MODELO INFORMÁTICO PARA AUTENTICIDAD DE CONTENIDOS MEDIANTE EL CONCEPTO DE WEB OF TRUST SOBRE PLATAFORMAS VIRTUALES LCMS

Paulo Alonso Gaona García

Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, pagaonag@udistrital.edu.co

Carlos Enrique Montenegro Marín

Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, cemontenegro@udistrital.edu.co

Elvis Eduardo Gaona Garcia

Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, egaona@udistrital.edu.co

RESUMEN

El presente documento tiene como finalidad plantear una estrategia para el manejo de la autenticidad de contenidos en el desarrollo de Objetos de Aprendizaje LO "Learning Objects" sobre plataformas LCMS, basado en conjunto de especificaciones SCORM e IMS para garantizar la procedencia de contenidos creados en este tipo de ambientes de aprendizaje, y permitiendo la interoperabilidad entre diversas plataformas virtuales de aprendizaje mediante conceptos de Web de Confianza y mecanismos de seguridad que garanticen este tipo de actividades.

Palabras Clave: SCORM, IMS, LO, Objetos de Aprendizajes, seguridad informática, LCMS, firma digital

ABSTRACT

This document presents a strategy for managing the authenticity of contents on the development of Learning Objects LO "Learning Objects" on LCMS platforms, all based on SCORM and IMS specifications to ensure the provenance of content created in this type of learning environments, and enabling interoperability between different virtual learning platforms by concepts of Web Of Trust and security mechanisms to ensure this type of activity.

Keywords: SCORM, IMS, Learning Objects, Information Security, LCMS, digital sign

1. INTRODUCCIÓN

Los objetos de aprendizaje son uno de los elementos más representativos dentro de un proceso de enseñanza sobre plataformas virtuales, por lo tanto son la fuente para la presentación de contenidos alineados a metodologías y estrategias pedagógicas trabajados en instituciones académicas y centros de formación; su crecimiento y acogida en los últimos años, ha permitido ser uno de los factores más importantes para el desarrollo de contenidos bajo un conjunto de especificaciones, cuya única finalidad es que sea lo más transparente e interoperable a la hora de visualizarse en diferentes plataformas de aprendizaje. Este conjunto de especificaciones ha sido uno de los puntos claves que ha permitido una gran acogida a nivel académico, pero al mismo tiempo presenta una serie de características a nivel de autenticidad de los mismos no son claros a la hora de representarse en un ambiente virtual, lo que genera siempre un grado de desconfianza en el uso de este tipo de recursos sobre las plataformas.

El siguiente artículo pretende exponer una estrategia basada en autenticidad de contenidos sobre Objetos de Aprendizaje que permita determinar un grado de confianza de los contenidos que se trabajan sobre una plataforma virtual, la interoperabilidad sobre otras plataformas virtuales y que al mismo tiempo se pueda divulgar información de confianza a través del concepto de WOT (Web of Trust). Para llevar a cabo esta actividad, la estrategia abordada, se orientara a trabajar directamente sobre una serie de normas y conjunto de específicamente dadas por SCORM.

2. Panorama de Autenticidad de Contenidos sobre Plataformas LCMS

Los **LCMS** (Learning Content Management System) han sido producto de iniciativas de grupos de trabajo en Internet y la integración y creación de diferentes tipos de comités que a nivel mundial han permitido apoyar esta iniciativa para tratar de estandarizar los procesos de desarrollo de plataformas; cuya finalizada en particular es la formación académica y que por tanto según [1] ha permitido ser un factor determinante para facilitar metodologías de estudio diferentes a las tradicionales basadas en entrenamiento **CBT** (Computer Based Training), **IBT** (Internet Based Training) y **WBT** (Web Based Training).

Uno de los factores críticos que se lleva a cabo bajo esta iniciativa, es el manejo que se tiene a nivel de la información, tanto para su acceso, creación ó divulgación, lo que ha permitido generar un panorama que desde el punto de vista de seguridad informático apoyada sobre el uso de herramientas en este tipo de plataformas, sea un tema que no se ha abordado en su totalidad, dejando abierto muchos fallos a nivel del sistema que dejan vulnerables este tipo de plataformas y que por lo tanto dejan abiertos serios riesgos de manejo y manipulación de información sobre usuarios no confiables. Si bien es cierto que existen mecanismos que sirven de refuerzo para este tipo de actividades, el grado de confianza generado para identificar la procedencia y creación de contenidos académicos en este tipo de plataformas es un hecho que no ha sido controlado en su totalidad por ningún mecanismo informático y que a la luz de instituciones académicas representa un tema fundamental dentro de los procesos de formación y evaluación a nivel formativo. Partiendo del anterior referente se pretende reforzar este hecho a partir de los resultados obtenidos del análisis a nivel de autenticación de aplicaciones informáticas a más de 300 empresas del sector empresarial dentro de las cuáles se destacan el sector, salud, financiero y educativo realizados por el **CSI** (Computer Security Institute) en cabeza de su director [2] a finales del 2008, el cual representa que el uso inadecuado de la información es uno de los factores más críticos en la mayoría de aplicaciones informáticas y por ende a nivel educativo representan el segundo sector más vulnerable de ataques mediante el uso de herramientas de comunicación y de aprendizaje que en este caso las enmarcamos dentro de las plataformas virtuales de aprendizaje LCMS (Learning Content Management System).

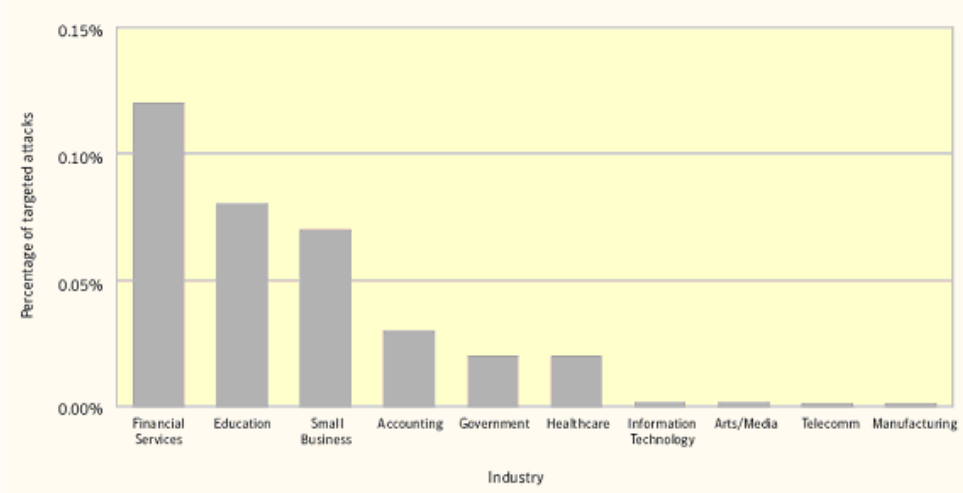

Figura 1 Número de Incidentes ocurridos en los últimos 10 años en sectores gobierno, financiero, salud y académicos. Fuente: [Symantec, 2008]

En la figura anterior, se puede observar que una de las áreas de mayor influencia aparte del sector financiero a nivel de seguridad son las entidades educativas. La razón radica en el hecho que son redes con bajos niveles de seguridad, aptas como laboratorio de pruebas para estudiantes que cada vez desafían sistemas de seguridad con altos niveles de inseguridad, las cuales tienen acceso a redes públicas y en algunos casos a redes privadas. Lo que refuerza esta propuesta de trabajo para este sector en particular.

Los principios de seguridad, han sido la base para plantear modelos y alternativas de trabajo comunes a múltiples empresas y de esta manera tener diferentes mecanismos que logren garantizar la autenticidad de la información que diariamente viajan por cada uno de los sistemas de comunicación de toda la Red Informática y que al mismo tiempo se definen conceptos para tratar de llevar a cabo ciertos niveles de confianza sobre los contenidos, elemento que se lleva a cabo mediante Webs de Confianza y que ha sido un concepto enormemente difundido en Internet, bajo las culturas que se ha formado a través de las Redes sociales.

3. Web Of Trust y Redes Sociales

El concepto de **WOT** "Web of Trust" se ha venido trabajando desde la creación del mecanismo **PGP** "Pretty Good Privacy" para seguridad de correos electrónicos [3], el cuál trata de plantear la idea de permitir y aceptar la identidad de un usuario en un sistema de comunicaciones siempre y cuando sea reconocido por otro usuario perteneciente a la plataforma, lo cual garantiza unas condiciones mínimas de Confianza para aceptarlo dentro de la plataforma que están compartiendo. En este sentido nace un concepto que permite la interacción de usuarios sobre Redes Sociales y el cual es relacionado mediante el proyecto **SIF** (Social Interaction Framework) [4], el cual, en este Framework un agente evalúa la reputación de otro agente basado directamente en observaciones de otros usuarios participantes en la misma plataforma, mientras que los sistemas tradicionales electrónicos se deben fiar de mecanismos externos que sirvan de intermediarios entre las personas que desean comunicarse.

Una evolución que ha tenido esta estrategia, se ve reflejado en los plugins de los navegadores de Internet, propuestas planteados por navegadores como Internet Explorer y Mozilla Firefox, mediante componentes conocidos como **WOT**. Este plugin es un componente que se descarga en el navegador del usuario y evita problemas asociados sobre Internet, como avisos de páginas no confiables, robo de identidad, páginas en Internet de Comercio electrónico no fiables, amenazas de seguridad de enlaces de páginas antes de ingresar en ellos, entre otros.

Algunos prototipos que han trabajado con este modelo de Webs de Confianza se pueden reflejar en el modelo de [5], construyendo una red de confianza por [6] y prototipos trabajados por [7], los cuáles requieren que los usuarios den una calificación para sí mismos y de esta manera tener un organismo central (puntuaciones directa) a otros usuarios de confianza (puntuaciones colaborativas).

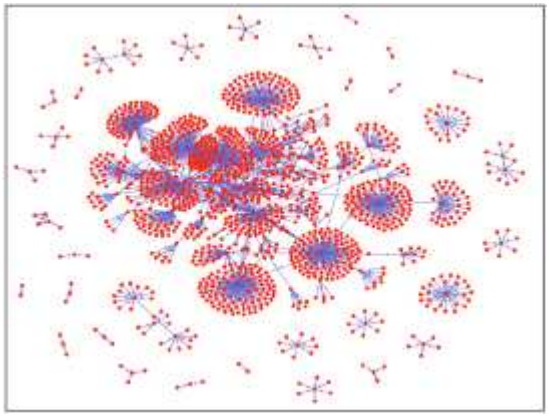

Figura 2 Representación de Webs de Confianza. Fuente [Semantic Web Trust and Security Resource Guide, 2009]

En este sentido un sistema central realiza un seguimiento de los usuarios que generan puntuaciones de cada uno, y utiliza esta puntuación para generar una reputación con respecto a un usuario específico. Estos sistemas requieren de relaciones sociales preexistentes entre los usuarios de su comunidad electrónica, pero lo que no es claro es cómo se establecen esas relaciones y cómo se propagan las calificaciones a través de esta comunidad, lo que ha generado la formalización de algunos proyectos que para nuestro caso nos permite reforzar esta propuesta de trabajo para lograr implementar un sistema de confianza de contenidos digitales sobre una **LCMS** basado en una serie de especificaciones mediante SCORM ó IMS, el cual se comentara a continuación.

4. Modelos de Empaquetamiento de Datos

Existen varios modelos que logran representar el empaquetamiento de contenidos sobre el desarrollo de Objetos de Aprendizaje, los cuáles se pueden resaltar trabajos de grupos de interés a nivel internacional que han permitido determinado una serie de especificaciones para el manejo de contenidos, tal es el caso de SCORM mediante ADL [8],al igual que el consorcio IMS Content Packaging [9] para definición de estructuras de contenidos, IMS Simple Sequencing [10] para la estructuración de contenidos de aprendizaje y la evolución de estos mediante Learning Design [11] e IMS Model Data [12] con el fin de generar una estructura de datos dentro de una representación de diversos escenarios de aprendizaje para su aplicación dentro de diferentes enfoques pedagógicos, elementos propuestos en trabajos realizados por [13].

Dentro del modelo de empaquetamiento de Datos para contenidos sobre plataformas virtuales de aprendizaje LCMS existen referencias las cuáles sirven de base para determinar el funcionamiento de cada uno de ellos, en este sentido nos apoyamos en trabajos realizados a nivel de tesis doctoral por [14] para delinear las especificaciones más importantes basados en el consorcio IMS [15], al igual que SCORM [8],[16], al presentar características acordes a un modelo genérico para la definición de contenidos basados en estándares y especificaciones presentes en el mercado.

Para identificar partes funcionales de cualquier especificación o estándar, es importante resaltar el concepto de Objetos de Aprendizaje desde el punto de vista de la lógica para su desarrollo [17], el cual, resalta la idea de que actualmente este concepto está ligado para representar contenidos reflejados mediante creación de contenidos; por tanto define que actualmente este concepto ha evolucionado para lograr trabajar con objetos de aprendizaje reutilizable RLO (Reusable Learning Object) temas trabajados en su momento bajo recomendaciones dadas por la IEEE en su norma [18] y por el autor [19] para definición de metadatos y elementos válidos para definición de contenidos, los cuales tratan de adaptar en cierta forma al mundo del E-learning para ofrecer un paradigma de programación orientada a objetos en el uso de componentes dentro de las definiciones de la mayoría de especificaciones.

5. Modo de Contemplar Seguridad en Objetos de Aprendizaje

Para implementar objetos virtuales de aprendizaje (LO) que garanticen el uso de contenido ceñido a un conjunto de especificaciones como SCORM ó IMS, deben regirse por lo menos bajo tres elementos: Adaptabilidad, reusabilidad y accesibilidad. Aunque la adaptabilidad actualmente no es soportada completamente por muchos sistemas, de acuerdo a [6], por tal motivo existe plataformas CLMS como es el caso de la plataforma Moodle, el cuál es uno de los CLMS mejores preparados para soportarlo [20], y será en este caso uno de los elementos de mayor representatividad para analizar la seguridad desde el punto de vista de acceso a contenidos mediante SCORM.

Dentro del conjunto de especificaciones SCORM, hay elementos que sirven de partida para trabajar de manera estratégica y adaptar en este sentido a través del empaquetamiento de contenidos la parte de autenticidad de contenidos, el cuál será un parámetro de análisis que depende directamente del lenguaje que se maneje para trabajar autenticidad mediante Firma Digital, para este caso las definiciones dadas por XML que se comentará a continuación.

5.1 Estrategia de Seguridad sobre contenidos mediante XML-Security

A la fecha XML ha sido una iniciativa propuesta por la W3C (World Wide Web Consortium) (originalmente conocido como el comité de revisión editorial de SGML propuesto por IBM) en el año de 1996 y que en el año de 1998 se consolido como estándar, ha sido uno de los aportes más valiosos y significativos a nivel informático para el tratamiento, importación y exportación de datos sobre Internet y sobre cualquier tipo de plataforma informática, lo cual ha permitido generar nuevas alternativas para la distribución de información de manera clara, jerárquica y organizada sobre sistemas informáticos permitiendo ser un estándar para este tipo de procesos; XML Security, dispone de tres elementos representativos que permiten identificar los formatos aptos para el tratamiento de firmas digitales en un sistema de comunicaciones; por un lado las características dadas para la firma digital de documentos dadas por XML-Signature [21], por otro lado a nivel de encripción de datos mediante XML-Encryption Syntax and Processing [22] y finalmente la distribución de claves mediante XML-Key Management [23].

5.1.1 XML-Signature

La especificación dada por XML Digital Signature [22] utiliza tecnologías que a nivel de encripción de contenidos encontramos algoritmos asimétricos y generación de claves mediante funciones HASH, a través de alternativas como SHA1, RSA, entre otras. Bajo estos parámetros de encripción, es necesaria una infraestructura para la distribución de las claves públicas para proveer los elementos válidos de este mecanismo a nivel de identidad y no repudiación.

Las firmas digitales hayan su importancia en el hecho de que proporcionan garantías de integridad de un mensaje punto a punto, además de información de autenticación con respecto a la fuente del mensaje. Para una mayor efectividad, la firma debe ser parte de la información de una aplicación, con lo cual ésta es generada en el momento en el que se crea el mensaje, y de ésta manera verificada en el momento en que el mensaje es finalmente obtenido y procesado.

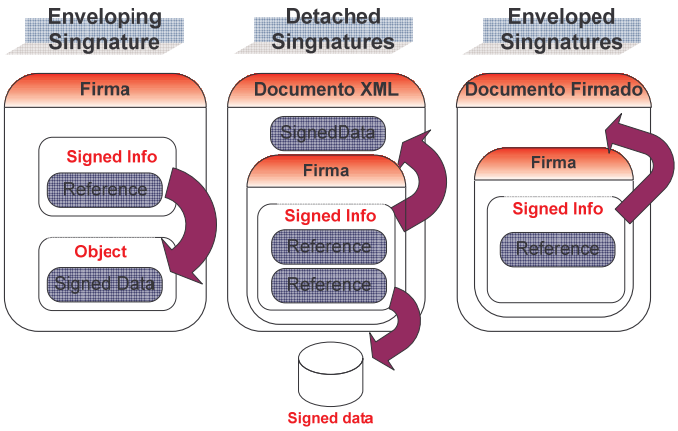

Figura 3 Características de XML Security. Fuente [22]

- ***Enveloping Signature:*** La firma XML envuelve al contenido que se firma.
- ***Detached Signature:*** El objeto que es firmado está separado de la firma XML.
- ***Enveloped Signature:*** El contenido que se desea firmar engloba a la firma.

5.1.2 XML- Encryption

XML- según la [22], describe la manera en que los datos firmados deben ir totalmente cifrados por la Web, con el ánimo de no ser detectados fácilmente por agentes externos dentro del proceso de comunicación, el siguiente esquema es una representación del método usado:

```
<EncryptedData Id? Type? MimeType? Encoding?>
        <EncryptionMethod/>?
        <ds:KeyInfo>
        <EncryptedKey>?
        <AgreementMethod>?
        <ds:KeyName>?
        <ds:RetrievalMethod>?
        <ds:*>?
        </ds:KeyInfo>?
        <CipherData>
        <CipherValue>?
        <CipherReference URI?>?
        </CipherData>
        <EncryptionProperties>?
</EncryptedData>
```

En el Proceso de Encripción y Firma definida por la [22] se identifican los siguientes roles:

- **Aplicación:** La aplicación que realiza la petición de encriptación XML a través de la provisión de datos y parámetros necesarios para su procesamiento.
- **Encriptación:** Una implementación de la Encriptación XML con la función de encriptar los datos.
- **Desencriptar:** Una implementación de la Encriptación XML con la función de desencriptar los datos.

6. Modelo de Seguridad sobre Archivo Manifiesto SCORM

En este sentido para cumplir con estos tres elementos se implementara XML-SECURITY mediante XML-SIGNATURE y XML-ENCRYPTION para tratar de contrarrestar estos problemas. Esta característica va inmersa en el archivo manifiesto mediante la siguiente representación:

Figura 4 Archivo Manifiesto con parámetros de seguridad a nivel de autenticidad de Contenido

Este archivo manifiesto cumple una labor importante dentro del proceso de creación, apertura y búsqueda del objeto de aprendizaje creado dentro de una plataforma LCMS bajo especificación SCORM, ya que permite ser puente para abstraer todas las características dadas por el objeto de aprendizaje, el cuál tiene como propósito resumir todas las características del mismo. Por lo tanto representa el elemento que permitirá identificar y etiquetar el contenido con seguridad apoyado del estándar LOM.

7. Propuesta de Seguridad sobre LOM

El trabajo que realiza LOM en este sentido es ubicar dentro de la etiqueta Derechos las características del tipo de firma que se agrega al contenido, para ello la parte de XML-SECURITY se apoyaría en gran sentido sobre esta

parte del estándar el cuál es la propuesta que se pretende abordar para llevar a cabo esta implementación y se representa a continuación:

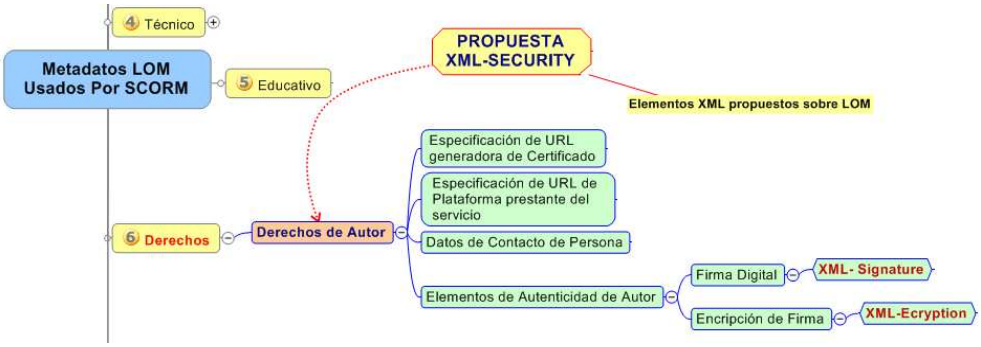

Figura 5 Propuesta de etiquetas de seguridad sobre Elementos de Derechos de Autor en LOM

En este sentido LOM apoyaría en gran medida el proceso de autenticidad de contenidos soportado por esta parte del estándar, pero es una etiqueta que solamente se menciona, mas no se agregan parámetros de seguridad que logren fortalecer la autenticidad del contenido que se genera por parte del autor.

8. Política a Definir dentro de Objetos de Aprendizaje

Para determinar la autenticidad de contenidos dentro de un conjunto de especificaciones a través de SCORM para determinar:

- ¿Quién genera espacios dentro de Plataforma?
- ¿Quién crea contenidos?
- ¿Quién usa contenidos?

9. Modelo de Seguridad de Contenidos Propuesto

El modelo propuesto parte de la representación funcional de las herramientas y elementos que se reflejan dentro del conjunto de especificaciones para contenidos definidos por SCORM. En este sentido a continuación se presenta un modelo genérico de la propuesta que se pretende abordar, los cuáles deben cumplir con los siguientes lineamientos:

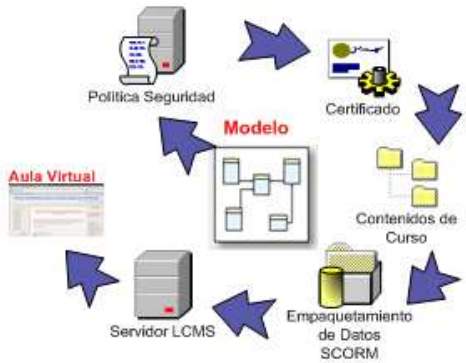

Figura 6 Propuesta de Modelo de Seguridad de Contenidos

Es importante reconocer la idea de la generación del Modelo que se presenta en la anterior figura, este modelo debe estar enmarcada dentro de una política de seguridad, para este caso mediante la representación realizada a través del estándar ISO/IEC 27002 comentado anteriormente, al igual que debe basarse en mecanismos de

seguridad, que para este caso se trabajará mediante certificados a través de una empresa para la generación de firmas realizadas sobre los contenidos que se encuentran regidos bajo un conjunto de especificaciones SCORM y que al mismo tiempo se encuentran sobre una Plataforma Virtual de Aprendizaje LCMS.

Para poder plantear una propuesta que se rija en los anteriores parámetros, es necesario entender la generación del modelo a partir de la representación de cada uno de los roles identificados dentro del proceso de comunicación (Administrador, Docente, Estudiante y/o Invitado). De manera general podemos indicar que el modelo que se propone pretende abordar los siguientes Casos:

Figura 7 Tipos de firmas generadas en una plataformas LCMS

En una plataforma LCMS no es posible medir el nivel de confianza por el numero de firmas, el nivel de confianza del certificador ni tipo de firmas, ya que cada usuario tiene un rol especifico que cambia según el ambiente donde se desempeñe, entendiéndose por ambiente un curso, un foro, etc. Por ejemplo: A la hora de establecer comunicación entre dos usuarios por medio de email interno, uno de ellos puede ser profesor en un aula virtual y alumno en otra. Si el otro usuario tiene las mismas condiciones, y su relación de confianza con el primer usuario es de alumno profesor en un aula, esta relación no se generaliza para toda la plataforma, ya que en otra aula la relación puede ser de alumno - alumno.

En este orden de ideas, los niveles de confianza no funcionan solamente como mecanismos para establecer una comunicación segura en las herramientas de una plataforma como foros, email interno, blogs, etc. si no que pueden servir de apoyo para la gestión de calidad de los objetos de aprendizaje, cursos, foros, etc. Por lo tanto los indicadores de confianza proporcionan una medida para asignar un nivel de confianza a un determinado usuario en un determinado contexto. Luego de enunciarlos el proceso a seguir es asignarle un valor al indicador para evaluar el impacto que tenga sobre el nivel de confianza, esto de acuerdo a las políticas organizacionales que se implemente sobre un LCMS.

10. CONCLUSIONES

Podemos determinar que en el mercado existen una gran cantidad de organizaciones apoyadas por grupos de investigación que se dedican a estandarizar componentes de uso sobre aplicaciones informáticas mediante arquitecturas de seguridad Web, los cuáles logran destacar la importancia del lenguaje XML, como uno de los elementos diferenciadores para garantizar todo proceso de comunicación que se logre gestar dentro de un entorno de trabajo orientado hacia la Web. Por lo tanto se resalta la importancia que grupos como [24], la IETF, la W3C y aportes realizados por autores a nivel investigativo como [14], [16] y otros tantos, resaltan la idea de que mediante las facilidades que nos ofrece XML, podemos plantear un ambiente seguro de comunicaciones para garantizar los procesos de integridad de información, que de manera representativa se ajustan al conjunto de especificaciones

trabajados por SCORM realizando una adaptación al modelo que trabaja para la creación de contenido sobre plataformas LCMS.

Para nuestro caso en particular, SCORM parece tener ventajas significativas sobre el conjunto de especificaciones analizadas, puesto que maneja de manera estratégica dentro de su estructura modular el estándar LOM, el cuál como se comento anteriormente maneja un metadato conocido como Derechos y trata particularmente los derechos intelectuales del objeto de aprendizaje, aunque poco profundo, pero sirve de punto de partida para los propósitos de este proyecto, el cuál solamente se podrá validar dentro del conjunto de especificaciones manejados por SCORM; donde encontramos elementos que sirven de partida para trabajar de manera estratégica y adaptar en este sentido a través del empaquetamiento de contenidos la parte de autenticidad de los objetos de aprendizaje, y al mismo tiempo será un parámetro de análisis que depende directamente del lenguaje que se maneje para trabajar autenticidad mediante Firma Digital, para este caso las definiciones dadas por XML-Security.

Finalmente podemos determinar, que para el planteamiento de mecanismos de seguridad a nivel de autenticidad de contenidos sobre plataformas LCMS, dependen directamente del conjunto de especificaciones que hay en el mercado, pero actualmente no han madurado lo suficiente para poderlas plantear y en ese sentido mejorar este tipo de parámetros. Por tanto dentro de la propuesta realizada es importante determinar que se tendrán en cuenta no solamente una firma digital dentro de un ambiente LCMS, sino que se tendrán en cuenta la validación de contenidos de personas que crean el espacio virtual por parte del administrador, personas encargadas de crear contenidos por parte del profesor y finalmente se generará una firma por parte de la persona que utiliza el material, para este caso el estudiante y/o invitado, lo que genera un nivel de seguridad alto en la procedencia de los contenidos disponibles en un LCMS, logrando plantear en este sentido un concepto sobre este tipo de plataformas que a la fecha se vienen trabajando en las Redes Sociales conocidos como Web of Trust WOT, el cuál permitirá generar un ambiente de trabajo más confiable sobre el material disponible en estos ambientes de aprendizaje.

Referencias

[1] BONEU, J. (2007), "PLATAFORMAS ABIERTAS DE E-LEARNING PARA EL SOPORTE DE CONTENIDOS EDUCATIVOS ABIERTOS". REVISTA DE UNIVERSIDAD Y SOCIEDAD DEL CONOCIMIENTO (RUSC). UNIVERSIDAD OBERTA DE CATALUNYA. 1698-580X. VOL. 4 NRO. I. PG. 36-47, [VIEWED APRIL 2009], HTTP://WWW.UOC.EDU/RUSC/4/1/DT/ESP/BONEU.PDF

[2] RICHARDSON, (2008). CSI: COMPUTER, CRIME & SECURITY SURVEY. COMPUTER SECURITY INSTITUTE. THIRTEEN ANNUAL. PUBLISHED BY COMPUTER SECURE INSTITUTE. [VIEWED MAY 2009] HTTP://WWW.GOCSI.COM/

[3] ZIMMERMANN, H 1980, OSI: OPEN SYSTEM INTERCONNECTION, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 28, NO. 4, PP. 425 - 432.(1980)

[4] SCHILLO, M., & FUNK P. WHO CAN YOU TRUST: DEALING WITH DECEPTION. IN PROCEEDINGS OF THE WORKSHOP DECEPTION, FRAUD AND TRUST IN AGENT SOCIETIES AT THE AUTONOMOUS AGENTS CONFERENCE, PAGES 95-106. (1999).

[5] YENTA, L, & FONER 1997, A MULTI-AGENT, REFERRAL-BASED MATCHMAKING SYSTEM. IN PROCEEDINGS OF THE 1ST INTERNATIONAL CONFERENCE ON AUTONOMOUS AGENTS, PAGES 301-307.

[6] KAREAL, F & KLEMA, J, ADAPTIVITY IN E-LEARNING. IN A. MÉNDEZ-VILAS, A. SOLANO, J. MESA AND J. A. MESA: CURRENT DEVELOPMENTS IN TECHNOLOGY-ASSISTED EDUCATION, VOL. 1, PP. 260-264. (2006)

[7] YU, B 2000, MAHADEVAN VENKATRAMAN, MUNINDAR P. SINGH. AN ADAPTIVE SOCIAL NETWORK FOR INFORMATION ACCESS: THEORETICAL AND EXPERIMENTAL RESULTS.

[8] ADL, [2004], ADVANCED DISTRIBUTED LEARNING. SCORM 2004 SHARABLE CONTENT OBJECT REFERENCE MODEL. [VIEWED APRIL 2009], HTTP://WWW.ADLNET.ORG/PAGES/DEFAULT.ASPX

[9] IMS-CP, 2005, GLOBAL LEARNING CONSORTIUM. IMS CONTENT PACKAGE. VERSION 1.2. PUBLIC DRAFT SPECIFICATION, VIEWED APRIL 2009, HTTP://WWW.IMSGLOBAL.ORG/CONTENT/PACKAGING/INDEX.HTML

[10] IMS-SS, (2003), GLOBAL LEARNING CONSORTIUM. IMS SIMPLE SEQUENCE. VERSION 1.0 FINAL SPECIFICATION, [VIEWED APRIL 2009], HTTP://WWW.IMSGLOBAL.ORG/SIMPLESEQUENCING/INDEX.HTML

[11] IMS-LD, (2003), GLOBAL LEARNING CONSORTIUM. IMS LEARNING DESIGN. VERSION 1. [VIEWED APRIL 2009], HTTP://WWW.IMSGLOBAL.ORG/LEARNINGDESIGN/INDEX.CFM

[12] IMS-MD, (2006), GLOBAL LEARNING CONSORTIUM. IMS META DATA. VERSION 1.3 FINAL. [VIEWED APRIL 2009], HTTP://WWW.IMSGLOBAL.ORG/METADATA/INDEX.HTML

[13] BURGOS, D., TATTERSALL, C., & KOPER, R. HOW TO REPRESENT ADAPTATION IN ELEARNING WITH IMS LEARNING DESIGN. INTERACTIVE LEARNING ENVIRONMENTS, 15(2), 161-170. (2007)

[14] BURGOS, D. DOCTORAL THESIS. ESTUDIO DE LA ESTRUCTURA Y DEL COMPORTAMIENTO DE LAS COMUNIDADES VIRTUALES DE APRENDIZAJE NO FORMAL SOBRE ESTANDARIZACIÓN DEL E-LEARNING. MADRID, ESPAÑA: TESIS DOCTORAL. UNIVERSIDAD EUROPEA DE MADRID. (2006)

[15] IMS-GC, (2009), GLOBAL LEARNING CONSORTIUM. [VIEWED APRIL 2009], HTTP://WWW.IMSGLOBAL.ORG

HTTP://WWW.IMSGLOBAL.ORG/LEARNINGDESIGN/INDEX.CFM

[16] MARQUEZ, J. ESTADO DEL ARTE DEL ELEARNING. IDEAS PARA LA DEFINICIÓN DE UNA PLATAFORMA UNIVERSAL. TRABAJO DE INVESTIGACIÓN DOCTORAL. UNIVERSIDAD DE SEVILLA. DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS. MARZO (2007)

[17] VÉLEZ, J. ARQUITECTURA PARA LA INTEGRACIÓN DE LAS DIMENSIONES DE ADAPTACIÓN EN UN SISTEMA HIPERMEDIA ADAPTATIVO. TRABAJO DE INVESTIGACIÓN DOCTORAL. UNIVERSITAT DE GIRONA. DEPARTAMENT DE ELECTRÒNICA, INFORMÀTICA I AUTOMÀTICA. MARZO (2007)

[18] LTSC. (2002). LEARNING TECHNOLOGY STANDARDS COMMITTEE. DRAFT STANDARD FOR LEARNING OBJECT METADATA. IEEE STANDARD 1484.12.1, NEW YORK: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, [VIEWED APRIL 2009] HTTP://LTSC.IEEE.ORG/WG12/20020612-FINAL-LOM-DRAFT.HTML

[19] WILEY D. & EDWARDS K. ONLINE SELF-ORGANIZING SOCIAL SYSTEMS: THE DECENTRALIZED FUTURE OF ONLINE LEARNING. QUARTERLY REVIEW OF DISTANCE EDUCATION, 3:33–46. (2002)

[20] SANTOS, O.C. TECHNOLOGY ENHANCED LIFE LONG ELEARNING FOR ALL. IN K. MAILLET AND R. KLAMMA: PROCEEDINGS FOR THE 1ST DOCTORAL CONSORTIUM ON TECHNOLOGY ENHANCED LEARNING. EUROPEAN CONFERENCE ON TECHNOLOGY ENHANCED LEARNING, P.66-71, (2006).

[21] W3C- SIGN. (2008). XML SIGNATURE SYNTAX AND PROCESSING (SECOND EDITION). W3C RECOMMENDATION 10 JUNE 2008. VIEWED MAY 2009, HTTP://WWW.W3.ORG/TR/XMLDSIG-CORE/

[22] W3C-ENC. (2002). XML ENCRYPTION SYNTAX AND PROCESSING. W3C RECOMMENDATION 10 DECEMBER 2002 VIEWED MAY 2009, HTTP://WWW.W3.ORG/TR/XMLENC-CORE/

[23] W3C-KEY, (2001). XML KEY MANAGEMENT SPECIFICATION (XKMS). W3C NOTE 30 MARCH 2001 [VIEWED MAY 2009]. HTTP://WWW.W3.ORG/2001/XKMS/

[24] OASIS,(2009), ADVANCING OPEN STANDARDS FOR THE INFORMATION SOCIETY, [VIEWED MAY 2009] HTTP://WWW.OASIS-OPEN.ORG/HOME/INDEX.PHP

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.