IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Impacto de las TIC en la sociedad.

La seguridad de la información en Entornos Virtuales de Aprendizaje

Information security in Virtual Learning Environments

Daudelyn Hernández Olmo [1*], Dunia M. Colome Cedeño [2]

[1] Universidad de Ciencias Informáticas. Carretera a San Antonio. Km 2 ½. Boyeros. La Habana. daude90@gmail.com
[2] Universidad de Ciencias Informáticas. Carretera a San Antonio. Km 2 ½. Boyeros. La Habana. dunia.colome@gmail.com

[*] Autor para correspondencia: daude90@gmail.com

Resumen
Las plataformas virtuales han producido cambios significativos en la educación y gracias a esto se producen nuevas formas de transferencia del conocimiento. El uso masivo de las tecnologías de la información y la comunicación ha traído consigo consecuencias sobre la que los sistemas educativos no pueden mantenerse al margen. La información tanto de estos sistemas como de cualquier otro, es el recurso más importante para cualquier organización. Por lo tanto, la protección de la seguridad es muy importante y debe convertirse en una prioridad para muchas organizaciones. La seguridad de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, de forma tal que garantice su confidencialidad, integridad y disponibilidad. El presente trabajo tiene como objetivo caracterizar la seguridad de la información en los Entornos Virtuales de Aprendizaje, describir los controles de seguridad, así como los estándares y normas que se utilizan para la seguridad de la información, a partir de las cuales se establecen criterios y métricas para la evaluación de la seguridad de estas plataformas.

Palabras clave: conocimiento, Entornos Virtuales de Aprendizaje, seguridad de la información, sistemas educativos

Abstract
Virtual platforms have produced significant changes in education and thanks to this, new forms of knowledge transfer are produced. The massive use of information and communication technologies has brought with it consequences that educational systems cannot stay on the sidelines. It cannot be denied that nowadays information is a very important asset for any modern organization. Therefore protecting its security is very important and becoming a top priority for many organizations. Information security depends on a set of administrative, organizational, physical, technical or logical, legal and educational measures, with a comprehensive and system approach, in such a way as to guarantee its confidentiality, integrity and availability. The objective of this work is to characterize the information security in Virtual Learning Environments, describe the security controls, as well as the standards and norms that are used for information security, based on which criteria and metrics for evaluating the security of these platforms.

Keywords: *knowledge, virtual learning environments, security of the information, educational systems*

Introducción

En la actualidad, con la aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) en el ámbito educativo y especialmente con el incremento del acceso a Internet, las posibilidades que ofrece la educación a distancia (EaD) han aumentado sustancialmente. Entre las facilidades es posible mencionar el conocimiento de casi todo lo relacionado al aprendizaje de los alumnos dentro de los Entornos Virtuales de Aprendizaje (EVA). Los avances tecnológicos están permitiendo que estos entornos resulten cada vez más abiertos, gracias a conceptos como la accesibilidad y la ubicuidad, la computación en la nube, la disponibilidad de contenidos por Internet, las nuevas interfaces de acceso en función del perfil del usuario y de su geolocalización, la participación en las redes sociales, entre otros (Gargallo, 2018).

La incorporación de nuevos medios de comunicación dentro de las plataformas para la educación virtual y la aparición de nuevas formas de interacción en línea han provocado que estos brinden una mayor facilidad de uso a los usuarios, logrando una integración más rápida y efectiva de los procesos educativos y una mejor interacción entre los estudiantes, profesores y tutores. 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 poner en riesgo el proceso educativo y de esta manera afectar la seguridad de la información (Santiso et al., 2016).

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad (Cuevas, 2015).

Ante esto, la información es el activo más valioso, por lo que es necesario protegerla de las incontables amenazas que existen y se generan a cada momento. Aquí es donde interviene la Seguridad Informática (SI), que debe ser lo suficientemente sofisticada y preparada para contrarrestar y garantizar la disponibilidad, confidencialidad e integridad de la información (Domínguez, 2015).

La evaluación de la seguridad de programas en educación virtual es un asunto reciente en Latinoamérica. Existen antecedentes de trabajos de investigación y publicaciones que hacen referencia al tema antes mencionado. En ellos se aborda el tema desde una perspectiva puntual, refiriéndose a la automatización de controles específicos de seguridad (Hamdi et al., 2007), en la detección de vulnerabilidades (Montesino, 2012), en el chequeo del cumplimiento de regulaciones (Koschorreck, 2011) y en la gestión de configuraciones (Schonwalder et al., 2010). En estos casos el objetivo fundamental es básicamente la identificación de riesgos y la generación de los documentos necesarios para la certificación, lo cual no llega a abarcar la automatización de los controles de seguridad ni el amplio espectro de controles de seguridad recomendados por estándares internacionales.

Sistemas para la gestión del aprendizaje (LMS, por sus siglas en inglés) como Moodle gestionan la seguridad mediante la activación de mecanismos de protección para su información. Particularmente, trata de proteger la información dejando la responsabilidad del acceso a la plataforma y su secuenciación en el tiempo en manos de los administradores de las aplicaciones (Romero, 2010).

En fuentes consultadas, (Fernandez, 2017; Bournissen, 2018; Santiso et al., 2016), se puede comprobar que la evaluación de la seguridad realizada a los cursos, diseñados en entornos virtuales, se enfoca en la protección de los sistemas informáticos, cubriendo con menor detalle temas como el acceso a la información y a la conectividad. Además, no se abordan otros aspectos importantes de la evaluación de la seguridad de la información, tanto de los recursos educativos como de las actividades evaluativas en el propio diseño de los cursos.

En Cuba existen profesionales con experiencia en el diseño de procesos de enseñanza-aprendizaje para la formación a distancia y ha sido siempre una prioridad del país facilitar el acceso a la educación. En el marco del XIV Congreso de la Central de Trabajadores de Cuba (CTC) de 1978 se propone buscar nuevas soluciones para satisfacer la demanda de acceso de la población a los estudios de nivel superior, desde entonces el Ministerio de Educación Superior ha venido trabajando en soluciones para esta necesidad (Rojas et al. 2014). También, en el VI Congreso del Partido Comunista de Cuba celebrado en el 2011, fueron aprobados los Lineamientos de la Política Económica y Social del Partido y la Revolución, donde se reconoce la necesidad de avanzar en la informatización del sistema educativo (Cortés et al. 2020). Teniendo en cuenta el acelerado desarrollo de las TIC, la propuesta de continuar impulsando su empleo en la educación, pudiera considerarse la aplicación de los programas diseñados en entornos virtuales en la educación superior cubana para la permanente capacitación de los profesionales.

La Educación a Distancia en Cuba ha ido transitando por un camino cada vez más completo y pertinente en aras de lograr una masificación de la enseñanza del aprendizaje en diferentes áreas del conocimiento. Actualmente, esta

modalidad de educación está enfocada en el empleo de herramientas didácticas y tecnológicas útiles tanto para el profesor como para el estudiante, con predominio de la virtualidad. La seguridad de la información de los cursos y/o contenidos digitales de esta modalidad de enseñanza, especialmente de los que se encuentran en los EVA, aún requiere de muchos estudios para evolucionar en su evaluación.

El presente trabajo tiene como objetivo realizar un estudio sobre la seguridad de la información en los EVA, los tipos de controles de seguridad que existen y los estándares y normas que se usan para la seguridad de la información.

Materiales y métodos

La concepción metodológica está basada en una investigación compleja, donde se combinan los enfoques metodológicos cuantitativos y cualitativos, descriptivos y explicativos que permitirán identificar componentes ya utilizados para la evaluación de los cursos diseñados en Entorno Virtual de Aprendizaje.

Para la obtención y análisis de información se utilizaron los métodos teóricos, orientados a la búsqueda del conocimiento, la fundamentación teórica, el análisis de la información y la elaboración de la propuesta; entre ellos el histórico – lógico para conocer la evolución de las teorías, condicionamiento y concepciones en su desarrollo; el enfoque sistémico para determinar la orientación del estudio en sus diferentes tipos de relaciones desde su carácter integral y contextual. También se emplearon métodos empíricos, orientados a la obtención de la información acerca del fenómeno objeto de estudio y aanálisis de documentos para obtener la información necesaria del estado actual del objeto de investigación.

Resultados y discusión

Cuando se piensa en la seguridad de la información, lo más habitual es que lo primero que se considere sea mantener la información, a salvo de indiscreciones. Sin embargo, cuando los usuarios están en contacto diario con las TIC y, en este caso, con las plataformas educativas, se dan cuenta de que hay otros puntos que tienen también gran importancia. Este es el caso, por ejemplo, de la información en sí misma, que debe ser mostrada de forma correcta y veraz; lo mismo sucede con el buen funcionamiento de los sistemas de información, que debe estar garantizado frente a problemas técnicos o de suministro.

Según las normas UNE/ISO-IEC 27001[1], la seguridad de la información se define como la preservación de su confidencialidad, integridad y disponibilidad, pudiendo estar involucradas otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad (Sadowsky et al. 2013; Caballero 2018; Shelupanov et al., 2019).

La confidencialidad se entiende como la propiedad de la información por la que esta no se muestra disponible o revelada para individuos, entidades o procesos no autorizados. La integridad es la propiedad de salvaguardar la exactitud y la completitud de los activos de información. La disponibilidad es la propiedad de ser accesible y utilizable por la demanda de una entidad autorizada (Lopéz, 2017).

La confidencialidad es el primer concepto que surge cuando se habla de seguridad de la información, incluso a veces se utiliza como término sustituto, aunque evidentemente es un error, pero ofrece una idea de la importancia que los usuarios le dan a este aspecto. El hecho de que la legislación reconozca la confidencialidad de cierta información como un derecho fundamental, añade énfasis a la importancia que se le otorga a este aspecto de la seguridad de la información (Caballero, 2018).

La disponibilidad es el aspecto más técnico y en el que no siempre se piensa como un tema de seguridad. Esto tiene la ventaja de que en muchos casos existen medidas encaminadas a asegurar la disponibilidad como un procedimiento rutinario, y por ello es un aspecto suficientemente cubierto (Caballero, 2018).

Controles de seguridad

Autores como, (Nieles et al., 2017; Shelupanov et al. 2019) plantean que los objetivos de control más habituales, tomados de la lista *Objetivos de control y controles* de las normas UNE/ISO-IEC 27001, que se utilizan para garantizar la seguridad de la información, son los mostrados en la Figura 1.

[1] UNE-ISO/IEC 27001 (2007): Sistemas de gestión de la seguridad de la información (SGSI).

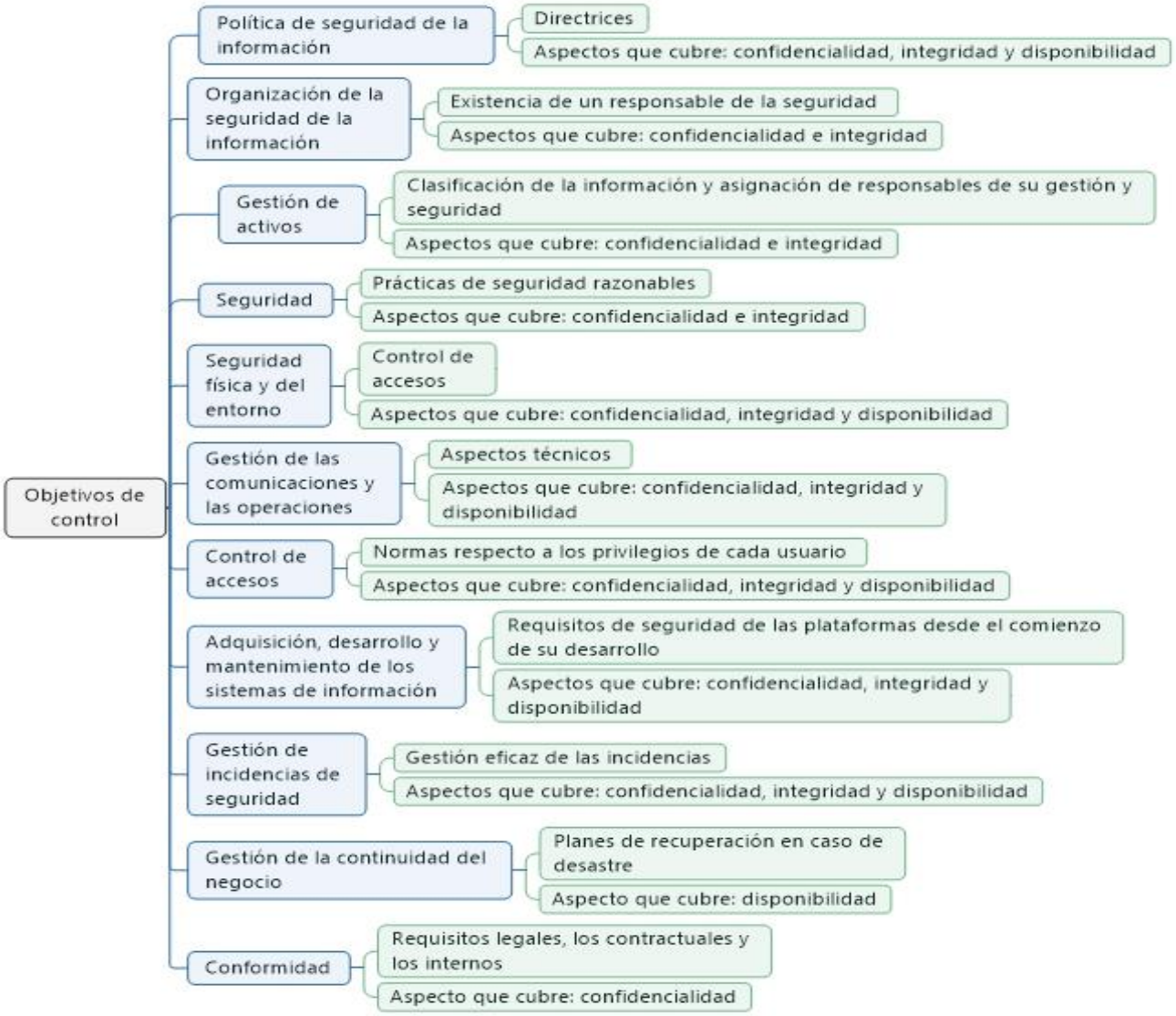

Figura 1. Objetivos de control más habituales. (Nieles et al., 2017; Shelupanov et al. 2019)

La seguridad de la información en las plataformas educativas

La dinámica actual del mundo académico se ve marcada en los últimos años por el avance de las TIC. En este sentido, la enseñanza en las universidades del mundo se apoya en plataformas interactivas para favorecer el proceso docente educativo y brindar al estudiante espacios más flexibles. Ante tal situación se ha asumido diferente EVA como soporte de la educación presencial, semipresencial y a distancia sin llegar a un acuerdo de un único recurso. Así se pueden citar como más usados: Moodle, Caroline, Atutor, Ilias, Dokeos, WebCT y Sakai (Antúnez et al., 2016).

A inicios de este siglo, se comenzaron a implementar en Cuba estas plataformas como decisión de cada centro universitario. La más utilizada ha sido Moodle y coincide con ser la más difundida en el mundo. Ya en los últimos años, el Ministerio de Educación Superior (MES) ha exigido su generalización y se ha intencionado su evaluación en la certificación de universidades (Rojas et al., 2014).

Un EVA es un espacio de comunicación que hace posible, la creación de un contexto de enseñanza y aprendizaje en un marco de interacción dinámica, a través de contenidos culturalmente seleccionados y elaborados, así como actividades interactivas para realizar de manera colaborativa. Los EVA utilizan diversas herramientas informáticas soportadas por el medio tecnológico y facilitan la gestión del conocimiento, la motivación, el interés, el autocontrol y la formación de sentimientos que contribuyen al desarrollo personal (Rodríguez et al., 2017; Hiraldo, 2013; López et al., 2009; Cruz et al., 2011).

López y otros (2009) mencionan algunos de los beneficios que ofrece el uso de entornos de aprendizaje, ellos son:

- ✓ El acceso al contenido es más flexible y no se restringe a las paredes de un aula.
- ✓ Posibilidad de acceder a la información desde cualquier lugar que posea conexión a internet.
- ✓ Combina distintos recursos para mejorar el proceso de enseñanza aprendizaje.
- ✓ Facilitan el aprendizaje colaborativo y cooperativo.
- ✓ Las aportaciones mejoran en cuanto a calidad se refiere, gracias a la flexibilidad temporal de la que nos dota el uso de estos sistemas.
- ✓ Existe retroalimentación, no sólo con el profesor, sino con el resto de compañeros.
- ✓ Aumenta la motivación y participación de los sujetos.
- ✓ Los sujetos son conscientes y partícipes de su propio aprendizaje.

A pesar de los beneficios que proporciona el uso de dichos entornos en la labor de los profesores, no se debe olvidar que el uso de cualquier tecnología en el aula puede traer consigo algunas desventajas que se deben controlar antes, durante y después de su uso. Al introducir un elemento nuevo en el aula, que modifique o adapte los procesos de enseñanza y aprendizaje, hay que ser conscientes de qué ventajas supondrá el uso de dicho elemento y cómo podría afectar al desarrollo del aprendizaje (Rodríguez et al., 2017).

En Cuba, El Centro Nacional de Educación a Distancia (CENED) fue creado en el 2015 y es el que orienta, dirige y controla el trabajo metodológico en esta modalidad, así como el desarrollo y aplicación de las tecnologías como medio de apoyo. Este centro tiene la responsabilidad de coordinar la formación de los docentes que trabajan en la EaD, ya sea como tutores, en la elaboración de los recursos educativos y/o en el sistema de evaluación. Por otra parte,

se ha notificado que se ha elaborado el modelo cubano de educación a distancia y deberá funcionar a través del modelo mixto, o sea, que esta se inserta en una institución tradicional de educación presencial (Antúnez et al., 2016).

Su modelo está enfocado en el Modelo de Educación a Distancia de la Educación Superior Cubana, se han asumido como principios generales, las dos ideas rectoras del proceso de formación para este nivel: la unidad entre la educación y la instrucción, y la vinculación del estudio con el trabajo. La posición asumida responde a la consideración de que los principios referidos son válidos para cualquier formación de profesionales o posgraduada, independientemente de la modalidad de estudio de que se trate.

Teniendo en cuenta las particularidades de la educación a distancia en Cuba se considera que el modelo debe potenciar los siguientes principios propios para esta modalidad de estudios: el principio de la flexibilidad, el principio de la interacción y la comunicación y el principio de la convergencia e integración tecnológica.

El Instituto Nacional de Tecnologías de la Comunicación (2008) dice que la principal particularidad de una plataforma educativa estriba en el uso masivo que los estudiantes hacen de ella. El futuro de la seguridad de las plataformas educativas, en opinión de los expertos, se divide entre los que consideran que el incremento de su utilización es directamente proporcional a los problemas de seguridad y los que consideran que habrá que estar alerta y adoptar una postura proactiva. Por otro lado, también menciona que existen diversas normas que repercuten en la seguridad de la información, tanto en el ámbito legislativo como relativas a las buenas prácticas. Ante la diversidad de amenazas que tienen o pueden tener las plataformas, es necesario realizar una estimación sobre la probabilidad de la ocurrencia de dichas amenazas y considerar los daños que causarían. Dicho análisis permite contrastar cuáles son los puntos fuertes (seguridad lógica, control de acceso, compra y desarrollo, ausencia de incidencias, concienciación y cumplimiento de la legislación) y las vulnerabilidades de las plataformas.

La seguridad de una aplicación web y por ende de un EVA depende del cumplimiento de algunos objetivos de seguridad tales como: autenticación, control de acceso, confidencialidad, integridad, disponibilidad, no repudio[2] y trazabilidad[3] (Rodríguez et al. 2017).

Estándares y normas para la seguridad de la información

[2] Proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, no pudiendo su receptor-transmisor negar que se haya producido.

[3] Proporcionar los controles que determinen que en todo momento se podrá determinar quién hizo qué y en qué momento.

Una plataforma educativa es un sistema de información bastante complejo debido a sus peculiares características, con funcionalidades muy variadas y un importante rango de usuarios, pero que comparte con cualquier otro sistema los problemas en cuanto a la definición de requisitos de seguridad y el control interno.

A continuación se detallan algunas de las normas internacionales y buenas prácticas, las cuales pueden ser utilizadas como referencia para desarrollar políticas y medidas de seguridad para las plataformas educativas, ya que están dirigidas, en general, a los sistemas de información.

La serie de estándares ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés). La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener los Sistemas de Gestión de la Seguridad de la Información (SGSI). Los rangos de numeración reservados por la ISO van de 27000 a 27019 y de 27030 a 27044. Las principales normas de esta serie son (Carnegie, 2019):

ISO 27001. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En su anexo A enumera, en forma de resumen, los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus Sistemas de Gestión de Seguridad de la Información.

ISO 27002. Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

COBIT

COBIT (Control Objectives for Information and related Technology) es una certificación creada por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés) y el Instituto de Gobernanza de las TIC (ITGI, por sus siglas en inglés). Además, COBIT es un marco de trabajo para el gobierno de las TIC que propone herramientas de apoyo que permiten a los directivos establecer relaciones entre los requisitos de control, las cuestiones técnicas y los riesgos del negocio (Cuzme et al., 2017).

La primera versión de los COBIT fue editada en abril de 1996, con el desarrollo de objetivos de control derivados del análisis y estudio de estándares y directrices internacionales, así como de buenas prácticas. Después se desarrollaron

directrices para realizar auditorías que evaluaran si estos objetivos de control se habían implantado adecuadamente. El contenido principal de los COBIT se divide en 34 procesos de TIC, y cada uno de ellos se cubre en cuatro secciones que contemplan como hay que controlar, gestionar y medir el proceso (Cuzme et al., 2017).

BS 7799

BS 7799 fue un estándar publicado originalmente por British Standard Institution (BSI) Group en 1995. Fue escrito por el Departamento de Comercio del Gobierno del Reino Unido e Industria (DTI) y constaba de varias partes. La primera parte, que contiene las mejores prácticas para SGSI, fue revisada en 1998, que finalmente fue adoptado por ISO como ISO17799, "Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información". La segunda parte de BS7799 fue publicada por BSI en 1999, conocido como BS 7799 y titulada "Sistemas de gestión de seguridad de la información - Especificación con guía de uso". BS 7799-2 se centró en cómo implementar SGSI, refiriéndose a la gestión de seguridad de la información estructurada y controles identificados en BS 7799-2, que posteriormente se convirtió en ISO 27001.

Conclusiones

El proceso de evaluación de seguridad de la información permite establecer el grado de confiabilidad en los EVA mediante un estudio exhaustivo de criterios previamente analizados y cuyos resultados pueden convertirse en el insumo de apoyo a la toma de decisiones en entidades educativas.

Los chequeos eficaces por parte de las plataformas para comprobar su seguridad, es una característica que se debería implementar en futuras versiones. Es por ello, que la caracterización y organización de las tecnologías informáticas encargadas de procesar dicha información permite ajustar estas medidas en correspondencia con la clase en la que se ubica dicha tecnología y por tanto favorece los procesos que se desarrollan en cada una de las entidades educativas.

La seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información. Este tipo de seguridad se orienta a proteger los activos de información, sin importar su forma o estado, valiéndose de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, para la aplicación y gestión de las medidas de seguridad apropiadas en cada caso.

Referencias

Antúnez Sánchez, A., Ramírez Sánchez, W., Rodríguez Valera, Y., Soler Pellicer, Y., & Flores Alés, A. (2016). La Educación a Distancia: Una Mirada En La Universidad de Granma, Cuba. Revista Didascalia. Publicación Cooperada Entre CEDUT-Las Tunas Y CEDEG-Granma, CUBA.

Bournissen, J. (2018). Modelo Pedagógico Para La Escuela de Estudios Virtuales.

Caballero, A. (2018). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. www.syngress.com.

Carnegie Mellon University. (2019). Computing Services Information Security Office. Information Security Essentials. http://www.cmu.edu/iso/aware/P2P/index.html

Cortés, M., Medina, F., Manzano, M., & León, J. (2020). Ventajas de La Plataforma Moodle Para La Enseñanza de Las Matemáticas En La Universidad de Cienfuegos. Revista Universidad Y Sociedad. 12 (6): 40–245.

Cruz, M., Hiraldo, R., & Estrada, V. (2011). El Aprendizaje Virtual Y La Gestión Del Conocimiento. Estudio de Caso de La Universidad Abierta Para Adultos, UAPA, República Dominicana. México. Revista de Educación a Distancia. 208.

Cuevas, R. (2015). Seguridad Informática En Las Empresas. Universidad Tecnológica de México (UNITEC). https://docplayer.es/6125952-Seguridad-informatica-en-las-empresas.html.

Cuzme, F., Suárez, L., Bracho, C., & Pupiales, C. (2017). Design of It Security Policies Based on Cobit 5 Reference Framework. Universidad Técnica Del Norte, Ecuador. https://www.researchgate.net/publication/318509533.

Domínguez, J. (2015). Seguridad Informática Personal Y Corporativa (Segunda Parte). IEASS, Editores. https://www.researchgate.net/publication/286371326_Seguridad_Informatica_Personal_y_Corporativa_Segunda_parte.

Fernandez, R. (2017). Instrumentos de Evaluación de Aprendizaje En Entornos Virtuales.

Gargallo C. & Felicitas, A. (2018). La Integración de Las TIC En Los Procesos Educativos Y Organizativos. Revista Educar, Curitiba, Brasil. 34 (69): 325–39.

Hamdi, H., Bouhoula, A. & Mosbah, M. (2007). A Software Architecture for Automatic Security Policy Enforcement in Distributed Systems. The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE).

Hiraldo, R.(2013). Uso de Los Entornos Virtuales de Aprendizaje En La Educación a Distancia. Universidad Abierta Para Adultos. Costa Rica.

Instituto Nacional de Tecnologías de la Comunicación. (2008). Estudio Sobre Medidas de Seguridad En Plataformas Educativas. Observatorio de La Seguridad de La Información. España. http://creativecommons.org/licenses/by-nc/2.5/es/.

Koschorreck, G. (2011). Automated Audit of Compliance and Security Controls. Sixth International Conference on IT Security Incident Management and IT Forensics, Stuttgart, Germany. 137–148.

López, R., Saucedo, L., & Escajeda, E. (2009). Ambientes Virtuales de Aprendizaje., Instituto Técnico Profesional. México.

Lopéz, R. (2017). Sistema de Gestión de La Seguridad Informática. Fondo Editorial Areandino. Fundación Universitaria Del Área Andina. 1.

Montesino, R. (2012). Modelo para la gestión automatizada e integrada de controles de seguridad informática. Universidad de las Ciencias Informáticas.

Nieles, M., Dempsey, K. & Yan, V. (2017). An Introduction to Information Security. National Institute of Standards and Technology Special. 800 (12): 1–101.

Rodríguez, A., Sánchez, B., María, H. & Caridad, M. (2017). Entornos Virtuales de Aprendizaje Como Apoyo a La Enseñanza Presencial Para Potenciar El Proceso Educativo. Revista Killkana Sociales. Universidad Católica de Cuenca. 1 (2): 7–14.

Rojas, N., Pérez, F., Torres, I. & Peláez, E. (2014). Las Aulas Virtuales: Una Opción Para El Desarrollo de La Educación Médica. EDUMECENTRO. 6 (2): 231–47.

Rojas, H. (2016). Seguridad de La Información, Seguridad Informática Y Ciberseguridad: ¿Son Sinónimos? https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridad- informática-y-ciberseguridad-son-sinónimos.

Romero, Luisa. (2010). La Seguridad Informática En El Trabajo Con La Plataforma Moodle. Revista de Humanidades. Universidad de Sevilla. 17: 169–90.

Sadowsky, G., Dempsey, J., Greenberg, A., Mack, B. & Schwartz, A. (2013). Information technology security and book. The International Bank for Reconstruction and Development. www.worldbank.org.

Santiso, H., Koller, J. & Bisaro, M. (2016). Seguridad En Entornos de Educación Virtual. Memoria Investigaciones En Ingeniería. no. 16.

Schonwalder, J., Bjorklund, M & Shafer, P. (2010). Network Configuration Management Using NETCONF and YANG. IEEE Communications Magazine. 48 (9): 166–73.

Shelupanov, A., Evsyutin, O., Konev, A., Kostyuchenko, E., Kruchinin, D. & Nikiforov, D. (2019). Information Security Methods—Modern Research Directions. Tomsk University of Control Systems and Radioelectronics (TUSUR). Russia.