SCIENTIAMERICANA ,Revista Multidisciplinaria
Volumen 2 Número 2, 2015

Seguridad de la información en plataformas virtuales de e- Learning
Information security virtual platform elearnig

Mario Roberto Monges Olmedo[1]

Artículo Recibido: 05/06/2015

Aceptado para Publicación: 15/07/2015

Resumen: Las plataformas de E-learning ofrecen numerosas ventajas a las universidades y usuarios, su campo 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. La metodología utilizada es la revisión bibliográfica en bases de datos internacionales especializadas en el tema. Son muchos los estudios que tratan sobre esos aspectos pero en muchos casos se deja de lado la seguridad, elemento fundamental en la transmisión integral del conocimiento. En este artículo se analiza la implementación de estándares de seguridad de la información como la ISO 27001. Se concluye el desconocimiento de este estándar por parte de los profesionales de las áreas de TICs según la bibliografía analizada.

Palabras Claves: Seguridad de la Información, Plataformas virtuales, E-learning.

Sumary: The E-learning platforms offer numerous advantages to universities and users, their field grows apace and are considerable impetus for existing initiatives. However, there have also been detected in some safety problems that hinder their implementation in the virtual platforms. The methodology used is the literature review in international data bases specialized in the subject. Many studies dealing with these issues but often neglects security, a key element in the comprehensive transfer of knowledge. This article describes the implementation of safety standards such as ISO 27001 information is analyzed ignorance of this standard by professionals in the areas of IT is concluded according to the literature reviewed.

Keywords: Information security, Virtual platforms, E-learning.

Introducción

Actualmente, se considera que vivimos la era de la información y que las sociedades de hoy encuentran su principal fundamento en el intercambio, generación y recreación de todo tipo de datos y contenido a nivel global. Es sabido que los Sistemas Virtuales de Formación

[1] Master en Ciencias de la Computación, Catedrático de Seguridad de la Información y Análisis de Riesgos de TI de la Universidad Nacional de Asunción – Facultad Politécnica. Asunción – Paraguay. Email. mario.monges@gmail.com

impregnan el mundo académico (Campus Virtuales) pero cada día más el de la empresa (Formación Continua). Las plataformas eLearning se nos presentan como herramientas adecuadas en estos contextos

Además, el e-learning continúa teniendo el problema de una cierta falta de confianza tanto por parte de las empresas como por parte del colectivo de profesores. Internet, las empresas y la filosofía "punto com" siguen considerándose como un medio no maduro. En general, se muestra una reticencia a pasar de la formación tradicional a un nuevo modelo de formación. El principal problema donde se focalizo el artículo de revisión nos plantea lo siguiente: ¿Cuál es el grado de seguridad de la información en la plataforma virtual de e-learning?

Como objetivo general del artículo encontramos Determinar el grado de seguridad de la información en la plataforma virtual de e-learning.

La justificativa de este trabajo es que con los esfuerzos por impedir, tecnológicamente hablando, que los contenidos web afecten la sensibilidad y desarrollo de los jóvenes, en muchos ámbitos de la sociedad se va imponiendo la educación en competencias digitales. Esto es, el cambio que se espera es un cambio interno, no sólo del control exterior a través de herramientas tipo anti firewall y demás. Se trata, pues, de la búsqueda de deseables en el desarrollo moral de los nativos digitales en la cultura web, es decir, el desarrollo de la capacidad para sopesar su propia exigencia frente a la de los otros.

La metodología utilizada es la revisión bibliográfica en bases de datos internacionales especializadas en el tema.

De la educación a distancia al e-learning

La educación a distancia fue creciendo a lo largo del siglo XX como una vía alternativa de formación en la que no se exigiesen las rigideces espacio-temporales propias de la docencia convencional (García Aretio, 2001) dirigida a aquellas personas que, bien por su situación geográfica (alumnos en zonas rurales), sus condiciones de trabajo (personas con poco tiempo para atender una enseñanza reglada), sus condiciones físicas

(personas con minusvalías) o bien por decisión personal, elegían una formación más acorde a sus necesidades (Marcelo et al., 2002).

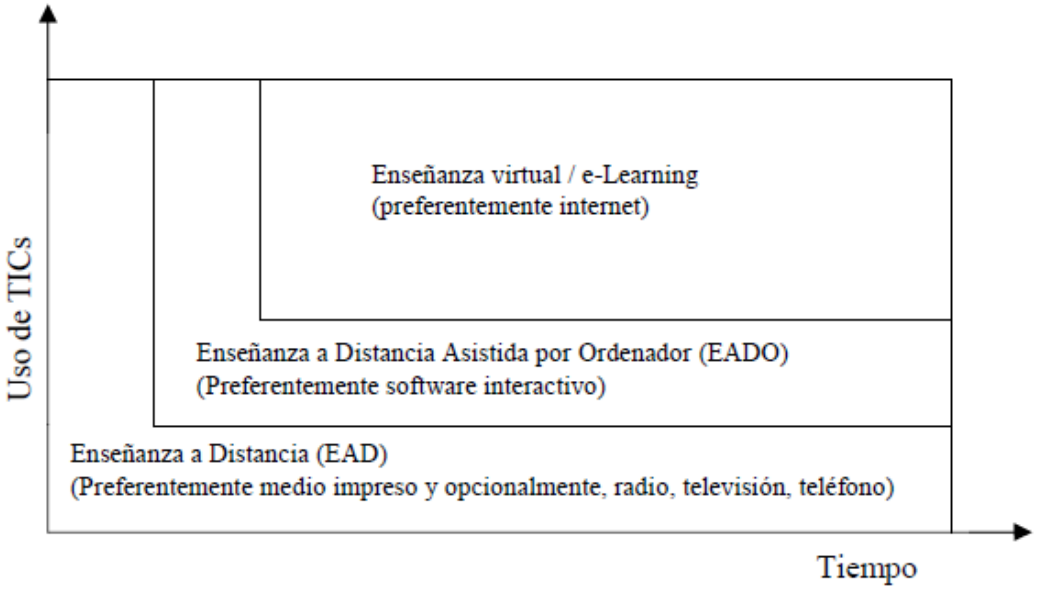

Figura 1. Etapas de la Educación a Distancia. Fuente: (Ruipérez, 2003)

Se puede definir el e-learning como "una enseñanza apoyada en las tecnologías de la información y la comunicación donde no es necesario el encuentro físico entre profesores y alumnos y cuyo objetivo es posibilitar un aprendizaje flexible (a cualquier hora y cualquier lugar), interactivo (con comunicaciones síncronas y asíncronas) y centrado en el alumno" (Martínez-Caro, 2005).

El e-learning presenta numerosas ventajas, las cuales tienen unos claros beneficiarios: Las empresas, las universidades, los usuarios finales y, en definitiva, la sociedad.

Ventajas para las Empresas	Ventajas para las Universidades	Ventajas para los Usuarios
✓ Reduce un 40-60% de coste respecto a la formación tradicional. ✓ Descentraliza la estructura empresarial. Permite impartir formación idéntica a todos los empleados de un determinado nivel, aunque trabajen en diferentes localizaciones geográficas de la misma empresa. ✓ Acceso a la formación de un mayor número de trabajadores (masa crítica). ✓ Fácil acceso a la formación y actualización del personal de la empresa, haciéndola más competitiva y eficiente. ✓ Crea hábitos de uso de nuevas tecnologías, que son aplicables posteriormente en el trabajo diario. ✓ Genera una cultura de Internet, que trasforma la comunicación y relaciones internas y externas, favoreciendo cambios organizativos y metodológicos.	✓ Permite a la universidad ofertar formación a las empresas sin los añadidos que suponen los desplazamientos, alojamientos y dietas de sus trabajadores. ✓ Permite a la universidad ampliar su oferta de formación a aquellas personas o trabajadores que no pueden acceder a sus cursos presenciales. ✓ Aumenta la efectividad de los presupuestos destinados a la educación: en muchos países los presupuestos de educación están congelados aunque la demanda aumenta. ✓ Responsabilidad del sistema educativo: los gobiernos no sólo esperan que las instituciones educativas mejoren su relación coste-eficacia, sino que también esperan que éstas justifiquen el uso que hacen del dinero público.	✓ Acceso en cualquier momento y en cualquier lugar. Disponibilidad del contenido 24x7 (24 horas del día, 7 días a la semana). ✓ Acceso a una amplia oferta formativa al superar las barreras geográficas. ✓ Agilidad en la comunicación. ✓ Alumno como sujeto activo y protagonista del proceso formativo. ✓ Personalización del aprendizaje (contenidos, ritmos de aprendizaje, tutorías, personalizadas). ✓ Mayor interacción entre participantes y profesores. Posibilidad de comunicación síncrona. ✓ Desarrollo de la formación en entornos colaborativos y dinámicos.

Tabla 1. Ventajas del e-learning para las empresas, universidades y usuarios. Fuente: (Bartolomé y Underwood, 1998) y (Formateca, 2003)

Información

La información es un activo que representa un gran valor dentro de la organización, sea este tangible o intangible, por lo tanto requiere una protección adecuada ya sea por diferentes medios o técnicas de seguridades implantadas. Para estos hay que tomar muy en cuenta el creciente ambiente interconectado de negocios es por esto que la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente (National Information Systems Security, 2000).

La información es el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador. El procesador del mismo requiere de información para cumplir una orden recibida, y toda tarea computacional implica el intercambio de un dato informativo de un lugar a otro. Esto no sólo ocurre en forma electrónica al interior del ordenador, sino que también es natural a las acciones que un usuario cualquiera ejecute con una computadora (Carlos Meyer, 2011).

Entre ellas, redactar un documento de texto, editar una imagen, reproducir o grabar un video, operar una calculadora son todas operaciones que implican un ingreso y egreso de información. Principalmente, aquellas actividades vinculadas a la Web tienen que ver con la búsqueda de información: navegar sitios de Internet, consultar enciclopedias, intercambiar mensajes con amigos y conocidos, crear un blog, etcétera.

Actualmente, se considera que vivimos la era de la información y que las sociedades de hoy encuentran su principal fundamento en el intercambio, generación y recreación de todo tipo de datos y contenido a nivel global.

Según (Morant, 1194) en el mundo de la informática, la unidad básica en la que trabajamos es definida como Dato, teniendo este concepto una aserción bastante general como un Carácter, una Representación o un Símbolo que se encuentra en forma aislada, sin un contexto determinado y sin un debido ordenamiento.

Esta asignación, orden o contexto está dado mediante el Conjunto de Datos que son procesados, que en informática esta misión está dada justamente por la Unidad Central de Procesamiento (CPU, también llamada Procesador) mediante la cual se obtiene una cantidad variable de Datos Organizados, que se significan y pueden ser interpretados.

Esta interpretación es entonces considerada como una Información, el concepto que analizaremos a continuación y que daremos una breve descripción para poder entender cómo funciona básicamente un equipo, las Aplicaciones que sobre él se ejecutan y los distintos Procesos que giran en torno al equipo.

Definimos entonces un Proceso de Comunicación del equipo como una de las formas de comunicación mediante Datos Binarios, que al tratarse de un Circuito Electrónico Cerrado, se define por ceros y unos que representan la transmisión o no-transmisión de impulsos eléctricos, teniendo entonces una comprensión de los mismos por parte de un dispositivo Emisor, como también por otro Receptor de estas señales eléctricas.

Este concepto de Información a su vez desglosa distintos conceptos que parten desde esta comunicación básica entre dispositivos eléctricos que forman parte de un Ordenador, por lo que también tenemos distintos niveles en los que se considera a la Información, teniendo por ejemplo los datos que estén contenidos en un Medio de Almacenamiento, como también los que son enviados o recibidos en una Red de Equipos determinada.

Es por ello que la Informática ahora contempla además como Información a la que es transmitida por la Red de Redes, teniendo por caso el análisis y gestión del envío de la Información en Internet, como también controlar qué es lo que allí se difunde, qué puede mostrarse y hasta qué contenidos estén cumpliendo o no con distintas normativas vigentes.

El concepto entonces de Información está aplicado no solo a lo que es el envío y recepción de datos dentro de un sistema cerrado, sino también a lo que respecta a la Comunicación Entre Equipos, como también qué es lo que comparten los usuarios con el mundo, siempre considerándose de que Datos Aislados no constituyen nada por sí mismos, sino que requieren de un debido Procesamiento para poder ser contextualizados y transformados en Información

Seguridad de la información

Últimamente se viene dando el cambio a seguridad de la información como traducción más adecuada de information security. Pero peso a ello todavía hay muchos especialistas que siguen llamando así al puro enfoque técnico.

En realidad la seguridad de la información es bastante más amplia, ya que no es simplemente una cuestión técnica sino responsabilidad de la alta gerencia y cuadros directivos de una organización (Carlos Meyer, 2010).

En tal sentido hay que tener en cuenta que el ambiente TIC tiende a estar orientado al servicio y actuar como función habilitante de los procesos de negocios. En esto difiere de los procesos centrales mismos de una organización que constituyen el núcleo de los negocios de una empresa.

De hecho, sin el involucramiento activo de las unidades y líderes de negocio, ejecutivos, directorio y steering-committee, no puede existir un plan sustentable de seguridad de la información, a partir de los riesgos determinados. Y todo esto dentro del sistema de dirección y control propio de un adecuado gobierno corporativo, como define la OECD (Organización para la Cooperación y Desarrollo Económico, OCDE en español) al corporate governance.

Ahora se trata, entre otras cosas, de considerar también la gente, los procesos y funciones de negocio, la protección de todos los activos/recursos de una organización. Donde toda la empresa es la impulsora, propietaria y beneficiaria de la seguridad de la información, en un marco de responsabilidades compartidas.

Esto implica entonces que para el marco de la seguridad de la información se requiere considerar no sólo los riesgos técnicos de TIC, sino también los riesgos de seguridad que se extienden a toda la empresa, es decir: organizacionales, operacionales y físicos.

Seguridad de la información vs Seguridad informática

Un ejemplo práctico es que la Seguridad Informática (IT Security) se describe como la distinción táctica y operacional de la Seguridad, mientras la Seguridad de la Información (Information Security) sería la línea estratégica de la Seguridad.

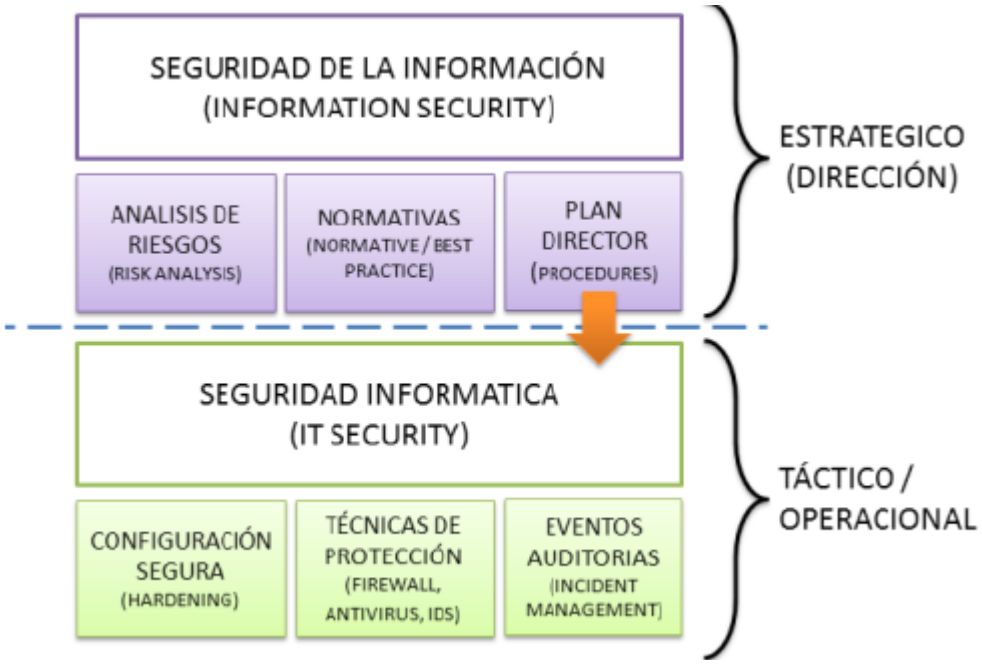

Figura 2. Diferencia entre seguridad de la información y seguridad informática. Fuente: Elaboración propia.

Sistema de gestión de la seguridad de la información (SGSI)

El modelo PDCA también conocido como el círculo de la calidad de Deming, se usa principalmente para determinar, implementar, monitorear, controlar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI).

Figura 3: Modelo PDCA. Fuente: Elaboración propia.

- **Planificar (diseñar el SGSI)**

En la fase de diseño, se desarrolla y se documenta las políticas de seguridad de la información. Aquí se definen los objetivos de seguridad de la información, los procesos relevantes y procedimientos; de esta manera se asegura que se gestionan los riesgos.

- **Hacer (Do – implementar el SGSI)**

En esta fase, se implementa la política de seguridad de la información y los procedimientos y medidas subyacentes.

- **Monitorear (Check – Monitorear el SGSI)**

En esta fase, se realiza el control utilizando autoevaluaciones (auditoria interna) y en lo posible se toman medidas para ver si la política de seguridad de la información se está cumpliendo correctamente.

- **Actuar (mantener y ajustar el SGSI)**

En esta fase, se realizan correcciones y se llevan a cabo medidas preventivas, basados en los resultados de las auditorías internas. EL SGSI se actualiza a la luz de nuevos requerimientos.

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, con acompañamiento de técnicos especialistas en Normalización del INTN 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 vigencia a partir de octubre de 2014, es un estándar auditable y certificable en seguridad de la información.

Esta norma contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos 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.

Contiene un total de 14 Dominios, 35 Objetivos de Control y 114 Controles.

Por qué debe ser segura una plataforma educativa

Las plataformas educativas, como cualquier otra aplicación de software, debe cumplir unos mínimos estándares de seguridad que garanticen su correcto funcionamiento, de forma que esté disponible cuando se necesite, existan garantías de que los datos se procesarán adecuadamente y que solo accederán a ella las personas autorizadas.

La principal particularidad de una plataforma educativa estriba en el uso masivo que los menores hacen de ella. En cualquier otra aplicación, hay un colectivo de usuarios que se segmentará en función de sus necesidades y atribuciones. Sin embargo, en este caso, una

parte muy significativa de este colectivo son menores de edad, por lo que hay que ser muy cuidadoso con la información a la que tienen acceso y la que se recoge de ellos, tanto para cumplir escrupulosamente la ley como para reducir los riesgos y evitar posibles incidentes. (INTECO, 2008)

El futuro de la seguridad de las plataformas educativas, 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.

Existen diversas normas que repercuten en la seguridad de la información, tanto en el ámbito legislativo como relativas a las buenas prácticas.

Expectativa de los usuarios

Los potenciales usuarios de estas plataformas son todos los actores de la comunidad educativa: administradores de centro, alumnos, profesores, padres, Administración pública, etc. Además de estos usuarios finales, tanto los desarrolladores como el personal que ofrece soporte a estas herramientas están muy interesados en que tengan un adecuado nivel de seguridad.

En general, todos estos usuarios tienen una visión muy concreta de qué esperan de las plataformas en cuanto a su seguridad. A grandes rasgos y con distintos matices, todos coinciden en que:

- La información y los datos personales no deben trascender a usuarios no autorizados, o simplemente a quien no afecte esa información. Por ejemplo, que las calificaciones de un alumno no sean visibles para los padres de otro. Independientemente de la consideración que por ley le corresponda, la información manejada en el ámbito educativo es muy sensible para sus usuarios, por lo que preservar la confidencialidad es fundamental.

- El control de accesos debe ser seguro. No se debe poder acceder a información indebida, solo a aquella relacionada con los trabajos y actividades que se llevan a cabo habitualmente, para evitar que alguien utilice fraudulentamente la información que almacenamos.
- Las plataformas deben estar disponibles siempre que se necesiten, por los múltiples trastornos que ocasionan si no es así: clases canceladas, trabajos no entregados, tareas administrativas retrasadas, etc. Dado que se utilizan para el trabajo cotidiano de muchas personas, es básico que las aplicaciones no tengan fallos de disponibilidad. Si un profesor que ha preparado su clase no puede acceder a ella en el momento de impartirla, o en el instante de preparar un trabajo no se puede acceder a las herramientas, puede disminuir sensiblemente el grado de utilización de las plataformas.
- Las plataformas deben ser fiables y de fácil utilización, de forma que cualquiera de los usuarios, por bajo que sea su nivel de conocimientos de informática, pueda hacer un uso eficaz y eficiente de los recursos disponibles. Además, debido a que los usuarios dan mucha credibilidad a lo que aparece en los sistemas de información de su entorno educativo, es importante que la información que almacenan sea correcta, completa y fiable. (INTECO, 2008)

Conclusión

La importancia que tienen las plataformas educativas como instrumentos para acercar las tecnologías a la educación hace que resulte necesario desarrollar estudios que analicen la seguridad en estos nuevos entornos virtuales de trabajo. Por el mismo es imperioso que participen todos los actores como directores, programadores y usuarios de plataformas educativas para poder relevar información para un análisis de brechas y así poder elaborar un plan de seguridad y con el mismo poder gestionar los riesgos de TICs.

Referencias

Álvarez, G., y Pérez, P.(2004).Seguridad informática para empresas y particulares. McGraw-Hill.

Bartolomé, a. R.; underwood, j. D. M. Teeode. (1998) Technology Enhanced Evaluation in Open and Distance Education. Barcelona: Universidad de Barcelona. FORMATECA. E-Learning. Visión y Tendencias. Albacete: Génesis XXI. 2003.

García Aretio, L. La Educación a Distancia. De la Teoría a la Práctica. Barcelona: Ariel Educación. 2001.

INTECO. Estudio sobre medidas de seguridad en plataformas educativas. Madrid, España. 2008.

MARCELO, C.; PUENTE, D.; BALLESTEROS, M. A.; PALAZÓN, A. E-Learning - Teleformación. Diseño y Desarrollo de la Formación a través de Internet. Barcelona: Gestión 2000. 2002

Martínez-Caro, E. La Mejora de la Calidad en la Educación mediante Entornos Virtuales de Aprendizaje. Tesis Doctoral, Universidad Politécnica de Cartagena. 2005 MEYER, C. ¿Seguridad informática vs. Seguridad de la información? Buenos Aires. Argentina. 2010.

NP ISO 27001:2014 - Tecnología de la información–técnicas de seguridad–sistemas de gestión de la seguridad de la información–requisitos. Asunción, Paraguay. 2014. RUIPÉREZ, G. Educación Virtual y eLearning. Madrid: Biblioteca AUNA Fundación. 2003.