La seguridad informática en las plataformas educativas que se utilizan en el nivel superior: una tarea pendiente

Data security in education platforms used in higher education: a pending task

Hugo Alberto Quiroz
Martínez Escobar,
Universidad del Valle de México,
México
hugh_draco@hotmail.com

David Alfredo Domínguez Pérez,
Universidad del Valle de México,
México
alfredodom07@yahoo.com.mx

María Natalia Pérez Rul
Universidad Nacional Autónoma de
México, México
licrul@yahoo.com

Recibido 15, octubre, 2015

Aceptado 27, noviembre, 2015

Resumen

En este mundo globalizado, cada vez más personas y organizaciones realizan sus actividades utilizando las tecnologías de la información; derivado de ello han surgido ambientes de educación a distancia que a través de herramientas informáticas y mediante el apoyo de plataformas educativas, trasladan todas las actividades de aula a un ambiente virtual. Pero su desarrollo e implementación se ha centrado más en la capacidad y velocidad que en la integridad de los datos que custodian, por lo que en este trabajo cuestionamos el tema de la vulnerabilidad, ya que al no contar con certificaciones que avalen la seguridad, estos ambientes virtuales son sensibles a sufrir ataques que busquen dañar o robar información. Para ello, con base en la Norma ISO/IEC 27007:2011, se realiza una auditoría de seguridad de la información a una plataforma educativa en una institución de nivel superior con modalidades presencial, mixto y en línea, que utiliza la herramienta Blackboard como soporte de sus materias en línea; se exponen los resultados y se dan recomendaciones pertinentes.

Palabras clave: seguridad informática, plataforma educativa, auditoría informática, nivel superior

Abstract

In this globalized world, more people and more organizations do their activities by constantly using information technologies. As a consequence, distance learning environments have emerged. Through them all the activities of a classroom have been moved to a virtual environment by using information tools and educational platforms, where speed and capacity are usually put over the safeguard integrity of data. Therefore, in this article we point out that the absence of a certification regarding information security remain virtual environments vulnerable to damage or information theft. Based on the ISO/IEC 27007:2011 norm, an information security audit was conducted to the platform used in a higher education institute that offers three educational modalities: in person, online and mixed. The platform uses the Blackboard platform as support for its online courses and subjects. The results and recommendations from the audit are reported in this article.

Keywords: *information security, educational platform, computer audit, higher education*

Introducción

En México la educación superior se ofrece en diversas modalidades; la presencial, donde el alumno asiste a las aulas todas las sesiones; la mixta, donde el alumno cursa parte del programa de estudios de manera presencial y otras materias en línea; el formato blended donde el alumno combina materias de forma presencial y en línea y por último, el modo virtual, donde todas las materias se cursan en internet; todas estas materias en línea requieren de una plataforma educativa.

El sistema educativo ha tenido que adecuarse al nuevo perfil de estudiantes que se caracterizan por tener limitados tiempos para traslados, largas jornadas laborales y responsabilidades familiares, para lo cual las instituciones ponen a su disposición plataformas educativas que pueden ser de: desarrollo propio (Cadel), de libre acceso (Moodle) o comercial (Blackboard). La plataforma utilizada dependerá de las necesidades que tenga la institución educativa en función al número de programas (carreras), materias a cursar, alumnos y tutores que se registrarán y que interactuarán entre sí y de los cuales se generará información como el número de profesor, matrícula del estudiante, número de materias a impartir o realizar, que concuerden con su programa de estudio, calificaciones, trabajos enviados, foros, etc.; por la cual la herramienta requiere de ciertos candados para su acceso.

En ninguna institución educativa se minimizan los posibles riesgos por la vulneración de su seguridad informática, debido a que no existen parámetros o certificaciones SSL (capa de conexión segura o incluso la ISO 27000 que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización sea pública o privada, no importando su tamaño sea grande o pequeña), que se deban cotejar con el proveedor de la plataforma educativa, ya sea cuando la contratan o cuando la desarrollan y esto hace que se encuentren expuestas, ya que están más preocupadas porque funcione, por la carga máxima que va a soportar, los tiempos de respuesta o en la operación (generando manuales para maestros y alumnos de cómo trabajar con la plataforma).

La vulnerabilidad en las plataformas de la educación en línea se hace más evidente y por ello es indispensable que éstas cuenten con políticas y certificados de seguridad; que se conozcan las barreras lógicas instaladas para el resguardo de la información, que se identifique y establezca con qué frecuencia se realizan auditorías informáticas para verificar tanto la seguridad de las plataformas, así como los planes de contingencia y de recuperación de información en caso de un siniestro. Lo recomendable es que este conjunto de medidas sean normadas por la propia Secretaría de Educación Pública para crear un estándar de control de las diferentes instituciones educativas que oferten aprendizaje virtual en cualquiera de sus modalidades con el fin de proteger los datos personales y generar mayor confiabilidad para los usuarios.

En las instituciones de educación superior siempre se mencionan las bondades del por qué estudiar en línea así como las ventajas del tipo de plataforma que se usa, pero no se mencionan los estándares de control de seguridad informática. Al momento de llevar la investigación se desconoce si existen políticas de seguridad en aquellas herramientas en donde el alumno plenamente confía que sus datos están bajo seguridad.

Desarrollo

Seguridad informática, el nuevo reto

García-Cervigón (2011) considera que la seguridad es un elemento primordial en los sistemas informáticos actuales. Ésta se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático. Dentro de la seguridad informática podemos encontrar elementos y técnicas como hardware, software, dispositivos físicos y medios humanos. Royer (2004) en cambio, considera a la seguridad informática como «la protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo».

Para Areitio (2004), la cada vez más dominante tendencia hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones, e incluso de las empresas, ha situado a la seguridad de los sistemas de información como un elemento central en todo el proceso de desarrollo de la sociedad. La seguridad ha pasado de utilizarse para preservar datos clasificados del gobierno, a tener una aplicación de dimensiones inimaginables y crecientes que va desde transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por internet hasta domótica, inteligencia ambiental y computación ubicua. Por ello, es imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.

Royer (2004) considera que proteger el sistema informático consiste en poner frenos contra cada una de las amenazas potenciales; y dado que ninguna protección es infalible, es necesario multiplicar las barreras sucesivas. Para De Pablos (2004) la creciente dependencia de las empresas y de la sociedad en general, de las tecnologías de la información y de las comunicaciones, así como el entorno cada vez más complejo en que estas se desarrollan, ha provocado la aparición de vulnerabilidades en los recursos utilizados que las organizaciones deben minimizar con las

medidas de seguridad oportunas. Son muchos los riesgos y los ataques a los que una compañía tiene que hacer frente: intentos de entrada en los sistemas de información tanto desde el interior como el exterior de la organización; fisgones y piratas informáticos; pérdidas, robos, destrucción o daño de datos; control ajeno y no autorizado de los equipos y recursos a través de programas espías; correo basura; ocupación de direcciones; desvío de información; espionaje industrial; desvío de dinero y virus informáticos.

Ramos (2004) menciona que en internet hay millones de interlocutores que acceden desde terminales con direcciones fijas o variables en el tiempo, que son expuestas extremo a extremo u ocultadas tras intermediarios. De forma manual o mediante herramientas automatizadas pueden tener acceso a recursos y difunden información mediante distintos sistemas de comunicación. En ocasiones precisa aportar información que vincule al origen, y en muchos casos, su identificación es una acción costosa.

El potencial de la red para conectar con otras personas permite plantear actividades que en otros ámbitos no resultarían económicamente viables. Apoyándose en técnicas que faciliten el anonimato o simplemente reiterando la utilización de las que permiten los sistemas y protocolos de internet, se intenta captar clientes rentables ante el coste ínfimo de «la red». Pero también hay otros objetivos, desde fraudes importantes o degradaciones que no deben dejarse de lado (Ramos 2004).

En la actualidad, las aplicaciones y los dispositivos operan maximizando el uso de las infraestructuras de las redes. Los enormes anchos de banda han permitido un comportamiento de los usuarios como suministradores y como demandantes de archivos e información. Esta proliferación ha sesgado las métricas de la palabra «fiabilidad».

Aprendizaje virtual y plataformas educativas a nivel superior

Con la evolución y uso de las tecnologías de la información y comunicación, se han acuñado nuevos conceptos y términos que tienen que ver con lo «electrónico» o lo «virtual». En cuanto al aprendizaje se habla del aprendizaje electrónico (*e-learning*), aprendizaje en línea (*on line*), aprendizaje digital, enseñanza interactiva, educación a distancia, aulas virtuales, entre otros conceptos.

Bernandez (2007) define al aprendizaje virtual como todas aquellas metodologías, estrategias o sistemas de aprendizaje que emplean tecnología digital y/o comunicación mediada por ordenadores para producir, transmitir, distribuir y organizar el conocimiento entre individuos, comunidades y organizaciones. Uno de los avances más importantes en el desarrollo de *e-learning* es la aparición de los sistemas que proveen en una misma plataforma diversos recursos para la interacción, actividades de aprendizaje, presentación de contenidos y gestión de alumnos.

Por otro lado, García (2003) comenta que el *e-learning* hace referencia a la enseñanza y aprendizaje, individual o colectivo, haciendo uso de las nuevas TIC (video conferencia, satélite, Internet, etc.) pero incluye también otras opciones como la radio, televisión, video, entre otras, para flexibilizar los procesos de aprendizaje.

Barberá (2008) establece que los componentes del *e-learning* se hallan distribuidos en distintos entes: alumnos que aprenden, materiales de estudio, programa informático que utiliza, institución titular de los cursos, etcétera. La arquitectura de internet hace posible que los estudiantes, el profesor y el centro docente estén en lugares distintos, por lo que el punto de encuentro es una plataforma tecnológica a la que se puede acceder desde cualquier ordenador conectado a la red en parte del mundo; y es que la aplicación de las TIC a los procesos de enseñanza y aprendizaje se han visto plasmados en los entornos virtuales de enseñanza y aprendizaje que se apoyan en sistemas informáticos basados en el protocolo *world wide web* (Arratía, 2009).

Un sistema de aprendizaje virtual está compuesto de a) un área de instrucción e interacción con los alumnos (*ILS-integrated learning system*), que incluye diversas herramientas para el aprendizaje asincrónico y sincrónico, tales como correo electrónico, chat, aula virtual, foros de discusión y áreas de presentación y acceso a contenidos y ejercicios, b) un área de gestión de contenidos (LCMS), que almacena y conecta contenidos en módulos reutilizables y c) un área de gestión de alumnos (LMS), que lleva registro de la situación de cada estudiante en términos de aprendizaje, participación y revista. Sierra (2008) a partir de sus investigaciones, considera que los principales obstáculos y problemas con los que se enfrenta el aprendizaje virtual, no son de nivel tecnológico o infraestructural, sino en su auténtica dimensión pedagógica, como espacio/herramienta para el proceso educativo y el aprendizaje.

Silva (2011) comenta que, actualmente, algunas plataformas están estandarizadas, mientras que otras son completamente personalizadas. Las plataformas estandarizadas ofrecen herramientas genéricas que permiten la adaptación a la situación del profesor o institución que diseña un espacio virtual. Existen las plataformas comerciales (*WebCT, FirstClass, LearningSpace, Blackboard*) y las plataformas de código abierto (*ATutor, Moodle, LRN, Claroline, Drupal*). Ciertas organizaciones han preferido desarrollar sus plataformas propias donde intentan dar una respuesta específica a sus necesidades técnicas (personalizadas).

Tabla 1: Plataformas educativas de algunas instituciones de educación a nivel superior en México

Plataforma	Institución	Tipo de cursos	Página web	Licencia
Tec Virtual <i>Blackboard</i>	Tecnológico de Monterrey	Educación continua Posgrados	http://alumnos.tecvirtual.itesm.mx/ http://miscursos.itesm.mx/	<i>Blackboard</i>
CADEL	Universidad del Valle de México (hasta 2013)	Licenciatura ejecutiva	http://www.uvm.edu.mx/cadel	Desarrollo propio
<i>Blackboard</i>	Universidad del Valle de México	Licenciatura tradicional Licenciatura ejecutiva Posgrado Cursos y certificaciones	https://uvmonline.Blackboard.com/	Licencia comercial
PoliVirtual	Instituto Politécnico Nacional	Bachillerato Licenciatura Posgrado Educación continua	http://www.aulapolivirtual.ipn.mx/	Desarrollo propio con base en <i>Moodle</i>

Plataforma	Institución	Tipo de cursos	Página web	Licencia
SUAyED Campus Virtual	Universidad Nacional Autónoma de México	Bachillerato Licenciatura Especialidades Posgrados Doctorados Educación continua	Campus Virtual http://suayed.unam.mx/index.php Aulas Virtuales http://aulasvirtuales.cuaed.unam.mx/index.php	Desarrollo propio con base <i>Moodle</i> aulas virtuales con <i>Blackboard</i> y <i>BigBlueButton</i>
Moodle	Instituto Tecnológico Autónomo de México	Educación continua	http://deude.itam.mx/moodle/	Código abierto
<i>Blackboard</i>	Universidad Anáhuac	Cursos Diplomados Maestrías	http://anahuac.blackboard.com	Licencia comercial
Virtu@mi	Universidad Autónoma Metropolitana	Diplomados Posgrados	http://virtuami.izt.uam.mx/aulas/apresencial/login/index.php	<i>Moodle</i>

Fuente: elaboración propia

Evolución de los entornos virtuales de aprendizaje

Gómez (2005) expresa que si buscamos en internet nos encontraremos con plataformas desarrolladas por usuarios entusiastas del medio, que con pocos recursos consiguen buenos resultados; bien porque crean su propia plataforma adaptada al propio entorno, o porque saben sacarle el mejor de los resultados a un conjunto de herramientas facilitadas por el proveedor de acceso a internet. Nos encontraremos también con plataformas profesionales e inalcanzables para el habitualmente escaso presupuesto de un único centro y que están orientadas a dar soporte a entornos académicos más complejos, que permiten gestionar cientos de cursos y alumnos. Y por último, y no menos interesantes, también encontraremos desarrollos profesionales basados en licencias de software de difusión gratuita (Universidad NaciED, 2011).

Un entorno virtual de aprendizaje (EVA), en algunos casos denominado también entorno virtual de enseñanza/aprendizaje (EVE/A) es una aplicación informática diseñada para facilitar la comunicación pedagógica entre los participantes en un proceso educativo, sea éste completamente a distancia, presencial, o de una naturaleza mixta que combine ambas modalidades en diversas proporciones (Adelle, Castellet y Pascual, 2004). En un entorno virtual de aprendizaje se combinan herramientas para la comunicación síncrona y asíncrona, para la gestión de los materiales de aprendizaje, para la gestión de las personas participantes, incluidos sistemas de seguimiento y evaluación del progreso de los estudiantes, ofreciendo desde el punto de vista didáctico, soporte tecnológico a profesores y estudiantes para optimizar distintas fases del proceso de enseñanza y aprendizaje, planificación, implementación, desarrollo y evaluación del currículum (Areito, 2007).

Silva (2011) comenta que a pesar de las bondades de los EVA, es necesario afirmar que la adopción de un EVE/A no garantiza la innovación ni la mejoría de la calidad de enseñanza; esto es porque los diseños de los espacios virtuales de aprendizaje responden a las concepciones del proceso

de enseñanza-aprendizaje que adscriben quienes los diseñan, siendo perfectamente posible utilizar estos espacios para implementar ambientes de aprendizaje que respondan a modelos cognitivos en lugar de constructivos.

Las comunidades virtuales

Las comunidades en línea han estado en la base del desarrollo de internet. En un inicio, estas comunidades aglutinaron a profesionales y agrupaciones de profesionales, que utilizaban la red para extender los lazos al interior de sus comunidades profesionales. Con el desarrollo de internet y la masificación de su uso, estas comunidades se ampliaron a ámbitos como el ocio y la formación. Hoy en día, los espacios virtuales y las herramientas para la comunicación que estos proveen pueden ser utilizados más allá de las instancias formativas regladas como en un curso, surgiendo las comunidades de aprendizaje online para mantener diálogo respecto a determinados temas (Silva, 2011).

Barberá (2008) señala que las comunidades virtuales de aprendizaje se caracterizan por la construcción inicial de una comunidad de aprendizaje; sus miembros están dispuestos a compartir y hacer crecer el conocimiento en los temas predefinidos; existen finalidades y objetivos compartidos; se focalizan en los procesos de enseñanza y aprendizaje y existe comunicación e interacción entre sus miembros; se distribuyen los roles y existe un control de la actividad distribuido entre todos los miembros y necesitan transformarse para tener continuidad a lo largo del tiempo.

Plataformas de formación online

Para dar vida a un entorno virtual de aprendizaje, EVA, se requiere contar con una plataforma para el aprendizaje online o Learning Manager System, LMS, un sistema integral de gestión, distribución, control y seguimiento de contenidos y recursos educativos en un entorno compartido de colaboración. Debe contener o permitir integrar herramientas de producción de recursos, comunicación entre profesores, profesores y alumnos y entre los propios alumnos en tiempo real y diferido, administración, gestión de cursos y agentes, creación de grupos de trabajo y comunidades de aprendizaje (Silva, 2011).

En la actualidad, las plataformas se han dividido en dos tipos: estandarizadas y personalizadas. Las plataformas estandarizadas permiten la adaptación a cierto nivel de algunas situaciones en concreto y ofrecen herramientas de tipo genéricas. Se encuentran las plataformas comerciales y las plataformas de código abierto. Las plataformas personalizadas son desarrollos propios de algunas instituciones que intentan dar una respuesta a sus propias y muy específicas necesidades. A través de aplicaciones es como se desarrollan, gestionan y diseñan plataformas educativas donde una organización (centro educativo, universidad, empresa, persona) administra aquellos recursos educativos que controla el profesor, el acceso a los estudiantes, la comunicación y los medios de comunicación que habrá. Herramientas de gestión de grupos y usuarios, asignación y creación de cursos y perfiles de usuario con información personal.

Las principales herramientas con que cuentan estas plataformas son: a) foros de discusión de tópicos, donde a través de respuestas se realiza una discusión entre los integrantes; b) glosario de términos para profundizar en algunos conceptos técnicos muy especializados y manejados a

lo largo del curso o uso de la plataforma; c) recursos o material didáctico que son los contenidos temáticos y actividades a realizar, abordados de diferentes maneras mediante el uso de software comercial ofimático, videos, lecturas, entre otras; d) cuestionarios para desarrollar test de opción múltiple, verdadero y falso o preguntas abiertas para evaluar temas o proponer encuestas; e) tareas para desarrollar casos, problemas o temas abiertos que incluyen la forma de gestión de contenido con las opciones de subida y vista de archivos; f) aulas o chat comunitario para que exista una interacción entre integrantes en temas específicos y g) anuncios para dar a conocer temas relevantes como son la bienvenida, avisos o cierres.

Diseño de un entorno virtual de aprendizaje

Para Silva (2011) el diseño de un EVA considera una serie de acciones que se desarrollan en cierto paralelismo dada su complementariedad. Es un proceso que en muchas ocasiones requiere volver a etapas o pasos anteriores y ajustarlos para que el diseño sea un todo armónico y coherente. El diseño puede ser realizado en su totalidad por un profesional especializado, por un tutor, o docente o, como en la mayoría de los casos, por la unidad de virtualización de una institución de docencia o de una empresa. Cuando se diseñan cursos, normalmente se trata de incluir a expertos en las áreas técnica, pedagógica y de diseño gráfico de interfaz. En las universidades que manejan la educación a distancia o *e-learning* como forma de educación se requiere de expertos en diseño instruccional en línea, manejo de las tecnologías de la información y comunicación y plataformas de formación.

Navegando en la internet y un entorno virtual de aprendizaje

Gómez (2005) comenta que una de las primeras fases que se deben mostrar al abordar el uso de las plataformas en sus quehaceres virtuales es la experimentación con el aspecto del ordenador que se va a utilizar y el proceso de inicializar la plataforma. Las advertencias sobre los riesgos de virus, carecer de antivirus adecuados, certificados vencidos o, el simple hecho de tener que aceptar o rechazar una ventana emergente o un *add-on* puede alarmar a un usuario hasta el punto que puede prescindir del uso de las tecnologías.

Auditoría informática

Cada día un número mayor de empresas y organizaciones considera que la información representa uno de sus activos más importantes; así como toda la tecnología lógica y física asociada a la gestión, entrada, almacenamiento y salida de dicha información. Esta categorización conlleva a que los requerimientos de calidad, controles, seguridad y disponibilidad de la información sean indispensables; así como a cualquier otro activo de la empresa. La auditoría informática se encarga de comprobar la existencia y aplicación de los mencionados anteriormente.

La auditoría persigue como su objetivo primordial realizar una evaluación de las actividades ejecutadas en la organización a fin de verificar que cada una de ellas como unidad y todas en conjunto contribuyen a fortalecer el alcance del mejor de los resultados posibles: esto implica la detección de las debilidades y la identificación de amenazas con una definición clara de las causas de estas situaciones (Delgado, 1998). Chicano (2014) define a la auditoría informática como el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse. Para Rivas (2008), la auditoría informática

es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de forma puntual y de modo discontinuo, a diferentes instancias, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados. De Pablos (2006) nos comenta que la auditoría informática es la revisión, verificación y evaluación de los sistemas de información de una organización utilizando un conjunto de métodos, técnicas y herramientas, de forma discontinua y a petición del órgano directivo con el fin de mejorar su rentabilidad, seguridad y eficacia.

Uno de los objetivos de la auditoría informática es verificar las vulnerabilidades de los sistemas informáticos; donde los más comunes son: debilidades en el diseño de los protocolos de redes, errores de programación, configuración inadecuada de los sistemas informáticos, políticas de seguridad deficientes o inexistentes, desconocimiento o falta de sensibilización de los usuarios y de los responsables de la informática, limitaciones al tamaño de claves criptográficas, existencia de «puertas traseras» en los sistemas informáticos y el descuido de los fabricantes.

La protección y el control de la confidencialidad de los datos de la empresa implica la previsión de tres tipos de manipulaciones: a) el acceso no autorizado a los datos y al software, b) el robo o la copia de ficheros o software y c) la conexión física con las líneas de telecomunicación por las cuales circulan los datos.

Blanco (2008) expone que el proceso de trabajo de una auditoría se realiza a través de cuatro etapas: a) investigación preliminar, donde se selecciona el sistema a auditar, se determinan las pruebas a realizar, los métodos y herramientas a utilizar; b) planeación de la auditoría, donde se definen los objetivos y el programa de trabajo; c) ejecución de la auditoría, donde se realizan las reuniones de preparación, análisis de la documentación, evaluación del control interno, realización del plan de pruebas e investigaciones; y, por último d) conclusiones y análisis final, donde se realizan las conclusiones y recomendaciones, se elabora el informe final, se hace la reunión con la dirección y las personas auditadas y se discute el informe final.

Uno de los elementos que muchas veces se pasa por alto en la documentación entorno a la seguridad es el análisis de riesgo. Martínez (2002) lo define como un proceso de calidad total o mejora continua, que busca estimar las probabilidades de que se presenten acontecimientos indeseables, permitiendo medir la magnitud de dichos impactos negativos en el transcurso de ciertos intervalos específicos de tiempo. No sólo consiste en una observación detallada y sistemática, sino que es una propuesta metodológica, que permite el conocimiento de los riesgos y sus fuentes o causas (peligros), las consecuencias potenciales y remanentes, y la probabilidad de que esto se presente.

Los principales tipos de riesgo o los más conocidos y, por lo tanto, los que representan los campos más frecuentes de evaluación de riesgos y que están interrelacionados son: riesgos de seguridad social y pública, riesgos de higiene y salud, riesgos medioambientales (internos y externos), riesgos de interés social o general y riesgos técnicos y de inversión.

Sistemas de gestión de la seguridad de la información

Según la ISO/IEC 27001:2013 un SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o correo electrónico, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información.

Auditoría de los sistemas de gestión de seguridad de la información

Según la ISO 19011:2011-Directrices para la auditoría de los sistemas de gestión y la ISO/IEC 27007:2011-Tecnología de la información-técnicas de seguridad-directrices para la auditoría de sistemas de gestión de la seguridad de la información el proceso de auditoría se lleva a cabo a través de dos etapas: revisión documental y auditoría en sitio.

En la revisión documental los registros deberán incluir, conforme aplique, los documentos y registros del sistema de administración, así como los reportes de auditorías pasadas. La revisión de los documentos deberá tomar en cuenta el tamaño, naturaleza y complejidad del sistema de administración y organización del auditado, y los objetivos y alcance de la auditoría. Posteriormente a la revisión documental se llevará a cabo la auditoría en sitio empezando con la elaboración del plan de auditoría.

El plan de auditoría debe ser lo suficientemente flexible como para permitir cambios, según el desarrollo de la auditoría. Dicho plan deberá cubrir o hacer referencia a los siguientes puntos: a) objetivos; b) alcance, que incluya la identificación de las unidades organizacionales y

funcionales, así como de los procesos a ser auditados, c) criterios de auditoría y documentos de referencia; d) localizaciones, fechas, tiempos y duración de las actividades incluyendo juntas con la administración del auditado; e) métodos de auditorías a implementar, incluyendo el alcance en el cual el muestreo de la auditoría es necesario para obtener suficientes evidencias de auditoría y el diseño del plan de muestreo, si aplica; f) roles y responsabilidades de los miembros del equipo auditor, así como de los guías y observadores; g) ubicación de recursos apropiados a áreas críticas de la auditoría (OIE ISO 19011:2011). Las actividades de auditoría son normalmente conducidas en una secuencia definida que puede variar para adecuarse a las circunstancias de auditorías específicas: a) junta de apertura; b) revisión de documentos; c) recolección y verificación de información; d) preparación de conclusiones de auditoría; e) junta de cierre; f) preparación y distribución del reporte de auditoría.

El reporte de auditoría debiera ofrecer un registro completo, exacto, conciso y claro y también deberá incluir o hacer referencia a lo siguiente: a) objetivos; b) alcance, particularmente la identificación de las unidades o procesos organizacionales y funcionales auditados; c) identificación del cliente de la auditoría; d) identificación del equipo auditor y los participantes del auditado en la auditoría; e) fechas y localizaciones donde las actividades de auditoría fueron conducidas; f) criterios de auditoría; g) hallazgos de auditoría y evidencias relacionadas; h) conclusiones de auditoría; i) una declaración del grado en el cual los criterios de auditoría se hayan cumplido (OIE ISO 19011:2011).

Resultados

Plan de auditoría

Dependencia o proceso auditado:	Plataforma de educación en línea Blackboard
Responsable del proceso o dependencia:	Mtro. Martín Chávez Ramírez
Auditor principal:	M. en A. Hugo Alberto Quiroz Martínez Escobar
Fechas de realización de la auditoría:	4 y 5 de agosto de 2015
Fecha de presentación del informe:	5 de agosto de 2015

1. Objeto de la auditoría

Evaluar la seguridad de la información en la plataforma de educación en línea *Blackboard* utilizada por la Universidad del Valle de México, UVM, con el fin de verificar si cuenta con procedimientos de salvaguarda de la información sin obstruir el flujo de la misma.

Los objetivos particulares son:

- Evaluar la seguridad de la información en la plataforma de educación en línea *Blackboard*
- Verificar los accesos y los controles de acceso a la plataforma
- Verificar la existencia de certificados de seguridad en la plataforma
- Verificar el uso de protocolos de seguridad en la plataforma
- Verificar la documentación interna de la plataforma y los procedimientos documentados de soporte técnico

2. Alcance de la auditoría

La presente auditoría se realizará únicamente en el Centro de cómputo del Campus San Ángel de la Universidad del Valle de México, UVM, para acceder a la plataforma de educación en línea *Blackboard* que utiliza la universidad; donde se analizarán y verificarán en primera instancia la seguridad lógica de la plataforma, así como los procesos y procedimientos de trabajo del soporte técnico en campus, con la finalidad de detectar inexistencias o deficiencias en los mismos u otorgar recomendaciones que mejoren las prácticas actuales

3. Documentos de referencia

Recursos de inducción a la plataforma *Blackboard* en:

https://uvmonline.blackboard.com/bbcswebdav/institution/asignaturas_civ/videosInduccion/index.html

Aviso de privacidad uvm en: <http://www.universidaduvm.mx/aviso-de-privacidad/>

4. Logística de la auditoría

La auditoría tendrá una duración de dos días: inicia el martes 4 de agosto de 2015 y concluye el miércoles 5 de agosto de 2015, en un horario de 17:00 y 22:00 horas, se avisará con anterioridad la llegada de los auditores para iniciar el proceso

5. Equipo de auditoría

Hugo Alberto Quiroz Martínez Escobar

Sergio Roberto Santiago Cruz

Silvio Hernández Flores

6. Funcionarios entrevistados

Martín Chávez Ramírez, Director de servicios informáticos

Gerardo Saldaña Bernal, Jefe de soporte operativo

Israel Ángel Figueroa Pineda, Auxiliar de centro de cómputo

Luis Manuel Contreras Quintanilla, Auxiliar de centro de cómputo

7. Plan de actividades

Fecha: martes 4 de agosto de 2015

HORA	SUBPROCESO	#	AUDITOR	AUDITADO
17:00	Entrevista de Inicio	1	Todos	Martín Chávez
17:30	Verificación de la documentación de soporte técnico	2	Hugo Quiroz	Gerardo Saldaña
19:30	Verificación de los recursos de inducción	3	Sergio Santiago	Israel Figueroa
21:30	Reunión final primer día del equipo Auditor	4	Todos	N/A

Fecha: miércoles 5 de agosto de 2015

HORA	SUBPROCESO	#	AUDITOR	AUDITADO
17:00	Verificación de accesos y controles de acceso	1	Silvio Hernández	Luis Contreras
18:00	Verificación de Certificados de Seguridad	2	Sergio Santiago	Israel Figueroa
20:00	Verificación de protocolos de seguridad	3	Hugo Quiroz	Gerardo Saldaña Martín Chávez
21:00	Reunión final de auditoría	4	Todos	N/A

8. Aprobación

Hugo Alberto Quiroz Martínez Escobar
Auditor principal

Martín Chávez Ramírez
Jefe de proceso

Informe final de auditoría

Equipo auditor	M. en A. Hugo Alberto Quiroz Martínez Escobar Mtro. Sergio Roberto Santiago Cruz Mtro. Silvio Hernández Flores
Fecha	4 y 5 de agosto de 2015
Duración	9 horas, 50 minutos
Objetivos de la auditoría	Evaluar la seguridad de la información en la plataforma de educación en línea <i>Blackboard</i> Verificar los accesos y los controles de acceso a la plataforma Verificar la existencia de certificados de seguridad en la plataforma Verificar el uso de protocolos de seguridad en la plataforma Verificar la documentación interna de la plataforma y los procedimientos documentados de soporte técnico
Proceso auditado	Plataforma de educación en línea <i>Blackboard</i>
Lugar de la auditoría en sitio	Salón A006 del Centro de Cómputo del Campus San Ángel de la Universidad del Valle de México (UVM)
Personas entrevistadas y su cargo	Mtro. Martín Chávez Ramírez Director de Servicios Informáticos Mtro. Gerardo Saldaña Bernal Jefe de Soporte Operativo Israel Ángel Figueroa Pineda Auxiliar de Centro de Cómputo Luis Manuel Contreras Quintanilla Auxiliar de Centro de Cómputo
Personas encuestadas y cargo	N/A

Aspecto	Situación actual	Puntos débiles y amenazas	Recomendación	Oportunidad de mejora
Acceso	Alta de cuentas en automático con inscripción	El alumno no recibe capacitación de uso de la plataforma	Brindar a los estudiantes una capacitación completa de la plataforma	Realizar un proceso documentado para primeros pasos de la plataforma
Control de Acceso	Existe un usuario y contraseña	Usuario y contraseña son las mismas (matrícula)	Cambio a contraseña personalizada después de primer acceso	Manejo de contraseñas alfanuméricas de longitud mínima
Protocolo de Seguridad	Se cuenta con <i>Hypertext Transfer Protocol Secure (HTTPS)</i>	Contenido estático, indexación de sitio entero, ataque criptográfico	Utilizar <i>Server Name Indication (SNI)</i> y no utilizar <i>Hosting virtual name-based</i>	Mantener actualizados los navegadores web, utilizar <i>HTTPS Everywhere</i>
Certificados de Seguridad	Se tiene el <i>Secure Sockets Layer (SSL) 2.0</i> por default de servidor <i>Blackboard</i>	Ataques de renegociación, reversión de versiones, BEAST, CRIME, BREACH, Relleno, POODLE, RC4	Actualizar a <i>SSL 3.0</i> o <i>TLS 1.0</i> para mejorar el cifrado y la autenticación de certificados y resistencia a los choques	Cambiar a <i>Transport Layer Security (TLS) 1.0</i> y mantener navegadores actualizados en sus últimas versiones
Documentación Interna	Videos y slides de los temas más comunes en una materia en línea y en la plataforma	Formas de cerciorarse que son vistos o consultados, texto plano, videos sin sonido	Capacitar presencialmente en lugar de dejar todo en línea sin cerciorarse que hay consultas	Curso de capacitación de primer ingreso con todos los puntos de los temas de la documentación interna

Procedimientos documentados	No existe un manual o documentación al respecto ni política de seguridad conocida	No hay procesos documentados para realizar de manera correcta actividades de soporte	Realizar un manual de procedimientos documentados para establecer las formas en cómo realizar las actividades de soporte	Realizar un manual de procedimientos documentados para establecer las formas en cómo realizar las actividades de soporte
Conclusiones de la auditoría	La autoría en sitio (<i>in situ</i>) cumplió con los objetivos y alcance que se habían planteado en el Plan de Auditoría, se contó con la participación de las partes interesadas. Se realizaron las reuniones finales, se analizaron las evidencias y emitieron recomendaciones			
Áreas no cubiertas en el alcance de la auditoría	Se cubrieron todas las áreas y procesos propuestos para la auditoría			
Informe del proceso de auditoría	La auditoría se realizó en tiempo y forma, no se encontraron obstáculos, las personas estaban debidamente en sus lugares de trabajo y con actitud positiva para realizar el proceso de auditoría. El director de servicios informáticos acompañó en todo momento al equipo auditor. Se recomienda escoger para las auditorías futuras un horario que no impacte las clases (19:00 a 22:00 h) ya que hay alumnos en el centro de cómputo y los auxiliares tienen que atenderlos.			
Anexos	Se anexan el Plan de auditoría			

Hugo Alberto Quiroz Martínez Escobar
Auditor principal

Sergio Roberto Santiago Cruz
Auditor

Silvio Hernández Flores
Auditor

Discusión

El equipo auditor conformado por Sergio Roberto Santiago Cruz, Silvio Hernández Flores y Hugo Alberto Quiroz Martínez Escobar, fungiendo este último como auditor líder, realizó la auditoría informativa a la plataforma de educación en línea *Blackboard* utilizada por la Universidad del Valle de México. El equipo estuvo conformado también por siete testigos (estudiantes de la materia de Auditoría de la información y de la carrera de Licenciatura en sistemas de computación administrativa) y dos invitados (autoridades del campus San Ángel de la UVM).

El equipo auditado fue conformado por Martín Chávez Ramírez, Director de servicios informáticos, que fungió como guía de la auditoría y representante de la dirección; así como Gerardo Saldaña Bernal, Jefe de soporte operativo; Israel Ángel Figueroa Pineda y Luis Manuel Contreras Quintanilla, Auxiliares de centro de cómputo; que fueron los que asistieron al equipo auditor durante todo el proceso. El proceso de auditoría informática se dividió en dos partes: revisión documental y auditoría *in situ*.

Durante la primera parte, realizada el 4 de agosto de 2015 en un horario de 17:30 a 19:30 h, se revisó la Política de seguridad, se definió el alcance de la auditoría; se revisó el análisis de riesgo, la selección de controles y la revisión de todos los documentos referentes a la plataforma *Blackboard*. Para sorpresa del equipo auditor, el área no contaba con ninguno de los

documentos o manuales y desconocían su existencia en el área corporativa central de la Universidad del Valle de México (primer hallazgo). Por lo tanto, el equipo auditado desconocía la Política de seguridad, el análisis de riesgos lógicos, los procedimientos de realización de las actividades de la plataforma (soporte técnico) y la Declaración de aplicabilidad para la selección de controles para la plataforma.

Con base en la Revisión documental se elaboró el alcance de la auditoría por parte del equipo auditor. Así mismo se construyó el Plan de Auditoría que fue entregado al equipo auditado para su conocimiento y validación. Debido a la ausencia de la documentación; el equipo auditor definió, para la auditoría, los controles críticos de seguridad de la plataforma por riesgos e importancia para las actividades; siendo éstos: accesos, control de accesos, protocolos y certificados de seguridad y documentación interna de la plataforma.

Durante la segunda parte, realizada el 4 de agosto de 2015 en un horario de 19:30 a 21:50 h y el 5 de agosto de 2015 en un horario de 17:00 a 22:00 h, se realizó la auditoría en sitio donde se verificaron los accesos y control de accesos a la plataforma *Blackboard*, se verificaron los protocolos de seguridad utilizados y los certificados de seguridad instalados; así como una revisión a la documentación interna de la plataforma. Mediante las técnicas de entrevistas al personal con el uso de preguntas abiertas, cerradas y dirigidas, y la observación de las actividades se realizó la búsqueda de evidencias objetivas.

Los principales hallazgos encontrados fueron:

- Accesos: el alta de las cuentas de los usuarios se da en automático con su inscripción de nuevo ingreso y la carga de su primera materia en línea; con base en sus procesos anteriores de inscripción, es que un usuario es válido y cuenta con información fidedigna.
- Control de accesos: la plataforma cuenta con un usuario y una contraseña, que, por default, son el número de matrícula del estudiante; aunque existe la forma de cambiar la contraseña por una personalizada no se hace en automático y el estudiante debe hacer algunos pasos adicionales no establecidos de primera mano.
- Protocolo de seguridad: se cuenta con el *hypertext transfer protocol secure* (HTTPS) que establece un ambiente seguro de transferencia de datos; sin embargo no se especifica si el usuario debe utilizar un navegador en particular o que requiere mantener las versiones más actualizadas; lo cual genera brechas de seguridad en este protocolo para un ataque criptográfico.
- Certificado de seguridad: se cuenta con el *Secure Sockets Layer* (SSL) 2.0 por default del servidor de la plataforma *Blackboard*; esta versión tiene cifrados débiles y no autentica los certificados y es vulnerable a algunos ataques como son: Renegociación, Reversión de versiones, BEAST, CRIME, BREACH, Relleno, POODLE, RC4, entre otros.
- Documentación interna: está en una liga externa dentro de la pantalla principal de la plataforma *Blackboard*, abre una nueva ventana del navegador donde a la izquierda están los principales procesos de la educación en línea y de uso de la plataforma explicados por animaciones básicas y videos tutoriales; no se cuenta con una forma de asegurar que el estudiante tiene acceso y que los revisa para solucionar dudas.

Al finalizar la auditoría se convocó a una reunión final con el equipo auditado el 5 de agosto de 2015 a las 21:00 h donde se agradeció la colaboración, se recordó el alcance y los objetivos para verificar su cumplimiento, se dio un resumen de los resultados de la auditoría, se informaron las recomendaciones, se entregó el informe final de auditoría para firmarse de conformidad de ambas partes y se dio el cierre de la auditoría.

Conclusiones

La educación en línea cada vez es más adoptada como modelo educativo y, las plataformas virtuales o ambientes virtuales de enseñanza son el centro focal de este proceso. La investigación bibliográfica arroja que los principales retos y enfoques de estas plataformas son el diseño curricular y el enfoque pedagógico para la elaboración de cursos; posteriormente, los enfoques van encaminados a la explosión de herramientas tecnológicas desde el punto de vista de medios de comunicación, acceso a la información o desempeño y rendimiento de carga máxima. En ningún momento se analiza el enfoque de la seguridad de los datos que se tienen almacenados en las plataformas; eliminándola como una prioridad o un tema a consideración.

Existen plataformas comerciales, de código abierto y de diseño personalizado enfocadas a las necesidades, requerimientos, alcances y presupuestos de las diferentes instituciones educativas, centros de enseñanza y empresas. Las plataformas comerciales brindan medidas de seguridad en la información básica y elemental que, aunque sirve como barrera inicial, no brinda los mejores estándares para preservar la integridad de los datos que se encuentran almacenados en la plataforma. Las plataformas de código abierto o de desarrollo personalizado son más vulnerables ya que no cuentan con las barreras mínimas para la seguridad de los datos al momento de su desarrollo. Esta información, al no resguardarse o no tener las salvaguardas a un nivel elevado, tiene el riesgo de ser atacada, robada o modificada, convirtiéndose en una base de datos lucrativa para diferentes entes.

La seguridad informática debe ser un tema común cuando se habla de plataformas de educación en línea; por ello, debe ser regulada por instancias normativas e incluso ser un valor agregado para el marketing de las mismas.

Debido a que manejan grandes volúmenes de información; universidades, centros de enseñanza y empresas deben de adoptar mecanismos mínimos de seguridad informática: definir una política de seguridad (comunicarla), redactar procedimientos documentados en un manual (darlo a conocer e incentivar su uso), realizar el análisis de riesgos para aplicar declaraciones de aplicabilidad y selección de controles de seguridad.

Los organismos reguladores deben incentivar el uso, aplicación y certificación de las normas de seguridad de la información como es la ISO/IEC 27001:2011 de carácter internacional o la NOM-185-SCFI-2012 de carácter local en México. Esto debido al gran volumen de información que manejan las empresas hoy en día a través de dispositivos electrónicos.

Referencias

- Adelle, J., Castellet, J. y Pascual, J. (2004). Selección de un entorno virtual de enseñanza/aprendizaje de código fuente abierto para la Universitat Jaume I. Centro de Educación y Nuevas Tecnologías de la UJI. Recuperado de <http://cent.uji.es/pub/>
- Areito, L. (2007). *Unidades didácticas y guías didácticas en la UNED*. Universidad Nacional de Educación a Distancia
- Areito, J. (2008). *Seguridad de la información*. Barcelona, España: Ediciones Paraninfo
- Arratía, O. (2009). *Innovación en docencia universitaria con Moodle*. Alicante, España: Editorial Club Universitario
- Barberá, E. (2008). *Aprender e-learning*. Madrid, España: Ediciones Paidós
- Bernardez, M. (2007). *E-learning*. Washington, EUA: AuthorHouse
- Blanco, L. (2008). *Auditoría y sistemas informáticos*. La Habana, Cuba: Editorial Félix Varela
- Chicano, E. (2014). MF048y_3: Auditoría de seguridad informática, Certificado de Profesionalidad IFCT0109-Seguridad informática. Barcelona, España: IC Editorial
- Delgado, X. (1998). *Auditoría Informática*. San José, Costa Rica: Editorial EUNED
- De Pablos, C. (2006). Dirección y gestión de los sistemas de información en la empresa: una visión integradora. Madrid, España: Universidad Rey Juan Carlos ESIC
- De Pablos, C. (2004). *Informática y comunicaciones en la empresa*. Madrid, España: Universidad Rey Juan Carlos
- García, J. (2003). *El E-learning en España modelos actuales y tendencias de actuación*. Barcelona, España: Colección EOI Tecnología e Innovación
- García-Cervigón, A. (2011). *Seguridad Informática*. Madrid, España: Ediciones Paraninfo
- Gómez, E. (2005). *Aplicaciones educativas de las tecnologías de la información y comunicación*. Madrid, España: Ministerio de Educación y Ciencia, Secretaría General de Educación, Instituto Superior de Formación del Profesorado
- Martínez, J. (2002). *Introducción al análisis de riesgos*. Distrito Federal, México: Limusa Noriega Editores
- Organización Internacional para la Estandarización ISO (Suiza). *ISO 19011:2011 Directrices para la auditoría de los sistemas de gestión: 2011*. Ginebra, Suiza, 2011
- Organización Internacional para la Estandarización ISO (Suiza). *ISO/IEC 27007:2011 Tecnología de la Información-Técnicas de Seguridad - Directrices para la auditoría de sistemas de gestión de la seguridad de la información: 2011*. Ginebra, Suiza, 2011

- Organización Internacional para la Estandarización ISO (Suiza). *ISO 27001:2013 Tecnología de la Información-Técnicas de Seguridad-Sistemas de Gestión de la Seguridad de la Información-Requisitos: 2013*. Ginebra, Suiza, 2013
- Ramos, B. (2004). *Avances en criptología y seguridad de la información*. Madrid, España: Ediciones Díaz de Santos
- Rivas, G. (2008). *Auditoría informática*. Madrid, España: Ediciones Díaz de Santos
- Royer, J. (2004). *Seguridad en la informática de la empresa; riesgos, amenazas, prevención y soluciones*. Barcelona, España: Ediciones ENI
- Sierra, I. (2008). *Docencia e Interacción en entornos virtuales escenarios y posibilidades*. Córdoba, Colombia: Universidad de Córdoba Facultad de Educación y Ciencias Humanas
- Silva, J. (2011). *Diseño y moderación de entornos virtuales de aprendizaje (EVA)*. Barcelona, España: Editorial UOC
- Universidad Nacional de Educación a Distancia (2011), Presentación del curso *E learning, redes globales y plataformas*, Recuperado de:
http://portal.uned.es/portal/page?_pageid=93,8050613,93_20527912&_dad=portal&_schema=PORTAL&idAsignatura=23305134