Plataformas E-Learning, sus riesgos y amenazas
E-Learning Platforms Their Risks and Threats

Johan Sebastián Diaz Contreras[1]
johan.diaz00@usc.edu.co

Diana Lucía Villota Oliveros[2]
diana.villota02@usc.edu.co
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de Información (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de Información (2)

Resumen

En todo ambiente de educación virtual o E-Learning habrá la participación de estudiantes, profesores o tutores y las autoridades encargadas de la administración o coordinación de los cursos. Por otra parte, para que un sistema E-Learning funcione sin contratiempos, requiere que se apliquen estrategias de integridad, lo que se traduce en aplicar políticas de seguridad por ser este un sistema que trabaja sobre la Internet.

Por lo anterior, el aprendizaje E-Learning estará expuesto a amenazas y riesgos por parte de los hackers informáticos, quienes atacaran los diferentes activos digitales o contenidos del curso, con especial énfasis en la violación de los derechos de autor (Delgado Peña, 2018). Es esta situación la que genera el objetivo de realizar una investigación documental acerca del tema tratado.

El presente artículo hace una reseña de las amenazas a las que está expuesta una plataforma E-Learning y la forma como se pueden mitigar los riesgos que puede presentar la educación a distancia, para que se le pueda proveer de confianza a todos los actores del aprendizaje a distancia cuando usen plataformas virtuales E-Learning.

Palabras Clave: E-learning, Educación Virtual, Amenazas, Riesgos, Seguridad E-Learning.

Abstract

In any virtual education environment or E-Learning there will be the participation of students, teachers or tutors and the authorities in charge of the administration or coordination of the courses. On the other hand, for an E-Learning system to work smoothly, it requires integrity strategies to be applied, which translates into applying security policies as this is a system that works on the Internet.

Due to the above, E-Learning learning will be exposed to threats and risks by computer hackers, who will attack the different digital assets or contents of the course, with special emphasis on the violation of copyright (Delgado Peña, 2018). It is this situation that generates the objective of carrying out a documentary investigation about the treated topic.

This article reviews the threats to which an E-Learning platform is exposed and the way in which the risks that distance education can present can be mitigated, so that all actors of remote learning can be trusted, when they use virtual platforms E-Learning.

Keywords: E-Learning, E-Learning Security, Virtual Education, Threats, Risks

1. INTRODUCCIÓN

El uso de la Internet ha traído grandes cambios en las empresas, en las personas y por supuesto en la forma como se estudia o se hace investigación, a través de la internet se puede conseguir todo el material y documentación que se necesite para estudiar o profundizar en un tema específico.

Según De Houwer, Barnes-Holmes & Moors (2013) al E-Learning se le conoce como la "realización de actividades de aprendizaje a través de la Internet, es un nuevo modelo de aprendizaje y de formación", que está cambiando el paradigma de la educación presencial técnica, tecnológica y universitaria en especial de los procesos de apoyo, "al contar con tecnologías multimedia que posibilitan un mayor nivel de comprensión de los contenidos curriculares y en general de los cursos E- Learning". El uso de plataformas E-Learning requiere la participación de un conjunto de actores como los son: autores de contenido digital; estudiantes; administrativos o coordinares de programas o cursos; profesores o tutores; desarrolladores o administradores de las plataformas E-Learning.

Por estar este sistema de aprendizaje soportado por la Internet, está sujeto a los ataques de los hackers informáticos, quienes podrán robar activos digitales o contenidos digitales como documentos, exámenes, test, audios, videos y en el peor de los escenarios, obtener diplomas o certificados sin haber cumplido con el desarrollo de un curso. Esta problemática es el objetivo y la que ha llevado a los autores a realizar una investigación documental acerca de los problemas y riesgos informáticos a los que se expone la educación e- learning y la forma de mitigar los mismos.

Los avances tecnológicos seguirán cambiando las formas de aprendizaje y los modelos educativos, traerán además cambios en la forma como se guía un curso por parte de los profesores ahora llamados tutores (Li, Y. W. 2016), todo esto sin perder el horizonte que el medio es la Internet y por tanto estará sujeto a amenazas y riesgos que se deben mitigar para ofrecer confianza a los actores que participan en un programa o curso E-Learning. En este artículo podrá ampliar lo expuesto a través de los capítulos de: e-learning en la educación, riesgos en el uso de tecnología E-Learning, mitigación de riesgos. Todos ellos tratados para comprender las amenazas y los riesgos a los cuales está expuesta la educación E-Learning.

2 PLATAFORMS E-LEARNING

Nuestro modelo tradicional de educación, desde inicios del siglo XX estaba fundamentado en recibir las clases de formar presencial y físicamente en un aula de clase, esto quiere decir que el aula de clase estuvo conformada por estudiantes y un profesor que dirigía el proceso de enseñanza y aprendizaje. En el siglo XXI la evolución de las computadoras, la internet, las aplicaciones web y la telefonía celular han cambiado radicalmente la forma como se implementan los procesos de enseñanza y aprendizaje.

Esta evolución nos condujo a estar frente a una nueva forma o alternativa de enseñanza-aprendizaje para adquirir conocimientos, competencias y habilidades. De acuerdo con De Houwer, Barnes- Holmes & Moors, (2013) "En esencia, estamos hablando del e-learning, que algunos autores definen como un sistema educativo basado en un sistema de información que, usando un computador y la internet, actúa como una herramienta que le permite a los estudiantes o personas en general, aprender en cualquier lugar y en cualquier momento un tema, curso o habilidad específica". Ha sido tanto el nivel de penetración de estos sistemas de información, también llamados plataformas E-Learning, que hoy en día mediante el uso del e-learning muchos de los currículos o contenidos de los programas de estudio incluyen al menos un curso e-learning, usando estas tecnologías de apoyo en la educación técnica, tecnológica o universitaria.

Según datos de la plataforma SNIES del Ministerio de Educación Colombiano, a nivel universitario en el país se ofrecen 197 programas universitarios en la modalidad virtual, los cuales se distribuyen por departamentos así:

DEPARTAMENTO	***CANTIDAD***
ANTIOQUIA	39
ATLANTICO	7
BOGOTA D.C	112
BOLIVAR	1
BOYACA	3
CALDAS	6
CAUCA	3
CUNDINAMARCA	3
MAGDALENA	2
NORTE DE SANTANDER	1

QUINDIO	1
SANTANDER	10
SUCRE	6
VALLE DEL CAUCA	2
TOTAL:	197

Fuente: SNIES[1] junio 2019

De acuerdo con De Houwer, Barnes-Holmes & Moors (2013), las plataformas E-Learning han evolucionado tecnológicamente logrando contribuir a cerrar la brecha geográfica entre las personas y las instituciones que ofrecen educación de cualquier nivel, quiere decir esto que personas, que por su localización geográfica antes no podía estudiar ahora lo están haciendo (Alia Arafeh. 2018). E-learning ofrece la capacidad de compartir material educativo en todo tipo de formatos: videos, presentaciones de diapositivas, documentos de word, documentos PDF, audio entre muchas otras posibilidades.

Mediante este tipo de plataformas se pueden realizar webinars (video de clases online en vivo) y los estudiantes se pueden comunicar con sus profesores mediante un chat (mensaje instantáneo en vivo), otra de las posibilidades es el uso del foro como aprendizaje compartido o colaborativo, donde el profesor coloca un tema para que sea debatido con la participación de los estudiantes del curso.

Hay una cantidad de diferentes sistemas e-learning, los cuales se conocen con el nombre de Learning Management Systems (LMS), que mediante distintos métodos permiten que los cursos lleguen a los estudiantes y que usando las herramientas adecuadas pueden realizar proceso de automatización y calificación de las pruebas o exámenes, así como la creación de contenido multimedia bastante atractivo a los estudiantes (De Houwer, Barnes-Holmes & Moors, 2013). E-learning le proporciona los estudiantes una forma o capacidad de adaptarse al aprendizaje en torno a su estilo de vida, permitiéndole incluso a la persona más ocupadas poder estudiar.

Por otra parte, cuando se habla de E-Learning se debe comprender que existen dos modalidades básicas de E-learning (Sangrà, Vlachopoulos & Cabrera, 2012):

- E-leaning propiamente dicho: cuando el conocimiento y el proceso de enseñanza-aprendizaje se realiza de forma exclusiva usando la internet.
- B-learning o blended learning: cuando el conocimiento y proceso de enseñanza-aprendizaje se combina tanto a distancia usando la internet como de forma presencial usando un aula de clase.

Así mismo se debe comprender que el e-learning se fundamenta en tres pilares básicos (Sangrà, Vlachopoulos & Cabrera, 2012):

- Lo que se pretende enseñar (enseñanza o contenidos).
- La tecnología a través de la cual se quiere transmitir y ayudar a construir el conocimiento (plataforma de e-learning).
- El factor humano (profesores-formadores y alumnos).

En concreto se puede resumir diciendo que una plataforma de e-learning es una herramienta tecnológica utilizada para distribuir el conocimiento, con unas funcionalidades generales como son:

- Autenticación en el sistema
- Generación de contenidos
- Visualización de contenidos
- Diferentes medios de comunicación con el profesor o tutor
- Diferentes tipos de actividades: tareas y trabajos en grupo
- Reporte de actividades realizadas por el estudiante
- Herramientas de evaluación

Y que existen diferentes tipos de plataformas:

[1] https://snies.mineducacion.gov.co/consultasnies/programa#

- CMS (Content Management System): para proyectos pequeños en los que se necesita crear contenido dentro del sistema. Ejemplo de estos tenemos a PHPNuke, Drupal, Mambo
- LMS (Learning Management System): se enfoca en el área educativa principalmente y permite llevar un control tanto de los contenidos como de los usuarios que interactúan dentro de él. Los contenidos cargados son creados por una herramienta externa como Frontpage. Ejemplo de estos tenemos a Moodle, Chamilo, Edx.
- LCMS (Learning content Management System): son plataformas que Integran las utilidades de los anteriores, pero con un módulo o funcionalidad para crear contenido. Ej. Blackboard o Saba.

2.1 Riesgos en el uso de tecnología E-Learning

La evolución de la tecnología y en particular el uso de las Tecnologías de la Información y la Comunicación aplicadas al E-Learning, han permitido experimentar grandes cambios en distintos niveles de educación tanto técnico, como tecnológico y universitario. En este sentido la Internet es un medio muy poderoso que ayuda a satisfacer la creciente demanda de material de estudio básico, avanzado, de profundización y de recursos asociados a este material. Hoy en día cualquier institución educativa (universidad, organización, corporación) ve con preocupación como sus proyecciones financieras se pueden ver afectadas por este tipo de innovaciones tecnológicas y del aprendizaje, ya que en la era de la globalización, los estudiantes de diferentes regiones, inclusive de diferentes países y comunidades pueden estar demandando el mismo tipo de curso o estudio, para lo cual la distancia o ubicación geográfica ya no tiene barreras.

Tal como se expresó en el anterior apartado, E-Learning se aplica y se conoce en una variedad de contextos, como el aprendizaje a distancia, el aprendizaje en línea y el aprendizaje en red o el aprendizaje para promover las interacciones educativas entre estudiantes, profesores y comunidades de aprendizaje (Karforma Sunil, Ghosh Basudeb, 2013). Esto significa que por ser una aplicación que funciona a través de la internet, puede ser atacado por los piratas informáticos

quienes pueden cambiar o modificar los documentos alojados en la plataforma E-Learning, entre ellos tenemos: materiales de aprendizaje; certificados; cuestionarios; exámenes; materiales de lectura; hojas de calificaciones y en general todo lo conocido como activos digitales. Todos estos elementos se transfieren o comparten entre un tutor, un administrador a los estudiantes o desde los autores a los estudiantes cuando sea necesario o de acuerdo con el contenido y plan del curso.

Por lo general en el aprendizaje E-Learning participan cinco integrantes bien significativos como lo son: autores del material; estudiantes; directores de programas; profesores o tutores; desarrolladores del software o administradores de plataformas e-learning.

- Autores del Material: son las personas que producen documentos electrónicos como textos, audios, videos e imágenes, que se pueden constituir como obras sujetas de propiedad de derechos de autor.

- Estudiantes: son las personas que se matriculan en un programa o curso virtual (Chua, C., & Montalbo, J. (2014).).

- Directores de Programa: son las personas encargadas de la dirección o coordinación de un programa virtual o e-learning.

- Profesores o Tutores: son las personas encargadas de guiar y asistir a los estudiantes durante el desarrollo de un curso e-learning.

- Desarrolladores de Software: son las personas encargadas del desarrollo del software e-learning y que por lo general tienen grado de ingeniería o tecnología en el área de la programación de computadores.

- Administradores de Plataformas E-learning: son personas que parametrizan la herramienta e-learning, para que docentes y estudiantes participen en el desarrollo del curso según las reglas establecidas por la entidad que ofrece el curso.

Como se puede apreciar el uso del E-Learning al ser un componente de uso electrónico y pasar por muchas personas es factible de riesgos. Para este contexto se define un riesgo como la probabilidad de que ocurra una amenaza particular y la pérdida de uno o varios elementos. El riesgo electrónico implica el riesgo en el momento de la transacción electrónica, mientras que la amenaza significa un peligro anticipado. Las amenazas más comunes en las computadoras son los virus, usurpación de la red, robo y modificación no autorizada de datos, escuchas ilegales y no disponibilidad de servidores y computadoras personales.

Para el caso del E-Learning, los documentos originales pueden ser modificados, manipulados o destruidos por los ataques pasivos y activos de los hackers y para entender la problemática se introducirán los siguientes conceptos según cada uno de los actores:

2.2 Amenazas y Riesgos

La pérdida de un activo es causada por la ejecución efectiva de una amenaza y la explotación de una vulnerabilidad que tenía un riesgo. Todas las amenazas/riesgos se realizan a través de una o unas vulnerabilidades en los sistemas de información. Entre las principales amenazas tenemos (Singh,B. 2012):

Principales Amenazas	Descripción
Violación de confidencialidad	Una parte no autorizada que obtiene acceso a los activos alojados en el sistema de e- learning.
Violación de integridad	Una parte no autorizada que accede y se apropia de un activo utilizado en el sistema de e-learning.
Denegación de servicio	Prevención de derechos de acceso legítimos al interrumpir el tráfico durante el Transacciones entre los usuarios del sistema E-Learning.
Uso ilegítimo	Explotación de privilegios por parte de usuarios legítimos.
Programa malicioso	Líneas de código para dañar otros programas.
Repudio	Negación de la participación de uno de los participantes en la plataforma E-Learning en cualquier transacción de documentos.
Enmascaramiento	Una forma de comportamiento que esconde la identidad de los hackers.
Análisis de tráfico	Fuga de información al abusar del canal de comunicación..
Ataque de fuerza bruta	Un intento con todas las combinaciones posibles para descubrir lo correcto, en este caso las claves de acceso a la plataforma E-Learning.

Fuente: Autor

Como resultado de las amenazas anteriores (Weippl Edgar 2011), en un curso E-Learning se presentan riegos durante el proceso de ejecución de este, al estar permeada por mensajes entre diferentes participantes. De acuerdo con el actor en los sistemas E-Learning podremos identificar los siguientes riesgos:

2.2.1 Riesgo atribuible al profesor

Los profesores o tutores son responsables de proporcionar todos los elementos académicos a los estudiantes. Los profesores pueden construir todo su contenido académico como, presentaciones, videos, audios, test de evaluaciones y exámenes entre otros o puede comprar a un tercero todos o parte de los elementos que componen el curso. Y es acá donde se puede caer en el riesgo, de que el material tenga derechos de autor y el profesor contribuya a infringir las normas, haciendo que la institución luego tenga un problema jurídico. Todos los riesgos de E-Learning no deben atribuírsele al sistema técnico, es por tanto necesario cubrir todos los aspectos y elementos que componen el curso.

Por la naturaleza humana de los profesores, se sabe que una metodología de enseñanza cambia de un profesor a otro, pero habrá riesgos comunes en eventos como dar conferencias, enviar notas y tareas, aceptar y marcar hojas de respuestas, preparar y distribuir hojas de calificaciones. Los foros en línea tienen la ventaja sobre las discusiones orales, sobre todo porque los documentos escritos se almacenan electrónicamente en un servidor, pero el almacenamiento digital de los documentos que aportan en una discusión constituye un gran riesgo para la privacidad de los estudiantes y los profesores, así como también a la violación de derechos de autor (Luminita,2011).

Dependiendo del contrato de trabajo, un profesor desempeña su rol especifico por ser el centro del proceso académico, por tanto, no debe ser quien se ocupe de todos los riesgos, sino que debe haber un equipo que se ocupe de los riesgos acá mencionados. El riesgo relacionado con el examen, por ejemplo, está directamente asociado con el engaño, además de ser un acto tramposo. Los profesores deben preocuparse por la disponibilidad y el no repudio de las evaluaciones, deben ser conscientes del riesgo en que se incurre, si los estudiantes reciben el cuestionario de preguntas antes del inicio de los exámenes. Siempre existe el riesgo de modificación de los documentos de clase antes de que las lecciones lleguen a los estudiantes.

2.2.2 Riesgo atribuible al director o administrador

Generalmente cuando se toma un curso E-Learning, existe una autoridad que emite un diploma, título o certificado al estudiante después de completar con éxito el curso. Pero la persona o personas autorizadas para otorgarlo siempre establecen unas reglas y normas para realizar cursos usando plataformas E-Learning. Se puede volver riesgoso entonces otorgar un título o certificación, al momento de valorar esas reglas y normas, si llegase a ocurrir una ambigüedad en el cumplimiento de esas reglas, puede ocurrir que se otorgue o se deje de otorgar un título, diploma o certificación a un estudiante.

Uno de los principales riesgos en el aprendizaje electrónico o E-learning, es que el curso lo desarrollen personas que suplantan a los estudiantes y que realicen las pruebas a nombre de estudiantes inscritos, lo cual es claramente un delito o fraude. (Caplinskas, Dzemyda & Lupeikiene, 2013). Los directivos de las facultades y los estudiantes tienden a no ponerle atención a los aspectos legales porque generalmente están más interesados en el campo académico. Los problemas legales, como los derechos de autor, las pruebas en línea, el envío de documentos oficiales, entre otros, son un gran riesgo para los participantes en el curso. (Caplinskas, Dzemyda & Lupeikiene, 2013).

Los directivos deben vigilar no solo la inscripción en un curso, sino también deben tener la certeza que los participantes en el curso y en especial los estudiantes, son los avalados para hacer parte del curso. Además, deben contar con un plan para hacer y mantener las copias de seguridad, así como tener la certeza que el proceso de recuperación de las copias de seguridad sea efectivo.

Otro de los aspectos que deben tener en cuenta los administrativos o coordinadores es la seguridad de mantener salvaguardas sobre las contraseñas y tener claridad sobre la responsabilidad en el soporte y mantenimiento de estas. También es un riesgo para la administración distribuir responsabilidades en temas delicados como el mantenimiento de los servidores y enrutadores, el suministro de energía al servidor y otros dispositivos de red.

Es responsabilidad del Administrador controlar la autorización, es decir, las estrategias de acceso (leer, escribir y ejecutar) de los estudiantes y demás participantes para lograr un funcionamiento eficiente del sistema. (Caplinskas, Dzemyda & Lupeikiene, 2013). Por otra parte, debe asignar personal para administrar la base de datos (DBA), para que se realicen las operaciones de optimización de índices, es decir, que cree o elimine índices, para la creación de nuevas tablas, para la alteración, adición o eliminación de atributos en una relación, además deben tener claridad sobre quien puede leer, insertar, actualizar y eliminar componentes de contenido como material multimedia de la plataforma E-Learning (Caplinskas, Dzemyda & Lupeikiene, 2013).

Además de todo lo anterior, se debe tener en cuenta que los computadores pueden verse afectados por virus desde la Internet, al recibir correo o ejecutar un software no autorizado, así que la administración debe contemplar mantener seguridad física del edificio, que no hayan daños en el acceso remoto, ser consciente que el desarrollo y mantenimiento de la plataforma tiene costos y que todas estas acciones pueden llegar a exceder las estimaciones presupuestales y que pueden agravar si los objetivos de producción no son claros.

2.2.3 Riesgos atribuibles al desarrollador del sistema

El diseño, el desarrollo y la entrega de productos de E-Learning requieren de una alta calidad de sus componentes como el hardware, el servidor web, el servidor de base de datos, el ancho de banda de internet y un LMS de calidad. (Sajjadi & Tajalli Pour, 2013). Es decir, se requiere de una infraestructura robusta capaz de soportar múltiples usuarios y aplicaciones en la red.

El equipo de desarrollo debe contemplar la existencia y la forma de mitigar los problemas que puedan aparecer por no contar con los elementos de alta calidad que se requieren para cumplir con su trabajo, de lo contrario el costo de ejecución del proyecto crecerá de manera inesperada. Otro riesgo es que el desarrollador escriba contraseñas en texto dentro del código de la aplicación, sobre todo si usa su nombre, el nombre de su mascota o alguna relacionada con su entorno familiar, lo que podría permitir que un estudiante inteligente puede tener acceso al código fuente y obtener acceso a la contraseña de las bases de datos (Sajjadi & Tajalli Pour, 2013).

El desarrollador debe saber y conocer que hoy en día, los atacantes están utilizando herramientas para adivinar contraseñas de usuario, que estas herramientas existen y son reales como la conocida ISQL (SQL INJECTION), de tal suerte que su código debe estar protegido contra este tipo de ataques (Sajjadi & Tajalli Pour, 2013).

SQL INJECTION es un método de infiltración de código intruso que se vale de una vulnerabilidad presente en una aplicación en el nivel de validación de las entradas al momento de realizar operaciones sobre una base de datos (Bizimana, Olivier & Belkhouja, Taha. 2017). Se dice que existe o se produjo una inyección SQL cuando, de alguna manera, se inyecta código SQL dentro del código SQL de un programa, con la finalidad de alterar el funcionamiento normal,

logrando que se ejecute la porción de código incrustado en la base de datos.

2.2.4 Riesgo atribuible al estudiante

Los estudiantes pueden clasificarse en diferentes niveles, desde nivel de primaria hasta el nivel de doctorado. Cada usuario debe estar al tanto de todos y cada uno de los materiales recibidos de la institución que oferta el curso. De otra parte, si los intrusos han editado los documentos de preguntas u otros documentos, los estudiantes podrían tener problemas en el momento de presentar sus evaluaciones.

Existen riesgos desde el momento que el estudiante inicia sesión, porque está manipulando su ID de usuario y contraseña. Los estudiantes deben ser conscientes del uso incorrecto de la información de inicio de sesión, de lo contrario, el atacante (McHoes, Flynn, Cortés Galicia & Flynn, 2011) puede impedir que un estudiante acceda al servidor de E-Learning mediante un ataque de contraseña. Una situación diferente sería si el acceso a al inicio de sesión se hiciera mediante biometría, este aspecto ayuda a mitigar los riesgos (Song, K. S., Lee, S. M., & Nam, S. 2013).

Por otra parte, los estudiantes deben conocer acerca del phishing, en el que el atacante configura sitios web falsos que parecen un sitio web de E-Learning real, y se les pide a los estudiantes que ingresen información confidencial (M. Arora & S. Sharma, 2017)**,** con lo cual dejan expuesta la plataforma a los atacantes.

Para tomar cursos E-Learning se requiere que los estudiantes tengan presente que la información que está en Internet o medios digitales está protegida por derechos de autor (Delgado Peña, P. (2018), dado que ha sido creada por alguien y por otra parte que mucha de la información que está en internet puede descargarse para fines de lectura o consulta personal, pero no se puede distribuir en ningún medio electrónico, sin obtener permiso del autor (Delgado Peña, P. (2018). Esto significa que le existe una responsabilidad al estudiante cuando envía documentos digitales a los foros o tutores del curso.

2.2.5 Otros riesgos y amenazas en E-Learning.

Además de los riesgos anteriores, existen otras amenazas en el sistema como: (Qwaider, 2012).

- **Amenazas Naturales**: las amenazas naturales pueden ser causadas por desastres naturales como incendios, tormentas, erupciones volcánicas, terremotos, inundaciones, etc. El sistema de E-Learning puede verse afectado por este tipo de amenazas.

- **Un acto deliberado o mal intencionado:** las amenazas pueden venir de fraude, chantaje, robo o secuestro como sucedido con la amenaza Ransomware o WannaCry (Routledge. 2017).

- **Amenazas involuntarias:** es posible que existan algunas amenazas inevitables, como un error en el computador, un apagón, un error de manejo, y cualquier otro no voluntario.

Por lo tanto, todos los participantes en el sistema de E-Learning deben someterse a un análisis de riesgo, y con la ayuda de empresas TI externas dedicadas a la seguridad se podría construir un mapa de riesgos que permita tener a la mano un conjunto de acciones para mitigar los riesgos.

3 MITIGACIÓN DE RIESGOS

La mitigatorio de riesgos es el proceso posterior a la identificación de los riesgos y tiene su fundamento en definir las estrategias, las responsabilidades y las actividades que formalmente se llevarán a cabo durante el desarrollo de los cursos e-learming para minimizar el impacto de los riesgos identificados. Por lo tanto, mitigar los riesgos requiere de la aplicación de un conjunto de herramientas o técnicas las cuales veremos a continuación:

3.1 Control de acceso mediante Firewall.

Un firewall es sistema de seguridad compuesto por hardware y software usado para evitar el acceso no autorizado a una red corporativa desde fuera de la organización (Sathyan.K, 2012). Un servidor de seguridad es una versión especializada de un enrutador, donde las reglas y funciones básicas de enrutamiento, se puede configurar para que realice la función de firewall, con la ayuda de recursos de software adicionales.

El principio fundamental es que, basándose en un conjunto de reglas se asegure todo el tráfico desde adentro hacia afuera y viceversa, esto se hace usando un firewall. Para lograrlo, primero se debe bloquear físicamente todo acceso a la red

local y solo permitir el acceso a través del firewall. De esta manera solo se permite el paso del tráfico autorizado según la política de seguridad. Por otra parte, el firewall debe ser lo suficientemente fuerte para neutralizar los ataques que los hackers le realizan a la red.

En implementaciones prácticas, un cortafuegos es una combinación de filtros de paquetes y puertas de enlace de aplicaciones (Sathyan.K, 2012). Los cortafuegos sofisticados pueden bloquear parte del tráfico entrante, pero permitir que los usuarios de E-Learning (estudiantes, profesores u otros) se comuniquen libremente desde el interior.

Lo anterior significa que la administración, coordinación o dirección de la institución debe contemplar la implementación de un firewall, así como contar con el personal capacitado para configurar y monitorear el firewall.

3.2 Derechos de autor en documentos o activos digitales E-Learning

Una estrategia comúnmente usada para reducir los riesgos asociados con los activos de E-Learning (Zamzuri Z. 2011) es la protección de derechos de activos digitales. Los recursos compartidos son recursos simples, como lo puede ser una página HTML estática, un documento PDF, un grupo de archivos, las imágenes o una simple hoja de estilo CSS.

Dado que los activos E-Learning se consideran en realidad como contenido E-Learning (notas, test, exámenes, calificación y otros), así como contenido también son las claves, los datos personales de los usuarios (estudiantes, profesores), los mensajes entre usuarios, los datos de inscripción de diferentes grupos, el ancho de banda de la red y muchos otros más. En contexto cuando hablamos de E-Learning, todo lo que este escrito se define como un activo de E- Learning., así como también lo son los servicios prestados por el sistema de E-Learning: recursos de aprendizaje; Preguntas de examen o evaluación; Resultados de los alumnos; Los perfiles de usuario; Contenido de los foros; Los anuncios de los alumnos (Zamzuri Z. 2011).

La definición clara de los derechos digitales hace que los contenidos del sistema E-Learning estén protegidos. El sistema E-Learning funciona en la Internet en la que los derechos de los activos van a estar asociados con los estudiantes, con los proveedores de contenido, con los profesores, tutores o instructores. Todos estos derechos están en juego a medida que se crean diferentes activos, se distribuyen, se agrega más contenido y se almacenan, todos esto sucede a medida que se utiliza ese contenido y los servicios E-Learning. Eso es lo que hace que sea necesario utilizar los acuerdos de licencia y la protección de derechos de autor, para evitar la copia sin permiso o autorización (Frattolillo, 2017).

3.3 Uso de la Criptografía

Como el propósito de la confidencialidad es garantizar que la información y los datos no se puedan revelar con facilidad a ninguna persona o entidad no autorizada, los participantes en un curso E-Learning deben poder confiar que esto es así durante el desarrollo del curso. Para lograrlo, se debe utilizar la criptografía (Kim, Wu & Phan, 2018). Se usan entonces diferentes técnicas y herramientas criptográficas para implementarle seguridad a las transacciones realizadas a través de la Internet. En particular los desarrolladores deben elegir entre una de las dos técnicas generales para encriptar la información; Algoritmos de clave secreta o algoritmos de clave pública.

3.4 Uso de autenticación biométrica

Con cualquier técnica de autenticación (Sundararajan & Woodard, 2018) de usuarios como las contraseñas, las tarjetas inteligentes, la firma digital o el certificado digital, no hay garantía de que los estudiantes deshonestos tengan su contraseña en secreto o no la compartan. Una contraseña puede ser mal utilizada cuando se está presentando una tarea, o recibiendo los documentos de estudio, o descargando el material del curso, es por esto por lo que la autenticación biométrica dará mayor seguridad a todos los participantes en el curso E-Learning. Es una práctica que poco se utiliza porque implica unos costos adicionales (Marnell, J. W., & Levy, Y. 2014), pero es la mejor opción para garantizar que un usuario autorizado es quien está trabajando en la plataforma E-Learning.

3.5 Usar marca de agua en documentos digitales

Es una técnica que permite usar avisos de derechos de autor sobre los documentos o activos E-Learning, haciendo que los activos estén protegidos contra uso indebido por parte de personas no autorizadas. De esta forma se disminuye la piratería de documentos o videos. Se podría colocar un texto con el nombre o iniciales de la institución, por ejemplo.

4. CONCLUSIONES

E-learning es una herramienta tecnológica utilizada para distribuir el conocimiento a través de la internet, que permite el aprendizaje ubicuo es decir sin tener que asistir a un aula de forma presencial, pero que está sujeta a una serie de

amenazas y riesgos.

Por ser el sistema E-Learning una aplicación web, estará sujeta a todo tipo de amenazas y riesgos, en particular tiene como gran amenaza la violación de los derechos de autor de los activos digitales.

Se recomienda que detrás de un sistema E-Learning haya un departamento de TI, que garantice la disponibilidad de los servicios mediante el uso de hardware redundante como servidores, enrutadores, monitoreo de la base de datos y optimización de los servicios web entre otros.

Se puede mejorar el nivel de seguridad en los sistemas E-Learning, usando diferentes técnicas que ayudan a minimizar los riesgos, entre ellos podemos mencionar la biometría, la criptografía y las marcas de agua en los activos digitales.

A medida que los costos de implementación de la biometría disminuyan, seguramente esa será la técnica preferida para autenticarse en un sistema E-Learning, dado que da una mayor garantía que el estudiante o usuario de la plataforma es quien realmente está inscrito en un curso E-Learning.

5. REFERENCIAS

Alia Arafeh (2018). Online Learning: Bridging the Cultural Gaps

Bizimana, Olivier & Belkhouja, Taha. (2017). SQL injections and mitigations Scanning and Exploitation using SQLmap.

Caplinskas, A., Dzemyda, G., & Lupeikiene, A. (2013). Databases and Information Systems VII. Amsterdam: IOS Press.

Chua, C., & Montalbo, J. (2014). Assessing students' satisfaction on the use of virtual learning environment (VLE): An input to a campus-wide e-learning design and implementation. In Information and Knowledge Management, 4(2), 108-115.

Delgado Peña, P. (2018). Derechos de autor en Colombia: especial referencia a su transferencia y disposición jurídica en el ámbito universitario. DOI: http://dx.doi.org/10.21615/cesder.8.2.3

De Houwer, J., Barnes-Holmes, D., & Moors, A. (2013). ¿What is learning? On the nature and merits of a functionaldefinition of learning. Psychonomic Bulletin & Review, 20(4), 631-642. doi: 10.3758/s13423-013-0386-

Frattolillo, F. (2017). A Digital Rights Management System based on Cloud. TELKOMNIKA (Telecommunication Computing Electronics And Control), 15(2), 671. doi: 10.12928/telkomnika. v15i2.5991

Karforma Sunil, Ghosh Basudeb (2013). On Security issues in e-learning System, "Proceedings' of COCOSY-09 University Institute of Technology, Burdwan University, Jan 02-04,2013.

Kim, J., Wu, H., & Phan, R. (2018). Cryptography and Future Security. Discrete Applied Mathematics, 241, 1. doi: 10.1016/j.dam.2018.03.001

Li, Y. W. (2016). Transforming conventional teaching classroom to learner-centered teaching classroom using multimedia- mediated learning module. International Journal of Information and Education Technology 6, 2 (2016), 105-112.

Marnell, J. W., & Levy, Y. (2014). Towards a model of factors affecting resistance to using multi-method authentication systems in higher-education environments. Information Security Education Journal, 1(1), 36-44.

McHoes, A., Flynn, I., Cortés Galicia, J., & Flynn, I. (2011). Sistemas operativos. Santa Fe, México: Cengage Learning Editores.

M. Arora, & S. Sharma. (2017). Synthesis of Cryptography and Security Attacks. International Journal of Scientific Research in Network Security And Communication, 5(5), 1-5. doi: 10.26438/ijsrnsc/v5i5.15

Luminita, D. (2011). Information security in E-learning Platforms. Procedia - Social and Behavioral Sciences, 15, 2689-2693. doi: 10.1016/j.sbspro.2011.04.171

Qwaider, W. (2012). Information Security and Blended Learning System Environment (BLSE). International Journal For E- Learning Security, 2(1), 147-151. doi: 10.20533/ijels.2046.4568.2012.0019

Sajjadi, S., & Tajalli Pour, B. (2013). Study of SQL Injection Attacks and Countermeasures. International Journal of Computer And Communication Engineering, 539-542. doi: 10.7763/ijcce. 2013.v2.244

Sangrà, A., Vlachopoulos, D., & Cabrera, N. (2012). Building an inclusive definition of e-learning: An approach to the conceptual framework. The International Review Of Research In Open And Distributed Learning, 13(2), 145. doi: 10.19173/irrodl. v13i2.1161

Sathyan.K, M. (2012). Security Enhancement of Firewall Policies in Virtual Private Network. IOSR Journal of Engineering, 02(02), 197-202. doi: 10.9790/3021-0202197202

Singh, B (2013). Network Security and Management 4tha ed. Prentice-Hall of India Pvt.Ltd., New Delhi (2013)

Sundararajan, K., & Woodard, D. (2018). Deep Learning for Biometrics. ACM Computing Surveys, 51(3), 1-34. doi: 10.1145/3190618

Routledge (2017). The WannaCry ransomware attack. Strategic Comments, 23(4), vii-ix. doi:10.1080/13567888.2017.1335101

Weippl Edgar R (2011). IT Security Context in E-Learning.
Yan Huang (2019). Creating Effective Collaborative Learning Groups in an Online Health Promotion Course

Zamzuri Z. F. (2011). Computer Security Threats Towards the E-Learning System Assets. Communications in Computer and Information Science, Volume 180, Part 3, 335-345.