, 2006.

[2] Cole, JR. *Using Moodle: Teaching with the Popular Open Source Course Management System*, OReilly & Associates, 2005.

[3] Harmelen, M. *Personal Learning Environments*. IEEE Int. Conf. on Advanced Learning Technologies (ICALT), pp. 815–81, 6Holanda, 2006.

[4] Instituto Tecnológico de Monterrey. *El estudio de casos como técnica didáctica*, 2005. (disponible online en `http://www.itesm.mx/va/dide2/documentos/casos.PDF`)

[5] Mertler, CA. *Designing scoring rubrics for your classroom*. Practical Assessment, Research & Evaluation, 7(25). 2001. (disponible online en `http://PAREonline.net/getvn.asp?v=7&n=25`

[6] Ministerio de Educación, Cultura y Deporte. *La integración del sistema universitario español en el Espacio Europeo de Enseñanza Supeior*, 2003 (disponible online en `http://www.eees.es/pdf/Documento-Marco_10_Febrero.pdf`.

[7] Riera, A., Vila, XA., Schuster, A., Barro, S. *Una Plataforma para el Soporte de Actividades Colaborativas en Entornos Docentes Presenciales*, Conferencia de la Asociación Española para la Inteligencia Artificial (CAEPIA), Santiago de Compostela, 2005.

[8] Salmon, G., *E–actividades: El factor clave para una formación en línea activa*, Editorial UOC, Barcelona, 2004.

[9] Universidad Politécnica de Madrid. *El método del caso. Guías rápidas sobre nuevas tecnologías*, 2008 (disponible online en `http://innovacioneducativa.upm.es/guias/MdC-guia.pdf`).

[10] Vila, X., Canay, R. *USC-Virtual: Five years improving services*, 3rd Int. Conf. on Multimedia and Information & Communication Technologies in Education (m-ICTE), Cáceres, 2005.