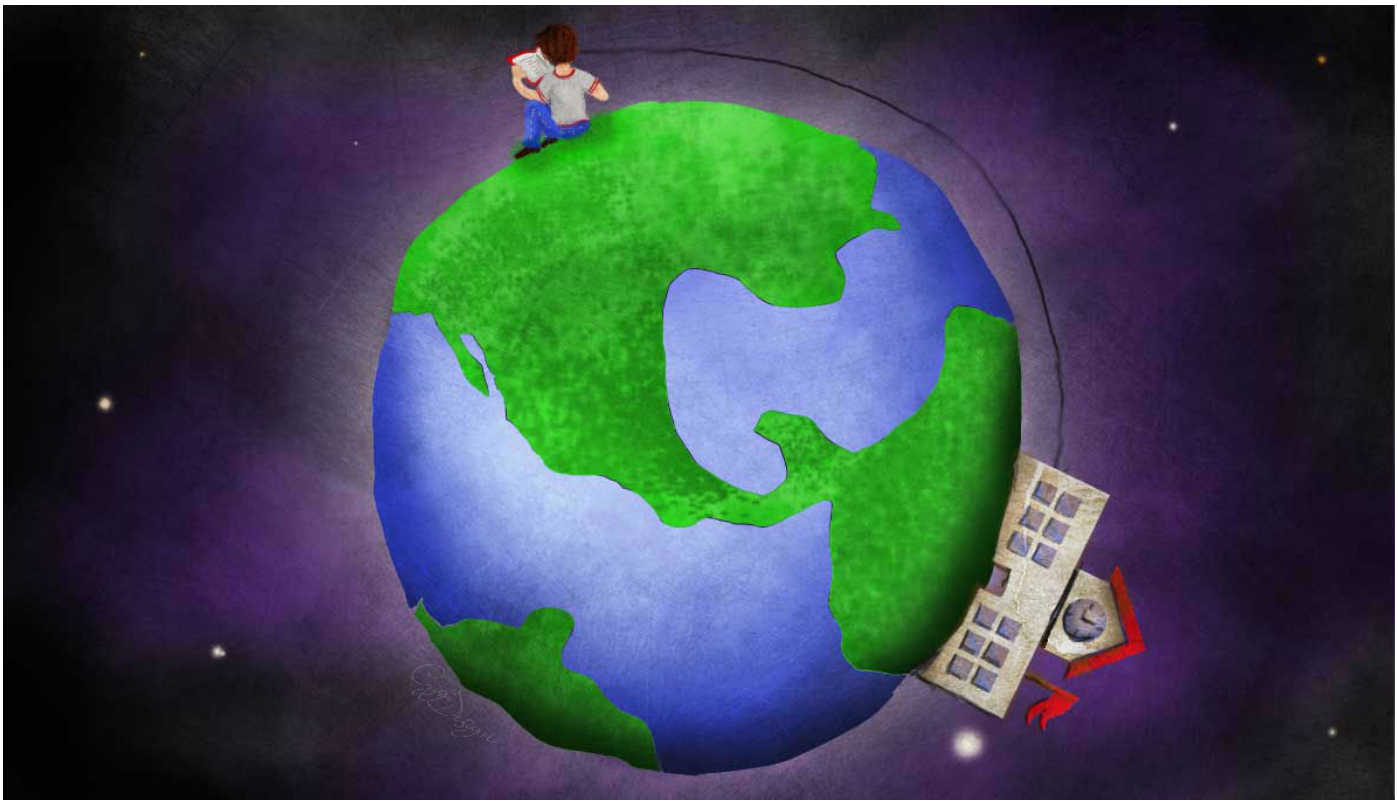
Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

CIBERSEGURIDAD PARA LA EDUCACIÓN ONLINE

Galvy Ilvey Cruz Valencia

ciberseguridad

numero-22



La demanda educativa en muchos países alrededor de mundo ha provocado que la educación a distancia, o la también llamada educación *online* o *e-learning*, sea una opción para miles de estudiantes. Esta condición ha marcado la necesidad de desarrollar plataformas cada vez mejores, que

respondan a procesos formativos o de aprendizaje para lograr un propósito de éxito concreto entre estos particulares usuarios.

Ahora bien, si los recursos y posibilidades de estudio están dados, también es verdad que representan una oportunidad para los ataques cibernéticos. El ciberfraude y el robo de identidad, entre otros problemas de seguridad, no deben pasar por alto.

Dos analistas reconocidos en este tema específico son los académicos de la Nova Southeastearn University, Yair Levy y Michelle Ramim, quienes en 2006 publicaron el artículo *Seguridad en sistemas E-learning: Un caso de operaciones de ciberataques y administradores novatos de TI en una pequeña universidad*, el cual revela que las operaciones de ciberataques pueden darse tanto por la falta de políticas de tecnologías de información como por la ausencia de procesos para la contención de daños en las plataformas de educación en línea.

Pero, ¿qué es una plataforma *e-learning*, cómo opera y qué parámetros debemos tomar en cuenta para cuidar la seguridad en ésta?

Una plataforma de este tipo consiste en un conjunto de recursos informáticos y web dispuestos para obtener conocimientos a distancia. Se basa en una serie de aplicaciones y contenidos accesibles a través de la computadora en la que forzosamente el usuario debe autenticarse para ingresar a la red.

Una vez que el usuario o participante ha ingresado a su cuenta personalizada (mediante un usuario y contraseña comunmente), accede a *cursos* configurados a través de sesiones o módulos.
Desde esta perspectiva, sobresale que estas plataformas son capaces de desarrollar y producir conocimiento mediante un aprendizaje, si bien puede darse de manera presencial, lo es sobre todo a la distancia; y es aquí donde conviene hacer una revisión acerca de cómo es posible.

LAS PLATAFORMAS PASO A PASO

Para revisar la arquitectura e ingeniería de las plataformas, debemos comenzar en primer término con su modelo, el cual está supeditado al dominio lógico antes que pedagógico; es decir, se trata de modelos más orientados a atraer la atención de los usuarios que a atender los problemas relacionados a escenarios pedagógicos, ya sea que estén planteados por su concepción, por su representación o por su planificación de actividades.

El segundo se refiere a las capacidades, aplicaciones y extensiones que pueden incorporar estas plataformas a fin de lograr sus objetivos pedagógicos; y más aún al interés que despiertan estos recursos informáticos para desarrollar contenidos y conocimientos que puedan dominar los usuarios, haciendo énfasis en que esto no es algo reducido, sino realmente exponencial.

El tercer aspecto a considerar acerca de estas plataformas se centra en un punto que acapara, en gran parte, la atención de este artículo: la utilización. Los problemas radican principalmente en la naturaleza convergente de disciplinas, pues pasa por el análisis de procesos de ejecución, el impacto de los contenidos, la organización de los módulos o sesiones y las acciones realizadas por los usuarios, las cuales hacen realmente la diferencia.

Si nos concentramos en caso de Moodle*[1]* sobresale el hecho de que se trata de una plataforma de características LAMP; cuyas siglas provienen, según señala Fernández [1] de la combinación de “Linux + Apache + Mysql +PHP. LAMP se ha convertido en uno de los ejes vertebrales de los servicios que pueden encontrarse en Internet”.

De la descripción de Fernández sobresale un aspecto de seguridad en la configuración que no puede

pasarse por alto: El servidor Apache concentra la gestión de páginas HTML; aunque vale la pena agregar que estas plataformas también pueden alojarse en sistemas Windows. Según señala Fernández, es necesario instalar una Socket Security Layer (SSL, también conocida como HTTPS) a fin de que las sesiones de los usuarios no se transfieran en modo abierto, esto sin duda nos llevará a la pregunta concreta:

¿QUÉ HACER POR LA SEGURIDAD DE LAS PLATAFORMAS EDUCATIVAS EN LÍNEA?

Como todo sistema, desde el punto de vista de seguridad, las plataformas LAMP requieren evaluar aspectos internos y externos para garantizar su funcionalidad, según señalan Kouninef, Djelti y Rerbal [2].

Entre los principales criterios internos que los desarrolladores deben verificar en primera instancia, es que estamos frente a una plataforma con necesidades de mantenimiento, y dado que esto depende estrictamente de los administradores, los usuarios están destinados a recurrir a respaldos continuos de información, sobre todo ante la posibilidad de un “apagón”.

Plantear la seguridad de la plataforma desde un punto puramente informático, como filtros de IP que tendrán acceso al curso con autorización por medio del ingreso de credenciales (usuario/contraseña), nos llevará a no entender las posibilidades de riesgo en su totalidad.

Por ejemplo, causar una posible denegación de servicio por el número de solicitudes múltiples si no se tiene contemplado en el desarrollo la cantidad máxima de usuarios que podría soportar la plataforma. O un usuario con intenciones maliciosas que sube un archivo infectado, si éste es descargado por un usuario administrador, ¿cómo garantizar que no hay posibilidades de propagación?

Una de las posibilidades de incrementar las condiciones de seguridad es realizar, en cada uno de los lenguajes de programación utilizados, una rutina de actualización que permita lograr una evolución favorable del sistema y de su capacidad actual.

Otro aspecto interno es el relacionado con la gestión de envío de correos electrónicos a los distintos participantes en el curso *online*. Debemos garantizar, por un lado, la correcta distribución en las libretas de direcciones, y por el otro, los receptores deben verificar la autenticidad de los emisores; recordemos que hay posibilidades de enmascaramiento que podrían llevar a recibir correos falsos, limitando las posibilidades de generar grupos de discusión.

Ahora revisemos los aspectos externos, los cuales podemos dividir en dos partes, aquellos que van propiamente de lado del ambiente del sistema y otro muy particular sobre el uso del sistema, lo cual involucra directamente al usuario.

En el primer caso, es preciso recordar que las plataformas funcionan en un medio y que este medio conlleva sus propios riesgos de seguridad. Por mencionar algo específico, consideremos los riesgos del navegador web y los problemas asociados a la viralidad de contenidos en aplicaciones de redes sociales como Facebook, YouTube y Twitter.

En el segundo caso, podemos evocar la extensa documentación que Levy [3] realizó en 2008, en la cual enlistó las 36 actividades que los estudiantes de plataformas *e-learning* consideran más valiosas durante su experiencia formativa, concluyendo que muchas de éstas podrían comprometer al sistema.

Por considerar algunas:

a) Alteración de contenidos del curso
b) Distribución de contenidos maliciosos
c) Cambios no autorizados
d) Alteración de calificaciones
e) Destrucción de bases de datos
f) Robo de identidad

A esto, es necesario sumar que el entorno ofrece riesgos como:

a) El *spam*, es decir, correo basura.
b) *Phishing*, sitios falsos dedicados al robo de credenciales de acceso.
c) *Spyware*, software malicioso para recabar información del usuario e instalar publicidad molestosa sin consentimiento del usuario.
d) *Malware*, software creado con la intención de robar información o dañar la computadora.
e) Los *crackers*, expertos informáticos dedicados a intervenir los sistemas con propósitos malintencionados.

Si esto pareciera ya muy extenso, los expertos de Nova Southeastern University van más allá, en 2007 [4] ofrecieron la plática ¿Quién presenta realmente el examen?, en la cual presentaban un punto crítico, ya no sólo de la seguridad informática, sino de la seguridad de la información, arguyendo que los opositores a esta modalidad de estudio justifican su postura respecto a la inoperatividad para autentificar al usuario que realiza las actividades y evaluaciones en las plataformas, por lo que el futuro de las plataformas pasará por las posibilidades de autentificación que hoy por hoy ofrecen las TIC, tales como la biometría; a fin de superar la mera autentificación con usuario y contraseña, como comúnmente se hace.

Finalmente, en cuanto a plataformas de *e-learning* se refiere, parece que la conducta ética de administradores, docentes y usuarios será determinante para la operatividad y concreción de propuestas educativas de esta naturaleza, atendiendo con sumo cuidado al hecho de que estas dinámicas están creciendo y respondiendo a necesidades educativas de un sector de la población caracterizado por su nivel educativo y adquisitivo; dos factores que se combinan en una suerte de gran atractivo para los delincuentes cibernéticos, por lo que indudablemente nos habituaremos a leer más

acerca de estos temas.

---

[1] En palabras de Fernández, 2005, p.87: *Modular Object - Oriented Dynamic Learning Environment* (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular). sobresale el hecho de que se trata de una plataforma de características LAMP; cuyas siglas provienen, según señala Fernández [1] de la combinación de “Linux + Apache + Mysql +PHP. LAMP se ha convertido en uno de los ejes vertebrales de los servicios que pueden encontrarse en Internet”.

Si quieres saber más consulta:

- Sugerencias de Seguridad para Sitios Web
- Aspectos Básicos de la Seguridad en Aplicaciones Web
- El Cifrado Web (SSL/TLS)

REFERENCIAS

[1] Fernández, J. (2005). La hora del e-aprendizaje. La plataforma educativa Moodle. Recuperado el 22 de junio de 2014, desde https://www.linux-magazine.es/issue/13/Educacion.pdf.
[2] Kouninef, B., Djelti, M. y Rerbal, S. (2007). Conception et réalisation d’une plate forme e-learning avec une migration au m-learning. Recuperado el 22 de junio de 2014, desde http://www.resatice.org/jour2007/communications/b-kouninef.pdf.
[3] Levy, Y. & Ramim, M. (2006). Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. Recuperado el 20 de junio de 2014, desde http://www.irma-international.org/viewtitle/3187/.
[4] Levy, Y. & Ramim, M. (2007). Who is really taking the e-exam? What can we do about it? Nova Southeastern University, Recuperado el 20 de junio de 2014, desde http://bit.ly/1vuf4mk.
Levy, Y. & Ramim, M. (2009). Initial Development of a Learners’ Ratified Acceptance of Multibiometrics Intentions Model (RAMIM). Recuperado el 21 de junio de 2014, desde http://www.ijello.org/Volume5/IJELLOv5p379-397Levy672.pdf.
