Impacto de un factor de seguridad de la información sobre Objetos de Aprendizaje en LMS

Luis A. Chamba Eras[1], Ana Arruarte[2], Jon Ander Elorriaga[2]

[1]Carrera de Ingeniería en Sistemas
Área de la Energía, las Industrias y los Recursos Naturales No Renovables
Universidad Nacional de Loja
Loja - Ecuador
lachamba@unl.edu.ec
[2]Departamento de Lenguajes y Sistemas Informáticos
Facultad de Informática
Universidad del País Vasco UPV/EHU
Donostia – España
{a.arruarte, jon.elorriaga}@ehu.es

Resumen. En este artículo se presenta los resultados obtenidos al evaluar el impacto de un factor de seguridad de la información sobre objetos de aprendizaje en sistemas de gestión de aprendizaje. El factor de seguridad de la información está integrado por dos componentes: derechos de autor y certificados digitales, los mismos que permitirán mejorar la confianza entre los participantes de comunidades virtuales de aprendizaje utilizando LMS. Se evalúa el factor de seguridad de la información con un grupo de estudiantes miembros de una comunidad de virtual de aprendizaje. Se utilizó un sistema de encuestas para recolectar información referente a la opinión e importancia del factor y un sistema de comunidades virtuales de aprendizaje sobre el cual se diseño el experimento.

Palabras clave: confianza, objetos de aprendizaje, comunidades virtuales de aprendizaje, factor de seguridad de la información.

1 Introducción

El desarrollo de Internet y de las herramientas colaborativas han propiciado la utilización de los Learning Management Systems (LMS) como apoyo a la formación presencial, semi-presencial, o virtual que ofrecen las universidades o las organizaciones que trabajan comportándose como comunidades virtuales de aprendizaje (CVA) donde los LMS permiten crear espacios en común y los usuarios comparten perfiles o características para comunicarse e intercambiar con toda confianza un sinnúmero de recursos educativos a través de las posibilidades que ofrecen las Tecnologías de la Información y la Comunicación.

Dentro de las Comunidades Virtuales (CV) una CVA se define como aquella agrupación de personas que se organiza para construir e involucrarse en un proyecto educativo y cultural propio, y que aprende a través del trabajo colaborativo, cooperativo y solidario. Una CVA está conformada por un grupo de personas que aprende conjun-

tamente utilizando herramientas comunes en un mismo entorno [1]. Los LMS actualmente permiten que los objetivos que persiguen las CVA se cumplan cuando las personas de la comunidad utilizan actividades de aprendizaje ligadas a la compartición de lo que producen en la comunidad (foros, glosarios) y estás experiencias son más exitosas cuando estén ligadas a la generación, producción y realización de tareas confiables que persigan fines comunes en beneficio de la comunidad.

Un LMS proporciona un ambiente de CVA en donde los miembros comparten materiales, creencias y formas de aprender diversos temas en común. Las CVA ayudan a disminuir los problemas que surgen por las dificultades, o incluso imposibilidad, de comunicación en tiempo real y a la vez ahorran tiempo al compartirse lecciones aprendidas por otros grupos de usuarios. Sin embargo, el hecho de que las personas puedan o no conocerse personalmente hace que la confianza se convierta en un factor determinante en el funcionamiento de las CVA mediados por un LMS.

Actualmente, tras el trabajo de diversas organizaciones [2,3] persiguiendo la estandarización de los recursos didácticos que se utilizan dentro de un LMS, se han definido los Objetos de Aprendizaje (OA) como unidades de aprendizaje reutilizables [4,5]. Se cuenta con propuestas donde algunas CVA implementan sistemas de seguridad sobre los OA [6] con firmas o certificados digitales, en cambio otras, no cuentan con ningún procedimiento que estime valores de confianza de los OA [7]. Este aspecto es importante en las CVA donde se crean espacios comunes de trabajo con los OA que van generando los usuarios.

En el contexto de la Educación Superior la formación presencial, semi-presencial y a distancia utilizan plataformas que facilitan la fluidez de comunicación entre cada uno de los miembros. Muchas universidades, institutos tecnológicos a nivel nacional y mundial ponen a disposición los OpenCourseWare (OCW) como fuente de apoyo o de divulgación por parte de su cuerpo docente. Parte de ese material, si proviene de una universidad, se considera fuente confiable.

El objetivo del artículo es evaluar el impacto del factor de seguridad de la información [8] para objetos de aprendizaje en sistemas de gestión de aprendizaje (LMS) con un grupo de estudiantes miembros de una comunidad de virtual de aprendizaje que participan en un curso de apoyo a la formación presencial de Introducción a los Algoritmos Genéticos conformado por actividades que permiten generar y compartir OA que se gestionan en un LMS. La estructura del artículo es la siguiente: Modelos de Confianza para OA en LMS, aquí se presenta formalmente el estado del arte relacionado a las investigaciones aproximadas realizadas en éste ámbito. Asimismo, se presenta de manera general modelos de confianza y reputación utilizados en entornos de CVA. Factor de la seguridad de la información para objetos de aprendizaje en LMS, aquí se observa los componentes del factor de seguridad de la información [8] y algunos conceptos de WOT[1]. En el caso de estudio se trabaja con el diseño instruccional del curso de Introducción de Algoritmos Genéticos en el LMS- EQUALA[2] combinado con el sistema de encuestas en línea (Limesurvey), se realiza éste caso de estudio con estudiantes universitarios de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja. Y por último tenemos la parte de Conclusiones en donde se describen las conclusiones extraídas en la investigación.

[1] Herramienta de navegación segura en Internet

[2] http://eqaula.org/eva, Red Social de Aprendizaje

2 Modelos de confianza para objetos de aprendizaje en LMS

El concepto de confianza puede tener múltiples definiciones que se aplican a diversos contextos. Se la concibe como la medida en la que una persona está confiada y ansiosa de actuar en base a las palabras, las acciones y las decisiones de otros [9]. La confianza es un concepto abstracto que en la mayoría de las veces es usado indistintamente con términos relacionados como: credibilidad, confiabilidad o lealtad. Se considera el término confianza como el nivel de seguridad que se tiene a la hora de interactuar con un agente ya sea humano o automático.

La reputación es la percepción que una persona tiene sobre las intenciones y normas de otra, así como la confianza de una persona sobre las capacidades, honestidad y formalidad de otra persona, basada en las recomendaciones de otros. La diferencia entre confianza y reputación depende de quién tenga experiencia previa con la fuente de información, es decir, si una persona tiene experiencia directa con una fuente de información se puede decir que la persona tiene un valor de confianza para esa fuente. Por lo contrario, cuando la fuente de información ha sido recomendada por otra persona que previamente ha tenido experiencia con esa fuente, entonces se puede decir que la fuente tiene un valor de reputación [10].

Los sitios Web de comercio electrónico ofrecen productos y servicios, la finalidad es ofrecer un entorno de confianza en donde los usuarios puedan adquirir sus productos o servicios sin temor a ser engañados. Para ello cada sitio de comercio electrónico implementa diferentes mecanismos que garantizan la confianza del cliente en el momento de realizar operaciones.

Por otra parte, existen modelos de confianza y reputación basados en agentes inteligentes. Un sistema basado en agentes se define como un sistema que busca lograr la cooperación de un conjunto de agentes autónomos para la realización de una tarea. La cooperación depende de las interacciones entre los agentes e incorpora tres elementos: la colaboración, la coordinación y la resolución de conflictos. Además, un sistema basado en agentes puede estar constituido por un único agente (SingleAgentSystem-SAS) o por múltiples agentes (SistemaMultiAgente-SMA). La mayor diferencia entre estos sistemas se basa en los patrones de comunicación. Un SMA se comunica con la aplicación y el usuario, así como con otros agentes en el sistema. Sin embargo, en los sistemas basados en un único agente los canales de comunicación están abiertos solamente entre el agente y el usuario. Es importante destacar que utilizar varios agentes para la solución de problemas no sólo implica dividir las tareas para cada individuo y esperar a que éstas se ejecuten, sino también que los agentes actúen entre sí y compartan conocimientos. Además se deben coordinar sus acciones ante los posibles cambios del entorno con el fin de lograr un objetivo común o permitir que cada uno de ellos cumpla sus objetivos personales de la manera más eficiente.

Los nuevos modelos de confianza se basan en el concepto de Web of Trust (WOT), en donde se utilizan técnicas de seguridad informática basadas en la criptografía para estimar valores de confianza y reputación en CV [9]. Un punto importante al trabajar con OA en las CVA gestionados por LMS, y que permite aumentar el nivel de confianza entre los participantes radica en la presentación de contenidos alineados a metodologías y estrategias pedagógicas en el ámbito virtual contenido bajo un conjunto de especificaciones (estándares-evaluación), cuya finalidad es que los OA sean lo más transparentes e interoperables entre los LMS y los usuarios que participan en

las CVA [7]. Algunos sistemas de confianza han trabajado con modelos de Webs de confianza basados en WOT, donde se construye una red de confianza que permite que los usuarios aporten una calificación para sí mismos y mediante un organismo central almacenar las puntuaciones directas sobre otros usuarios de la red [6].

En [11] se presenta un Sistema de Vigilancia Tecnológica y Agentes Inteligentes. Estos sistemas se dedican a procesar la información tecnológica del entorno para extraer conocimiento, como la identificación de tendencias y cambios. En este trabajo se hace hincapié en el problema fundamental de evaluar y gestionar fuentes de información. Dada la naturaleza y objetivos de un sistema como éste, se propone un diseño orientado a agentes donde la calidad de una fuente de información se mide de acuerdo con el modelo de confianza REGRET. En este modelo, los agentes representan tanto a los usuarios como a las distintas funcionalidades del sistema. El diseño sigue la metodología INGENIAS y fue realizado con las herramientas que dispone dicha metodología en el modelado de la confianza y reputación en los sistemas multi-agente.

En [12] se define una arquitectura multi-agente y un modelo de confianza para gestionar el conocimiento en comunidades de práctica. Esta arquitectura permite dar soporte, compartir conocimiento en las comunidades de práctica y evitar la sobrecarga de información mostrando aquella más confiable, así como detectar personas que introducen información irrelevante y potenciar la reutilización de información pudiendo recomendar información.

En [8] se define un modelo de confianza para OA en CVA. Se propone un modelo con 6 factores: rol, presentimiento, conocimiento, experiencia previa, calidad y CertificadoDigital-DerechosAutor (CDDA), todos estos factores relacionados a las fuentes de información que participan en una CVA. El factor de seguridad de la información CDDA se lo utilizará para evaluar el impacto de objetos de aprendizaje en los LMS para ello se preparó un diseño instruccional de un curso de Algoritmos Genéticos que permitirá a los participantes emitir su punto de vista sobre el impacto del factor de seguridad de la información.

En lo relacionado a modelos de confianza para OA en LMS, las investigaciones preliminares permiten observar que el LMS (Moodle 2.0) han acoplado un tipo de licencias de protección intelectual para los recursos que se disponen en él, actualmente un modelo de confianza específico no existe por lo que la línea de investigación en esta área es abierta.

3 Factor de seguridad de la información para Objetos de Aprendizaje en LMS

Partiendo de la propuesta [8] donde se define 6 factores para el modelo de confianza, se ha seleccionado el factor CDDA que combina Seguridad Informática en un entorno de CVA. Los componentes del factor que utilizaremos para evaluar el impacto sobre los objetos de aprendizaje en LMS son: derechos de autor y certificados digitales. Se observa en la Figura 1 la ubicación de los componentes del factor de seguridad en relación a los LMS como infraestructura de una CVA.

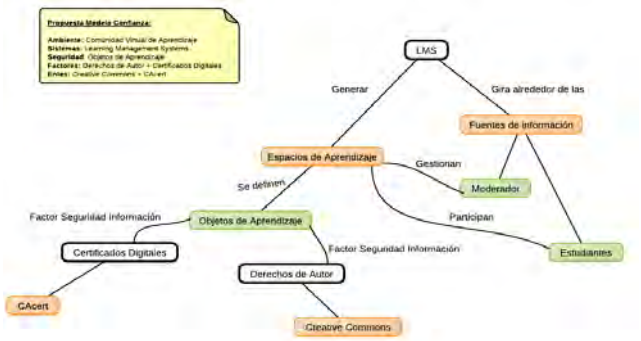

Fig. 1. Componentes del factor de seguridad de la información en ambientes LMS.

A continuación se describe el esquema presentado en la Figura 1:

- LMS: es el sistema que permitirá gestionar los OA que produzcan las fuentes de información en cada uno de los espacios de aprendizaje.
- Espacios de Aprendizaje: son los cursos virtuales que sirven de apoyo para la formación presencial, semi-presencial o a distancia y donde se consumirán, crearán OA.
- Fuentes de Información: son las personas que consumen, generan o producen conocimiento en los espacios de aprendizaje al compartir OA que serán valorados de acuerdo a al factor de seguridad de la información.
- Objetos de Aprendizaje: son los recursos que serán valorados y en base a ellos cada fuente de información obtendrá su nivel de confianza si cumplen el factor de seguridad de la información.
- Moderador: es el encargado de proponer actividades que permitan compartir (foros) crear y gestionar OA dentro de un espacio de aprendizaje.
- Estudiantes: son los que participan al crear y proponer OA en cada una de las actividades propuestas por el moderador. Son los encargados de evaluar los OA generados en la CVA.
- Certificados Digitales: componente del factor de seguridad de la información, se trata de certificados digitales emitidos por una entidad certificadora.
- Derechos de Autor: son los permisos o derechos que los creadores de OA les atribuyen a sus obras.
- CAcert: es una autoridad de certificación que otorga certificados de clave pública y que pueden ser usados para firmar y cifrar correo electrónico, identificar y autorizar usuarios a sitios web para la transmisión de datos.
- Creative Commons: son las licencias de derecho de autor de acceso libre que se utilizarán para los OA digitales que se gestionan en el LMS.

El factor de la seguridad de la información hace referencia a la confianza que tienen las fuentes de información sobre otras basándose en un nivel de seguridad digital sobre los contenidos que producen las fuentes de información. Este factor utiliza certificado/firma digital combinado con derechos de autor por medio de un tipo de licencia libre de los OA digitales. Además este factor combina los conceptos de la Web of Trust. El certificado/firma digital puede ser obtenido por una entidad certifi-

cadora como CAcert[3], así como los derechos de autor por medio de las licencias Creative Commons[4].

Para obtener un valor aproximado de confianza que se obtendrá por medio del factor de seguridad de la información se redefinirá la fórmula utilizada en el modelo de confianza definido en [8].

La nueva fórmula matemática será la siguiente:

$$T(i,j) = PCDDA * CDDA(j) \quad (1)$$

Donde:

- T(i,j), representa la confianza que una FI (i) de la CVA tiene sobre otra FI (j).
- CDDA(j), representa el valor de seguridad de los OA producidos por la FI (j).

Se cuenta con el peso PCDDA que permiten controlar el valor de confianza. El valor de este peso permitirá identificar el grado de importancia del factor de acuerdo a los diferentes escenarios en los que las fuentes de información se puedan comportar en la CVA gestionado por un LMS.

4 Caso de estudio

En esta sección se describe un caso de estudio realizado en un contexto educativo real con el objetivo de evaluar el impacto del factor de Seguridad de la Información definido la sección anterior, para ello se ha realizado un diseño instruccional de un curso de apoyo a la formación presencial con los temas de Algoritmos Genéticos[5], diseñado con actividades colaborativas como foros para generación y compartición de OA dentro de un espacio de aprendizaje en el LMS. EQAULA se utiliza como soporte LMS de una CVA. Además se cuenta con el sistema de encuestas on-line LimeSurvey[6] que permitirá recoger la opinión de los estudiantes participantes de CVA sobre los OA producidos y consumidos en el espacio de aprendizaje permitiendo evaluar el factor de seguridad de la información.

El diseño del caso de estudio está estructurado en dos fases de experimentación integradas por los sistemas web: EQAULA (LMS) y LimeSurvey (ver Figura 2).

[3] http://www.cacert.org/, Autoridad de certificación
[4] http://creativecommons.org/, Las licencias Creative Commons
[5] http://eqaula.org/eva/course/view.php?id=1800, Espacio Virtual de Aprendizaje en EQAULA
[6] http://lachamba.ec/limesurvey, Sistema Limesurvey para recolección de opinión usuarios

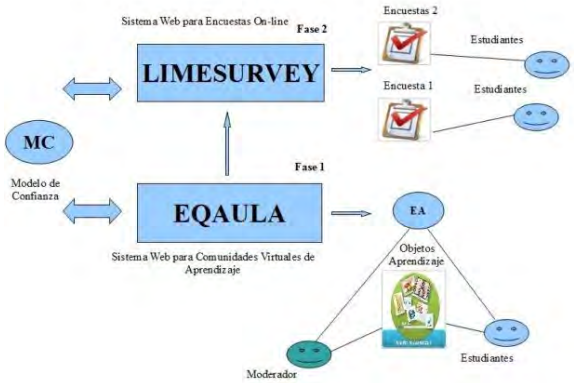

Fig. 2. Esquema del caso de estudio para el factor de Seguridad de la Información del modelo de confianza en LMS.

Para la experiencia práctica se ha trabajado con un grupo de estudiantes con su respectivo moderador que actúan como conocedores en el área de la temática a tratar en el curso de apoyo. Los miembros del grupo de estudiantes trabajan en la CVA teniendo en cuenta los componentes del factor de seguridad de la información.

Para el grupo de estudiantes se configuró la CVA creando un espacio de aprendizaje (EA) con sus respectivos participantes registrados (estudiantes, moderador). Se realizó el diseño instruccional del EA basado en los componentes del factor de seguridad de la información y creando los OA correspondientes. Por ejemplo se produjeron OA con licencias Creative Commons, así como el certificado digital para la fuente de información que modera el curso virtual, etc. El grupo tuvo la capacidad de producir y consumir OA en el transcurso del EA. Ésta CVA trata la temática relacionada con la Introducción a los Algoritmos Genéticos utilizando JGAP en el campo de la Inteligencia Artificial. Este grupo estuvo integrado por estudiantes del quinto año de la Carrera de Ingeniería en Sistemas de la Universidad Nacional (UNL) de Loja-Ecuador.

Se ha definido 2 encuestas orientadas al grupo de estudiantes:

- Evaluación de objetos de aprendizaje de la CVA: consta de 4 preguntas y está orientada a descubrir la opinión de los OA generados y consumidos en el LMS.
- Evaluación de participantes del grupo de estudiantes de la CVA: consta de 42 preguntas y está orientada al grupo de estudiantes.

Las encuestas se encuentran conformadas por preguntas dicotómicas-cerradas con respuestas de opción múltiple a escala que nos permitirán contabilizar los resultados utilizando la aproximación para el cálculo de pesos basados en la opinión de los participantes [8]. Cada una de las preguntas están relacionadas con los componentes del factor de seguridad de la información y tienen 4 opciones de elección del tipo: casi siempre, a menudo, rara vez y casi nunca o también del tipo: muy importante, importante, poco importante y nada importante.

A continuación, presentamos las configuraciones iniciales en el caso de estudio para el grupo de estudiantes:

- 51 estudiantes inscritos y participantes del EA dentro del LMS
- 1 moderador del EA

- 30 OA en el EA configurados en el LMS

Las encuestas nos van a permitir evaluar el impacto que el grupo de estudiantes otorga al factor de seguridad de la información.

La aproximación definida en [8] permite obtener valores de pesos estimados basándose en las respuestas obtenidas en las encuestas y será la que nos permitirá evaluar al factor de seguridad de información.

Se explica los componentes de la aproximación que utilizaremos:

- PF(i): peso del factor (i) de la fórmula de confianza definida en el modelo [8]
- Q(i,j): pregunta (j) sobre el factor (i)
- A(i,j,k): alternativa de respuesta (k) a la pregunta (j) sobre el factor (i) como por ejemplo: casi siempre (1), a menudo (2), rara vez (3) y casi nunca (4), numeradas de mayor a menor grado de valoración
- PORA(i,j,k): porcentaje obtenido por la alternativa (k) a la pregunta (j) sobre el factor (i)
- PA(i,j,k): grado de importancia de la alternativa (k) de la pregunta (j) sobre el factor (i) que se está valorando, es un valor continuo siempre en el intervalo]0,1], si la respuesta es no aplicable (NA) no se considerará para los cálculos
- VALP(i,j,k): es el resultado del producto del porcentaje de la respuesta obtenido PORA(i,j,k) multiplicado por el peso (PA(i,j,k))
- $VALP(i,j,k) = PORA(i,j,k) * PA(i,j,k)$
- SUMP(i,j): es el sumatorio entre cada uno de los valores de VALP(i,j,k), donde n es el número de alternativas por pregunta (j) sobre el factor (i)
- $SUMP(i,j) = \sum_{k=1}^{n} VALP(i,j,k)$
- MEDIASUMP(i): es la media aritmética de todos los SUMP(i,j), donde n es el número de preguntas por factor (i)
- $MEDIASUMP(i) = \frac{\sum_{j=1}^{n} SUMP(i,j)}{n}$
- PF(i), es el valor del peso del factor i del modelo de confianza.

$$PF(i) = MEDIASUMP(i)$$

Se presentan los resultados obtenidos en el caso de estudio realizado:

- En la encuesta de evaluación al grupo de estudiantes, participaron 48 estudiantes de la CVA.
- El EA contó con 30 OA para ser utilizados por los miembros del grupo experimental de la comunidad y a partir de ellos producir otros OA.
- Al finalizar el EA los miembros del grupo experimental la CVA produjeron un total de 204 OA.
- Los tipos de OA que se produjeron fueron: vídeos, documentos en formato pdf, doc, odt y html.
- Los OA en formato digital producidos tienen una licencia Creative Commons.

En la tabla 1 se presenta los valores para evaluar el impacto del factor de seguridad de la información realizado por el grupo de estudiantes.

Tabla 1. Valores resultantes al aplicar la aproximación al impacto del factor de seguridad de la información.

F(i)	Q(j)	A(k)	%A(k)	P A(k)	VP A (k)
Factor	**Pregunta**	**Respuesta**	**Porcentaje**	**Peso**	**VaIP**
Seguridad Información	1	1	57.45	1.00	0.57
		2	38.30	0.75	0.29
		3	2.13	0.50	0.01
		4	2.13	0.25	0.01
	2	1	42.55	1.00	0.43
		2	44.68	0.75	0.34
		3	12.77	0.50	0.06
		4	0.00	0.25	0.00
	3	1	10.64	0.25	0.03
		2	44.68	0.50	0.22
		3	36.17	0.75	0.27
		4	8.51	1.00	0.09
	4	1	21.28	1.00	0.21
		2	65.96	0.75	0.49
		3	12.77	0.50	0.06
		4	0.00	0.25	0.00
	SumP1	0.88		**Umbral**	**0.50**
	SumP2	0.82			
	SumP3	0.61			
	SumP4	0.77			
	MediaSumP	**0.77**			

De acuerdo a los resultados obtenidos por medio de la encuesta al grupo de estudiantes se afirma que el factor de seguridad de la información es importante en una CVA gestionado por un LMS en vista de que los valores obtenidos en el cálculo del peso son mayores al umbral de 0.50, en este caso del experimento fue 0.77.

Un factor importante en las CVA es la relación estudiante-moderador/es, ya que los participantes confían más cuando ya han tenido una relación previa de trabajo con ellos, permitiendo una mayor fluidez en el desarrollo y cumplimiento de actividades.

Los participantes del grupo de estudiantes confían en las fuentes de información que protegen sus OA con certificados digitales y además les proporcionen un tipo de licencia de derechos de autor. Esto hace notar que el factor de seguridad de la información es altamente aceptado ya que los participantes confían mucho en este factor.

5 Conclusiones

En este trabajo se ha presentado el impacto de un factor de seguridad de la información para OA en LMS que permite estimar la confianza sobre las fuentes de información que producen o consumen OA. El factor de seguridad de la información permite a los usuarios tener mayor confiabilidad sobre los recursos que se producen en un CVA.

Se ha planteado un escenario de experimentación real con el objetivo de evaluar el impacto del factor de seguridad de la información considerando la opinión de un grupo de estudiantes con diferentes características participativas en una CVA.

Se ha producido objetos de aprendizaje con sus respectivas licencias Creative Commons en el espacio de aprendizaje gestionado por un LMS basado en Moodle.

Referencias

1. Gairín Sallán, J. "Las comunidades virtuales de aprendizaje". Educar 37, (2006), Pp: 41-64.
2. Learning Technology Standards Committee (2002) (PDF), Draft Standard for Learning Object Metadata. IEEE Standard 1484.12.1, New York: Institute of Electrical and Electronics Engineers, [http://ltsc.ieee.org/wg12/files/LOM_1484_12_1_v1_Final_Draft.pdf, retrieved 2008-04-29].
3. Wiley, David A. (2000), "Connecting Learning Objects to Instructional Design Theory: A Definition, A Metaphor, and A Taxonomy", in Wiley, David A. (DOC), The Instructional Use of Learning Objects: Online Version, [http://reusability.org/read/chapters/wiley.doc, retrieved 2008-04-29].
4. Christopher Brooks, John Cooke, Julita Vassileva, "Versioning of Learning Objects" Advanced Learning Technologies, IEEE International Conference on, p. 296, Third IEEE International Conference on Advanced Learning Technologies (ICALT'03), 2003.
5. Chiappe, Andres; Segovia, Yasbley; Rincon, Yadira (2007), "Toward an instructional design model based on learning objects", in Boston, Springer (html), Educational Technology Research and Development, Boston: Springer, Pp: 671-681.
6. Gaona García, P. "Modelo Informático para autenticidad de contenidos mediante el concepto de Web of Trust sobre plataformas virtuales LCMS". Innovation and Development for the Americas, (2010), Pp: 1-10.
7. Dougglas Hurtado Carmona y Alfonso Mancilla Herrera. "Modelado de la seguridad de objetos de aprendizaje", Revista Generación Digital, Vol. 8, No.1, (2009), Pp: 38-42.
8. Chamba, L. Modelo de Confianza para Objetos de Aprendizaje en Comunidades Virtuales. Tesis de Máster. España-Donostia. Universidad del País Vasco. 2011.
9. Sanz, S. et al., "Concepto, dimensiones y antecedentes de la confianza en los entornos virtuales". Teoría y Praxis, No. 6 (2009), Pp: 31-56.
10. Chamba, Luis; Ana Ruarte y Jon Elorriaga. "Modelo de Confianza para Comunidades Virtuales de Aprendizaje", TISE2011, Santiago de Chile, Vol. 7. (2011), Pp: 80-87.
11. Rodríguez, C. Sistema de Vigilancia Tecnológica y Agentes Inteligentes. Tesis de Máster. España-Madrid. Universidad Complutense de Madrid. 2009.
12. Soto Barrera, J. P. Una arquitectura multi-agente y un modelo de confianza para gestionar el conocimiento en comunidades de práctica. Tesis Doctoral. España. Universidad de Castilla - La Mancha. 2006.