Artículos Originales

Seguridad de la Información en aulas virtuales

Information Security in virtual classrooms

Mario Monges[1,2], Viviana Jiménez[1]

[1]*Universidad Nacional de Asunción, Paraguay.*
[2]*E-mail: mario.monges@gmail.com*

Resumen

Las aulas virtuales ofrecen numerosas ventajas a las universidades y alumnos, su uso crece en ritmo acelerado y son considerables las iniciativas existentes para su impulso. Sin embargo, también se han detectado algunos problemas en la seguridad que dificultan su implantación en las plataformas virtuales. Son muchos los estudios que tratan sobre aulas virtuales, pero en muchos casos se deja de lado la seguridad, elemento esencial en la transmisión integral del conocimiento. Esta investigación trata de una revisión bibliográfica de autores a nivel internacional y nacional que ya han tratado el tema en cuestión, se hace un estudio de la seguridad de información para las plataformas virtuales de aprendizaje, se menciona la importancia del uso de aulas virtuales durante la pandemia de COVID-19 y el reto para los profesores por el cambio de metodología de enseñanza-aprendizaje. El objetivo de la investigación fue el de definir un estándar de gestión de la seguridad de la información para aulas virtuales. Se llega a la conclusión de que hay que asegurar la disponibilidad, confidencialidad e integridad de la información y el material dentro de los entornos de aprendizaje electrónico, esto se logra con procedimientos adecuados basados en estándares internacionales como la ISO 27001 y la ayuda de la tecnología.

Palabras clave: Seguridad, Aula virtual, Información, Educación a distancia.

Abstract

Virtual classrooms offer numerous advantages to universities and students, their use is growing at an accelerated rate and there are considerable initiatives to promote it. However, some security problems have also been detected that make it difficult to implement them on virtual platforms. There are many studies that deal with virtual classrooms, but in many cases security is left aside, an essential element in the comprehensive transmission of knowledge. This research is a bibliographic review of authors at international and national level who have already dealt with the subject in question, a study of information security for virtual learning platforms is made, the importance of the use of virtual classrooms during the study is mentioned. COVID-19 pandemic and the challenge for teachers due to the change in teaching-learning methodology. The objective of the research was to define an information security management standard for virtual classrooms. It is concluded that the availability, confidentiality and integrity of information and material must be ensured within e-learning environments, this is achieved with adequate procedures based on international standards such as ISO 27001 and the help of technology

Keywords: Security, Virtual classroom, Information, Distance education

El aula virtual es ampliamente utilizada como un método de aprendizaje que, en última instancia, depende de Internet en su ejecución. Los sistemas de aula virtual personifican los sistemas informáticos y las redes de la generación de Internet (Bandara, Loras, & Maher, 2014).

Los entornos virtuales de aprendizaje son algo nuevo por lo que Rodríguez Andino (2011) afirma que:

> un entorno virtual de enseñanza aprendizaje es un espacio de comunicación que hace posible, la creación de un contexto de enseñanza y aprendizaje en un marco de inter-

Recibido: 22/05/2020 *Aceptado: 22/07/2020*

> acción dinámica, a través de contenidos culturalmente seleccionados y elaborados y actividades interactivas realizadas de manera colaborativa, utilizando diversas herramientas informáticas soportadas por el medio tecnológico, lo que facilita la gestión del conocimiento, la motivación, el interés, el autocontrol y la formación de sentimientos que contribuyen al desarrollo personal (p. 9).

Estos sistemas son complejos y tienen como objetivo garantizar la satisfacción del alumno y mantener la buena imagen del proceso de aprendizaje. Existen evidencias claras de que las tecnologías educativas innovadoras, como el aula virtual, brindan oportunidades sin precedentes para que los estudiantes, aprendices y educadores adquieran, desarrollen y mantengan habilidades básicas y conocimientos esenciales (Scott & Vanoirbeek, 2017) Sin embargo, los sistemas de aula virtual emplean Internet como un lugar para obtener toda la información y el conocimiento necesarios.

Aula virtual es el término utilizado para describir el uso de la web y otras tecnologías de Internet en términos de mejorar la experiencia de enseñanza y aprendizaje. Comparte características similares de muchos otros servicios, tales como comercio electrónico, banca y gobierno electrónicos (Fernández Narnajo & Riveros López, 2014). Los comportamientos de los usuarios de servicios electrónicos son diferentes según sus roles y necesidades. Los usuarios de aulas virtuales se centran en cómo beneficiarse de E-learning en relación con la enseñanza y el aprendizaje (Najwa, Mohd, & Ip-Shing, 2010).

Los usuarios pueden necesitar pasar períodos de tiempo más largos al emprender el aprendizaje electrónico en comparación con otros servicios.

El sector de Educación Superior está explorando cada vez más el uso de sistemas de información y tecnología para satisfacer las necesidades y expectativas de diversos estudiantes que exigen más que solo las experiencias tradicionales en el aula. Los nuevos modelos de entrega de cursos intentan combinar elementos cara a cara con el aprendizaje electrónico. Seminarios web y otro contenido digital en línea. Crear confianza y fomentar el compromiso entre los usuarios de los sistemas de aprendizaje en línea es importante porque existen oportunidades para interacciones sincrónicas y asincrónicas con el sistema (Alberto Luiz & Marcus, 2017). El aprendizaje sincrónico ocurre en tiempo real, con todos los participantes interactuando al mismo tiempo, mientras que el aprendizaje asincrónico es autodidacta y permite a los participantes participar en el intercambio de ideas o información sin la dependencia de la participación de otros participantes en ese momento (Kashif & Zulfiqar, 2018).

Para que funcione un entorno de aprendizaje electrónico en línea, la necesidad de sentirse seguro debe estar presente para los estudiantes. Los estudiantes esperan que un entorno de aprendizaje electrónico en línea funcione igual de bien, si no mejor, que el entorno de aprendizaje tradicional (Rivera Aguilera, Rivera Aguilera, Ruiz, & Olvera Martínez, 2016). Por ejemplo, en el aprendizaje tradicional, los estudiantes envían sus tareas en formato impreso y lo envían al examinador para su evaluación.

AULA VIRTUAL

Según Horton (2000), el aula virtual es el medio en la WWW en el cual los educadores y educandos se encuentran para realizar actividades que conducen al aprendizaje.

El uso de las TIC en la docencia es de interés creciente, en parte debido al proceso de transformación de la enseñanza universitaria en tiempos de crisis sanitaria y a la eclosión de las plataformas de Teleformación y campus virtuales de e-learning.

La mayoría de las aulas virtuales se conciben como un espacio para la transmisión de información, ya que los profesores proporcionan a los alumnos documentos, lecturas y enlaces.

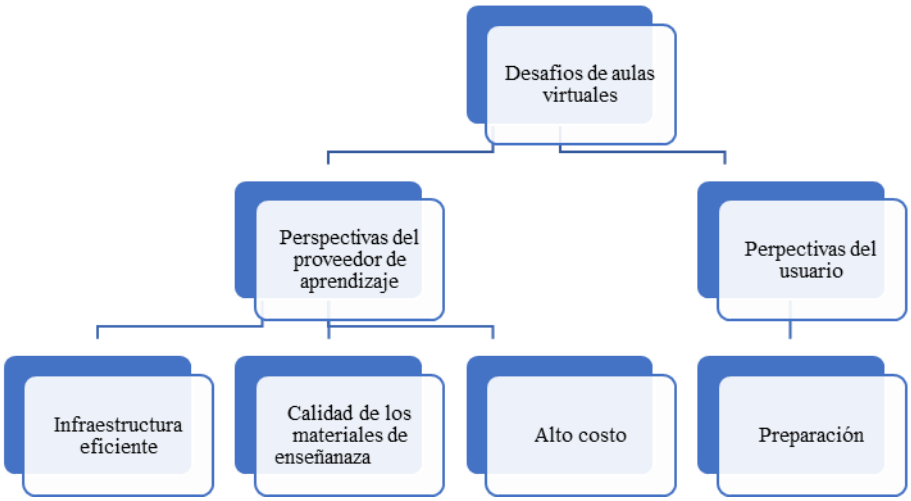
La educación virtual incorpora elementos pedagógicos de aprendizaje activo ya que se constituye en una herramienta interactiva y apropiada tanto para la transmisión de información como para la construcción del conocimiento por parte de los estudiantes lo que puede ayudar a mejorar su rendimiento cognitivo. (Alfonso, Sousa Martins, Barbosa, Ferreira, & Batista, 2018)

Desafíos en el aprendizaje electrónico

Implementar aulas virtuales no es una tarea fácil. A pesar de los muchos beneficios obtenidos del aprendizaje electrónico, también existen problemas y desafíos cuando se pretende que el aprendizaje electrónico sea exitoso.

Los desafíos, como se refleja en la Figura 1 se consideran desde dos perspectivas: el proveedor de aprendizaje y el usuario. Desde la perspectiva del proveedor de aprendizaje, las instituciones de educación superior están experimentando dificultades en relación con diversos problemas tecnológicos, como la preparación de una infraestructura eficiente. El ancho de banda y la conectividad son en última instancia necesarios, ya que los estudiantes dependerán de estas instalaciones para acceder a los materiales de aprendizaje en la web. Además, la entrega de contenido de alto ancho de banda, como el video digital, sigue siendo problemático para el usuario doméstico. El material de aprendizaje también es un problema, ya que se prepara una falta de contenido de calidad. El desarrollo de buen contenido para los estudiantes debe considerar muchos factores diferentes, como aspectos pedagógicos, interfaz humano-computadora y experiencia. Hay que asegurar que todo esto esté bien preparado, pero requiere un alto presupuesto; por lo tanto, se esperan altos costos de implementación. En un país en desarrollo, todos estos desafíos son aún más difíciles, simplemente debido a los problemas de recursos que enfrenta.

Figura 1: Los desafíos del *aula virtual* Año 2020



Fuente: Elaboración propia

Desde la perspectiva de los usuarios, están experimentando desafíos en los contextos de preparación. Aziz et al. (2006) proponen que los factores críticos en la preparación de las personas incluyen compromiso y habilidades. La preparación incluye la preparación del conocimiento, además de la preparación de la motivación para ganarse la vida.

Los estudiantes no están preparados para el aprendizaje electrónico debido a la baja alfabetización informática y los bajos niveles de autodisciplina para los métodos de autoaprendizaje.

También, de acuerdo con el modelo de aceptación tecnológica, la utilidad percibida y la facilidad de uso percibida tienen un impacto en la aceptación de los usuarios sobre el uso de la tecnología:

> si no ven cómo el aprendizaje electrónico puede ayudarlos, el estudiante finalmente resistir la continuación, o incluso inscribirse porque piensan que fallarían debido a la falta de apoyo y capacitación brindada por el proveedor de aprendizaje. Además, los instructores también sentirían lo mismo; posteriormente, otra razón para no querer usar el aula virtual es porque ven poca recompensa o reconocimiento, sin embargo, hay tantas acciones que llevar a cabo para garantizar el éxito del E-learning (Rodríguez & Chávez, 2020, p. 5).

Uso de aulas virtuales en tiempos de pandemia de COVID-19

El 12 de diciembre de 2019 fueron diagnosticados con la infección por el nuevo Coronavirus 27 individuos hospitalizados por casos de neumonía en la ciudad de Wuhan. Este virus, que pudo identificarse plenamente a inicios de 2020, al parecer fue transmitido a los humanos en un mercado de la ciudad, ya que un estudio realizado tempranamente reportó que el 55% de los infectados tenían antecedentes de haber visitado este sitio en el cual se comercializan de forma ilegal animales como serpientes, marmotas, aves y murciélagos para el consumo humano (Organización Mundial de Salud, 2020).

El primer caso en Paraguay fue confirmado el sábado 07 de marzo, el infectado es un hombre de 32 años de nacionalidad paraguaya quien regresó de Ecuador (Abc Color, 2020).

El 10 de marzo el gobierno nacional dispuso la suspensión de todas las actividades que implican aglomeración de personas, entre ellos las clases presenciales del sector educativo a fin de evitar la propagación del coronavirus. Con la decisión tomada por el presidente de la República, respecto a la suspensión de clases, las Universidades acataron la norma y suspendieron las actividades educativas presenciales a partir del 11 de marzo.

Las Universidades se vieron obligadas a migrar las clases presenciales hacia metodologías de enseñanza y aprendizaje virtuales. Las directrices acerca de la virtualidad suponen un reto para el quehacer docente, así como un desafío para las instituciones, más aún cuando el docente y sus estudiantes se encuentran familiarizados con un solo modelo educativo, el modelo tradicional de enseñanza-aprendizaje a través de clases magistrales, pues migrar desde este punto al modelo virtual genera sentimientos de angustia, desconfianza e incertidumbre para ambas partes. (Menendes, 2012)

Esto ha generado un reto para los profesores quienes se han visto en la necesidad de virtualizar sus asignaturas con el fin de darle continuidad y no traumatizar los calendarios académicos. El proceso puede ser arduo, pero se podría considerar como una experiencia enriquecedora que logre tumbar los mitos y barreras que muchos educadores han creado producto del miedo y la angustia que genera el perder la magistralidad, el control y la confiabilidad que da la transmisión de conceptos. (Moreno Correa, 2020)

Riesgos en el uso del aula virtual

En las últimas décadas, el vertiginoso avance de las herramientas para el procesamiento de información, así como el desarrollo de los mecanismos empleados para establecer comunicaciones, han generado dinamismo en los procesos productivos y de prestación de servicios, pero de manera proporcional han surgido riesgos a la tecnología informática.

Los riesgos contrastan con la preparación precaria de las organizaciones que adoptan la tecnología como elemento esencial para el desarrollo de sus actividades; en consecuencia se han desarrollado diversas guías para la administración de los activos de información, que se

convierten en estrategias para la preservación de la confidencialidad, integridad y disponibilidad de la información y a esto se le llama seguridad de la información. (Monges, 2015)

Sin embargo, el aula virtual en línea ha cambiado este enfoque tradicional, tanto el formato de la asignación como los canales de entrega están en formato electrónico. Esto expone el aprendizaje electrónico en línea a las amenazas y vulnerabilidades de internet. Por lo tanto, los requisitos básicos de seguridad, como la integridad, la confidencialidad y la disponibilidad, deben garantizarse cuando los estudiantes aprenden en este entorno. Aquí se presenta un escenario que describe las preocupaciones de los estudiantes. Cada una de estas preocupaciones se explica dentro del contexto de cada requisito básico de seguridad (Raitman, Ngo, Augar, & Zhou, 2005).

La seguridad adquiere un significado de protección de la información y comunicación de los usuarios contra los problemas generados por el uso de las TIC (Barrow & Heywood, 2006) Está relacionada con la privacidad, la integridad y la eficiencia de la tecnología e información de Internet. Se refiere a los conocimientos, habilidades y actitudes del profesorado para diseñar y desarrollar experiencias de aprendizaje para promover, modelar y formar al alumnado como ciudadanos digitalmente responsables. Para adquirir esta competencia, el papel de quien enseña alcanza especial protagonismo, porque su figura es modelo y guía que cuida, orienta y forma sobre el uso responsable en la navegación, comunicación y colaboración y compartir información a través de Internet.

Sin embargo, puede ser un problema debido a una concepción errónea por la que los docentes enseñan sobre la seguridad pretendiendo que el alumnado solo entienda o tenga un concepto sobre Internet (Gallego, Torres-Hernandez, & Pessoa, 2019) que ha sido base para elaborar el marco de referencia de la competencia digital docente. Incluyen competencias sobre seguridad digital, como la protección de datos personales y el respeto a la privacidad, la protección de la salud, y la adecuada gestión de la identidad digital. Destacan el uso responsable, el respeto a los principios de privacidad en línea aplicables a sí mismo y a otros y el cuidado del medio ambiente. En el área de seguridad, el usuario competente es capaz de revisar la configuración de seguridad de los sistemas y las aplicaciones; reaccionar si su equipo informático se infecta con un virus, y configurar, modificar el cortafuegos y los parámetros de seguridad de sus dispositivos electrónicos; encriptar correos y archivos; aplicar filtros para evitar el spam del correo.

Los sistemas educativos reconocen la importancia de la formación del profesorado para el dominio de las TIC y en particular sobre la seguridad, aunque en los programas de formación inicial del profesorado el tratamiento de la competencia digital suele ser transversal (Napal, Peñalva-Vélez, & Mendióroz, 2018).

En los planes de estudio se observa una clara dispersión de las asignaturas obligatorias de tecnologías en la educación, y su presencia es distinta en universidades, institutos politécnicos u otros centros de Educación Superior. Indudablemente, el futuro docente necesita conocimientos (pedagógicos y de contenido), habilidades (sociales y técnicas) y actitudes vinculadas a la seguridad digital y cómo enseñarla.

Se espera que los docentes asuman responsabilidad en la enseñanza de la seguridad digital y orienten a los estudiantes sobre las normas de comportamiento en Internet, aunque es frecuente carecer de una preparación adecuada para entender los riesgos y los comportamientos poco éticos (Chou & Chou, 2016).

La seguridad en el aprendizaje en línea se refiere a la protección contra el mal uso malicioso o accidental de los recursos en el aprendizaje en línea. La confidencialidad se refiere a la protección de la información confidencial del acceso de personas no autorizadas (Serb, Defta, Jacob, & Apetrei, 2013) y la ausencia de divulgación no autorizada de información. Dado que hay una gran cantidad de usuarios en cualquier aprendizaje en línea (entre ellos estudiantes, visitantes, instructores, tutores y administradores), se necesita un sistema de

inicio de sesión y una delimitación fuerte que marque a los usuarios registrados y grupos de usuarios para salvaguardar el acceso al usuario apropiado (Serb, Defta, Jacob, & Apetrei , 2013). Para proteger la información personal, generalmente se implementan salvaguardas de seguridad como la autenticación y el cifrado. La integridad, un elemento crítico de seguridad, se refiere a "la protección de datos contra cambios no autorizados intencionales o accidentales" y "la ausencia de un sistema incorrecto alteraciones". Asegura que "la información y los datos no se han modificado o destruido accidental o maliciosamente, y están en forma original precisa, correcta y completa". El control de acceso es la clave para mantener la integridad en el entorno de aprendizaje en línea. Disponibilidad significa la disponibilidad para el servicio correcto (Weippl & Ebner, 2008). Connota que los usuarios autorizados pueden acceder a un sistema de aprendizaje en línea cuando sea necesario (Serb, Defta, Jacob, & Apetrei, 2013). Y asegura que "los recursos de información y comunicación sean fácilmente accesibles y confiables de manera oportuna por personas autorizadas". La disponibilidad se puede dañar principalmente por la denegación de servicio y/o la pérdida de capacidades de procesamiento de datos.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN AULAS VIRTUALES

En la actualidad, la tecnología, el hardware y el software de seguridad de la información se han utilizado para proteger el entorno de aprendizaje electrónico. Yang, Lin y Lin (2002) sugieren la obligación de contar con mecanismos efectivos para el control y la gestión de la seguridad y la privacidad. Tener un control sin una planificación adecuada sobre cómo administrar el control no ayuda a reducir las amenazas en aulas virtuales. Una analogía a esto es: para mantener una casa o una habitación de datos valiosos, la puerta se cierra con llave, usando la llave y la cerradura como mecanismo de control. Solo las personas autorizadas reciben la clave para acceder a la casa.

Desafortunadamente, sin embargo, el proceso (la gestión del proceso) de entregar la clave a las personas validadas se maneja de manera insuficiente, lo que puede llevar a que la clave termine en manos de personas maliciosas En una situación diferente, la clave también podría perderse o duplicarse y luego ser utilizada por personas no autorizadas. Por lo tanto, no es solo la solución o los controles lo que importa, sino la gestión de seguridad, que determinará el éxito de los controles de seguridad y la solución implementada (Benavides Sepúlveda & Blandón Jaramillo, 2018).

A pesar de considerar la solución de hardware y software, la seguridad de la información se puede lograr mediante un conjunto adecuado de controles, conocido como Information Security Management (ISM) o Sistema de Seguridad de la Información en español (SGSI). El SGSI incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. (Kritzinger & Von Solm , 2006) sugieren cuatro elementos principales de seguridad de la información dentro de los entornos de aprendizaje electrónico, que incluyen garantizar la gobernanza de la seguridad de la información del aprendizaje electrónico, crear políticas y procedimientos de seguridad de la información del aprendizaje electrónico, implementar contramedidas de seguridad de la información del aprendizaje electrónico y monitorear contramedidas de seguridad de la información de aprendizaje electrónico. Sin embargo, los sistemas de aula virtual emplean Internet como un lugar para obtener toda la información y el conocimiento necesarios. Desgraciadamente, Internet también se ha convertido en el lugar de un nuevo conjunto de actividades ilegales, el llamado cibercrimen.

En investigaciones realizadas por varios autores a nivel mundial encontramos a los siguientes que manifestaron:

Santiso et al. (2016) concluyeron lo siguiente:

La incorporación de nuevos medios de comunicación dentro de las plataformas de educación virtual como el chat, el streaming de video y los sistemas de voz sobre IP, la aparición de nuevas formas de interacción en línea como las redes sociales y los teléfonos inteligentes, brindan una mayor facilidad de uso a los usuarios logrando una integración más rápida y efectiva de los procesos educativos a las plataformas virtuales.

Sin embargo, la inclusión de estas nuevas tecnologías trae aparejado nuevos riesgos que, si no son identificados y mitigados de manera apropiada, generan vulnerabilidades que pueden afectar la seguridad de la información, afectando así al proceso educativo (p. 68).

Es importante destacar que, para cada organización sea cual sea la función que desempeña, necesita ejecutar procesos que regulen el funcionamiento de sus operaciones y actividades, como derivación de esto las plataformas educativas se enfrentan a nuevos riesgos informáticos que pueden afectar la seguridad de los sistemas informáticos y por ende información sensible que maneja la institución educativa (Falconi Cabrera, 2019).

Para Romero Moreno (2010) que trabaja con la plataforma MOODLE afirma que:

> es bien conocido que los Sistemas Virtuales de formación están cobrando cada día mayor protagonismo, en la enseñanza a distancia (imprescindibles), en el ámbito de la universidad en general (campus virtuales asociados a todas ellas) y de una manera considerable en el contexto de las empresas (formación continua de sus profesionales). Pero los profesores y tutores de los cursos y enseñanzas necesitan trabajar con seguridad y tener la certeza de que sus herramientas están a salvo de ataques informáticos no deseados. La seguridad, en este contexto, se encarga de activar mecanismos de protección para la base de datos (p. 172).

La información asociada con el entorno de aulas virtuales, parte de la cual puede ser personal, protegida o confidencial, se expone continuamente a amenazas de seguridad porque los sistemas de E-learning están abiertos, distribuidos e interconectados (Monges, 2015), por lo que deben ser protegidos adecuadamente de acuerdo a normas internacionales de seguridad de la información.

Norma Técnica Paraguaya ISO 27001:2014 "Tecnología de la información–técnicas de seguridad–sistemas de gestión de la seguridad de la información–requisitos"

Esta norma técnica fue elaborada por el Comité Nº 54, cuya secretaría ejecutiva funciona bajo la dirección de la SENATICS actualmente MITIC (Ministerio de Tecnologías de la Información y Comunicación), con acompañamiento de técnicos especialistas en Normalización del INTN (Instituto Nacional de Tecnología, Normalización y Metrología) y profesionales del área de seguridad de la información de entidades públicas y privadas. Es la primera norma ISO nacionalizada en el Paraguay, entrando en vigor a partir de octubre de 2014, es un estándar auditable y certificable en seguridad de la información, la cual es también aplicable a plataformas virtuales de enseñanza.

Este estándar contiene los requisitos del sistema de gestión de seguridad de la información, es la norma con la cual auditores externos certifican los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados (Monges, 2015).

En Colombia las entidades del estado en cumplimiento del Decreto Reglamentario 1078/2015, deben implementar un SGSI que garantice los aspectos antes mencionados; que

tiene dentro de sus funciones brindar educación, la cual comprende los niveles de primaria, secundaria y media, a través de las Secretarías de Educación (Benavides Sepúlveda & Blandón Jaramillo, 2018)

CONCLUSIÓN

La demanda de aulas virtuales ha cambiado la forma en que la Educación Superior lleva a cabo su actividad principal de proporcionar cursos a varios alumnos. Las organizaciones deben encontrar e implementar nuevos servicios que permitan a los estudiantes estudiar de manera efectiva y segura en un entorno virtual. La mayor demanda de E-Learners de flexibilidad, movilidad y empoderamiento plantea un desafío importante para los departamentos de TI de educación superior, a quienes les resulta más difícil mantener el control sobre cómo se usan, almacenan y comparten los datos dentro y fuera de la clase virtual. La implementación de nuevos servicios, para satisfacer las exigentes necesidades de los usuarios, requiere la creación de entornos de aprendizaje electrónico seguros, estandarizados y de alta disponibilidad, así como la administración centralizada de aplicaciones.

Las aulas virtuales han crecido y se están expandiendo muy rápidamente. Los beneficios que ofrece aumentan el número de usuarios, la funcionalidad de aulas virtuales continúa expandiéndose y depende cada vez más fuertemente de Internet. Sin embargo, Internet tiende a convertirse en un lugar de actividades ilegales, que por lo tanto expone el aprendizaje electrónico a las amenazas. Asegurar la disponibilidad e integridad de la información y el material dentro de los entornos de aprendizaje electrónico requiere que se implementen contramedidas, tales como hardware y software de tecnología de seguridad, pero esto se considera insuficiente. Además, se necesita un SGSI (Sistema de Gestión de Seguridad de la Información) para garantizar la seguridad del entorno de aprendizaje electrónico.

Un SGSI para aula virtual no es diferente de otros servicios electrónicos; sin embargo, debido al factor de flexibilidad que ofrece el aprendizaje electrónico y los diferentes comportamientos de los usuarios, el aprendizaje electrónico requiere un marco de gestión de seguridad que pueda servir de guía para ayudar al proveedor (instituciones) de aprendizaje electrónico a gestionar la seguridad de la información en el entorno de aprendizaje electrónico. También la combinación de SGSI y la tecnología de seguridad de la información actual utilizada proporcionarán mejores resultados en el éxito de la implementación de seguridad.

REFERENCIAS

Abc Color. (1 de Abril de 2020). Abc color. Obtenido de https://www.abc.com.py/nacionales/2020/04/01/retorno-a-clases-lo-ultimo-que-habilitaria-el-gobierno-tras-la-cuarentena/

Alberto Luiz, A., & Marcus, B. (2017). Resistência à educação a distância na educação corporativa. Rio de Janeiro.

Alfonso, J., Sousa Martins, P., Barbosa, G., Ferreira, L., & Batista, M. (2018). Pedagogical mediation using the virtual learning environment and the new generation.

Aziz, A., Yunus, S., Bakar, A., & Meseran, H. (2006). Design and development of learning management system at universiti Putra Malaysia: a case study of e-SPRINT. Proceedings of the 15th international Conference on World Wide Web, (págs. 979-980). Edinburgh: ACM, New York.

Bandara, I., Loras, F., & Maher, K. (2014). Cyber Security Concerns in E-Learning Education. Proceedings of ICERI2014 Conference. Sevilla.

Barrow, C., & Heywood, E. (2006). The experience of English educational establishments: Summary and recommendations. British Educational Communications and Technology Agency. BECTA).

Benavides Sepúlveda, A., & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica.

Chou, H., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. Computers in Human Behavior, 334-345.

Falconi Cabrera, A. E. (2019). Medidas de seguridad informática en la plataforma virtual de la UTMACH entorno a phishing, malvertising, pharming e inyección SQL. Machala.

Fernández Narnajo, A., & Riveros López, M. (2014). Las plataformas de aprendizajes, una alternativa a tener en cuenta en el proceso de enseñanza aprendizaje. Revista Cubana de Informática Médica, 207-221.

Gallego, M., Torres-Hernandez, N., & Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. Revista Científica de Educomunicación.

Horton, W. (2000). Designing web based training. New York: Wiley Computer Publisher.

Kashif, L., & Zulfiqar, A. (2018). An Integrated Model to Enhance Virtual Learning Environments with Current Social Networking Perspective. International Journal of Emerging Technologies in Learning.

Kritzinger, E., & Von Solm, S. (2006). E-learning Incorporating Information Security Governance. Issues in Informing Science and Information Technology.

Menendes, C. (2012). Mediadores y mediadoras del aprendizaje. Competencias docentes en los entornos virtuales de aprendizaje. Revista Iberoamericana de Educación, 39-50.

Monges, M. (2015). Seguridad de la información en plataformas virtuales de e- Learning. ScientiAmericana, Revista Multidisciplinaria.

Moreno Correa, S. (2020). La innovación educativa en los tiempos del Coronavirus. Salutem Scientia Spiritus, 14-26.

Najwa, H., Mohd, A., & Ip-Shing, F. (2010). E-Learning and Information Security Management. International Journal of Digital Society.

Napal, M., Peñalva-Vélez, A., & Mendióroz, A. (2018). Development of digital competence in secondary education teachers training. Education Sciences, 8.

Organización Mundial de Salud. (5 de Enero de 2020). who.int. Obtenido de https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/es/

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the Online E-learning Environment. IEEE International Conference on Advanced Learning Technologies.

Rivera Aguilera, L., Rivera Aguilera, J., Ruiz, R., & Olvera Martínez, M. (2016). Desarrollo de cursos de educación a distancia: una experiencia entre la UASLP y el INEGI. México: Autónoma de San Luis Potos.

Rodríguez Andino, M. (2011). Los entornos virtuales de aprendizaje como potenciadores del proceso educativo. Experiencias de su aplicación en la enseñanza presencial y semipresencial. XIV Congreso Internacional de informática en la educación. La Habana.

Rodríguez, A., & Chávez, E. (2020). Cibernética educativa, actores y contextos en los sistemas de educación superior a distancia. Sophia, colección de Filosofía de la Educación, 117-137.

Romero Moreno, L. (2010). La seguridad informática en el trabajo con la plataforma Moodle.

Santiso, H., Koller, J., & Bisaro, M. (2016). Seguridad en Entornos de Educación Virtual. Memoria Investigaciones en Ingeniería.

Scott, P., & Vanoirbeek, C. (2017). Technology-Enhanced Learning. Technology-Enhanced Learning.

Serb, A., Defta, C., Jacob, N., & Apetrei, M. (2013). Information security management in e-learning. Knowledge Horizons. 55-59.

Weippl, E., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. In World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, (págs. 4001-4007).

Yang, C., Lin, F., & Lin, H. (2002). 'Policy based Privacy and Security Management for Collaborative E-education Systems. Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education, (págs. 501-505).