MODELO DE SEGURIDAD INFORMÁTICA PARA LA MINIMIZACIÓN DEL RIESGO EN ENTORNOS EDUCATIVOS VIRTUALES DE EDUCACIÓN SUPERIOR

Informatics security model for minimizing information risk in virtual educational environments of higher education

Chavez Salazar, Victor Hugo
Docente
Universidad Mayor de San Andrés
vicocba@gmail.com
La Paz, Bolivia

RESUMEN

En esta investigación se presenta el proceso de minimización del nivel de riesgo de la información en entornos educativos virtuales en educación superior a través del análisis y diseño de un modelo de seguridad informática, tomando en cuenta conceptos referidos a la seguridad informática, los entornos educativos virtuales y los riesgos informáticos. La investigación tiene una aproximación metodológica de enfoque cuantitativo con base empírica que tomo en cuenta una muestra aleatoria de una población. El desarrollo del modelo identifica siete fases donde se seleccionan perfiles de usuario, se aplican métodos, se plantean técnicas de recolección de datos y se adecuan componentes, estándares, fases, controles y procedimientos de seguridad para el planteamiento de un árbol general de requerimientos.

Palabras clave: modelo, seguridad informática, riesgo, entornos educativos virtuales

Abstract

This research presents the process of minimizing the level of information risk in virtual educational environments in higher education through the analysis and design of a computer security model, taking into account concepts related to computer security, virtual educational environments. and computer risks. The research has a methodological approach with a quantitative approach with an empirical basis that takes into account a random sample of a population. The development of the model identifies seven phases where user profiles are selected, methods are applied, data collection techniques are proposed and components, standards, phases, controls and security procedures are adapted for the formulation of a general tree of requirements.

Keywords: model, computer security, risk, virtual educational environments

INTRODUCCIÓN

La implementación de tecnologías de información en las universidades ha generado nuevas modalidades de realizar delitos informáticos, así como el uso no autorizado de sistemas informáticos, accesos no autorizados, manipulación de datos de entrada, manipulación de programas, manejo de datos de salida y la alteración de los datos almacenados en medios electrónicos.

La seguridad informática es un aspecto muy importante a ser tomado en cuenta dentro de los entornos educativos virtuales de una universidad, y toma más relevancia hoy en día en el sentido de que un entorno educativo virtual debe formar parte de la estrategia didáctica de cada docente después de la experiencia vivida por la aparición de la pandemia COVID-19.

Un entorno educativo virtual es un repositorio digital donde la tecnología ha cambiado la forma de enseñanza y la aplicación de estrategias didácticas por parte de los docentes dentro del sistema universitario nacional y más con lo ocurrido a raíz de la pandemia del COVID-19.

Según Fernandez (2018) los ambientes virtuales de aprendizaje representan una oportunidad para transformar los procesos de enseñanza-aprendizaje en las universidades bolivianas, adaptándose a las nuevas necesidades y tendencias de la educación superior en la era digital.

Arango (2019), arguye que seguridad informática en las universidades es un aspecto fundamental que no debe descuidarse, ya que los ataques cibernéticos pueden comprometer la integridad de los datos académicos, investigaciones y sistemas críticos.

Asimismo, un riesgo informático es la posibilidad de que un evento adverso cause daño a un sistema informático y pueden tener un impacto significativo en las universidades por lo que es importante tomar medidas para gestionarlos de una manera adecuada.

Para este autor, la aparición del COVID-19 cambio la forma de vida de toda la humanidad y especialmente en las universidades el uso de entornos educativos virtuales tomo bastante relevancia y recién se tomó en cuenta como una alternativa para que los estudiantes puedan aprender y formarse en un área de conocimiento sin asistir a un aula de manera presencial.

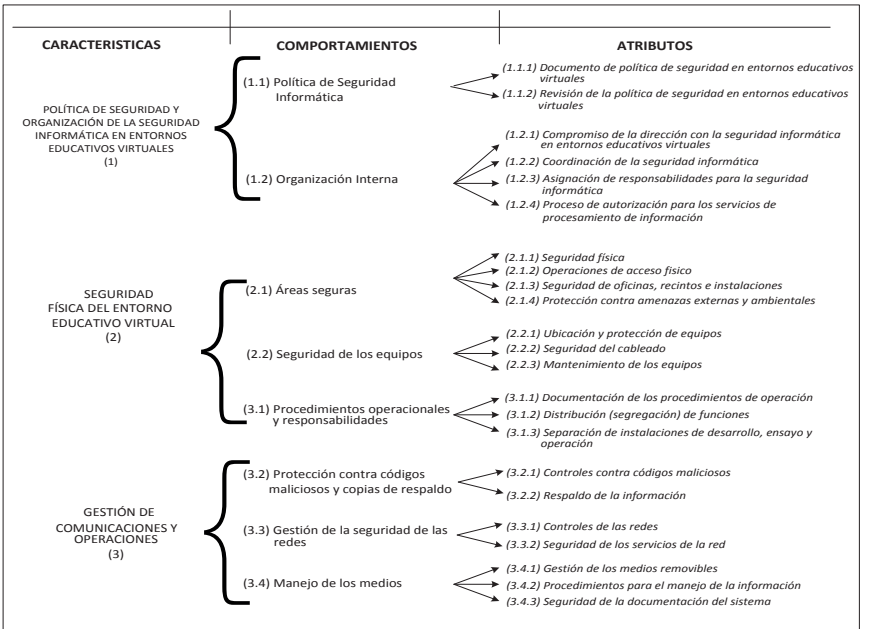
En esta investigación se describe el proceso de minimización del nivel de riesgo de la información en entornos educativos virtuales en educación superior a través del análisis y diseño de un modelo de seguridad informática.

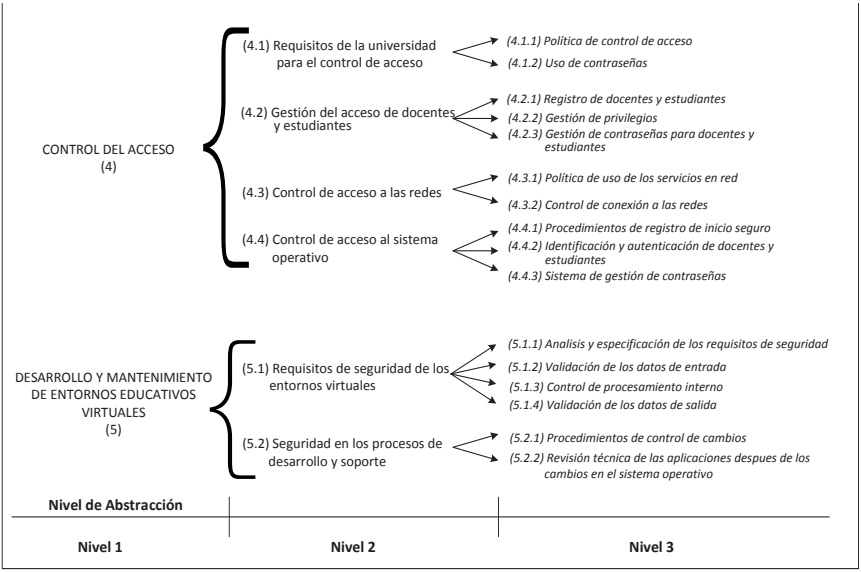
La investigación tiene una aproximación metodológica de enfoque cuantitativo con base empírica que tomo en cuenta una muestra aleatoria de una población, en este caso todos los docentes y estudiantes que se relacionaron de alguna manera con la creación, manejo, interacción y administración de entornos educativos virtuales.

DESARROLLO

Un aspecto muy importante para la presente investigación es plantear un árbol general de requerimientos para analizar, evaluar y comparar los diferentes controles que deben ser tomados en cuenta en un modelo de seguridad informática en base a características, comportamientos y atributos. El árbol general de requerimientos se observa en la Figura 1 y tiene como "base" los conceptos y lineamientos definidos en los estándares ISO 27001 e ISO/IEC 27000 (ISO/IEC, 2011).

Figura 1 Árbol General de Requerimientos





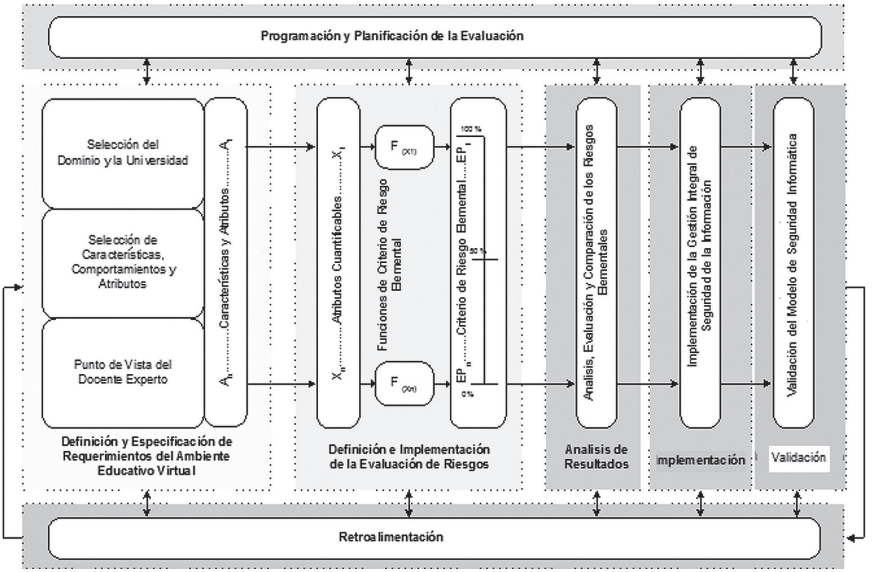
Las fases principales del modelo son las siguientes:

- FASE 1.- Fase de planificación y programación de la evaluación de la seguridad informática en el entorno educativo virtual
- FASE 2.- Definición y especificación de requerimientos del entorno educativo virtual
- FASE 3.- Definición e implementación de la evaluación de la seguridad y riesgos
- FASE 4.- Análisis de resultados
- FASE 5.- Implementación
- FASE 6.- Validación
- FASE 7.- Retroalimentación

En la Figura 2 se observa el modelo donde se identifican las relaciones entre cada una de las fases.

Figura 2

Fases del modelo de seguridad informática en entornos educativos virtuales



Fase de Planificación y Programación de la Evaluación de la Seguridad Informática en el Entorno Educativo Virtual

Definición del Dominio y Universidades de Evaluación

Según Chavez (2016), citando a Velásquez (2009) "define al dominio como un sistema real o abstracto del universo que existe independientemente del sistema de evaluación. El dominio debe tener un conjunto de entidades a los que se atribuyen propiedades que manifiestan un comportamiento y se relacionan entre sí. De manera que, el dominio se considera como la universidad a ser evaluada y a las entidades que serán objeto de análisis, comparación y medición".

Definición del Objetivo y Cronograma de Evaluación

De acuerdo a Chavez (2016) "el objetivo representa los propósitos que se debe alcanzar en el dominio a ser evaluado, aplicando las fases del modelo referidas a la definición e implementación de evaluación de riesgos, el análisis de resultados y la implementación".

"El cronograma de evaluación genera un "programa de acción", que se define como un instrumento que ayuda a alcanzar el objetivo trazado, por medio de la planificación de las tareas que se realizaran en cada fase, las entidades donde se realizara la recolección de datos y la estimación de tiempos para concluir toda la investigación" (Chavez, 2016).

Fase de Definición y Especificación de Requerimientos del Entorno Educativo Virtual

Selección del Perfil de Usuario

De acuerdo a Chavez (2016), para la elaboración del modelo se consideran los siguientes perfiles de usuario:

- "Docente", "por la relación que tiene en la parte de enseñanza en entornos educativos virtuales. El perfil del docente considera el conocimiento profundo y conocimiento de las principales características, comportamientos y atributos de la seguridad informática en entornos educativos virtuales" (Chavez. 2016).

- "Estudiante", "por la participación directa como parte de un entorno educativo virtual. El perfil del estudiante también considera el conocimiento profundo de las principales características, comportamientos y atributos de la seguridad informática en entornos educativos virtuales" (Chavez, 2016).

"Siguiendo un mecanismo de categorización y descomposición a mayor detalle, se divide a la categoría "Docente" en clases específicas, como ser: "Docente Participante" y "Docente Experto", además, los docentes participantes, serán descompuestos en audiencias específicas: docentes casuales y docentes iníciales" (Chavez, 2016).

- "El Docente Casual, se define como la audiencia que utiliza un entorno educativo virtual aleatoriamente, y donde la implementación está pensada para ser usada una sola vez" (Chavez, 2016).

- "El Docente Inicial, se define como a la audiencia que tiene al menos algún conocimiento o manifiesta algún interés por utilizar un entorno educativo virtual y la implementación está pensada para ser usada de manera continua" (Chavez, 2016).

El Docente Experto, tiene el perfil de que es un especialista para crear, manejar y gestionar un entorno educativo virtual, forman parte de este grupo los administradores de la plataforma virtual, los docentes de las áreas de tecnologías de información y comunicación y los analistas de sistemas, entre otros.

Representación de las Características, Comportamientos y Atributos

En este proceso se deben acordar y especificar las características, comportamientos y atributos que tendrá el modelo de acuerdo a la definición del dominio y las entidades sujetas a evaluación.

Fase de Definición e Implementación de la Evaluación de la Seguridad y Riesgos

"En esta fase se toman en cuenta diferentes tipos de escalas de riesgo, funciones, valores y rangos críticos para encontrar el indicador de riesgo para cada atributo cuantificable que permita realizar el proceso de medición de cada característica, comportamiento y atributo de la seguridad informática en entornos educativos virtuales" (Chavez, 2016).

Criterio de Seguridad

Para analizar y evaluar el nivel de seguridad de un entorno educativo virtual, se tendrán en cuenta los siguientes criterios:

a) **Integridad:** Es la propiedad que busca mantener la información exactamente cómo fue generada, protegiéndola de modificaciones accidentales y/o intencionales.
b) **Disponibilidad:** Es la cualidad, característica o condición que posee la información de encontrarse disponible de quienes quieran acceder a ella.
c) **Confidencialidad:** Es la capacidad para prevenir la divulgación parcial o completa de la información sensible a terceros.

Criterio de Riesgo Elemental

"El criterio de riesgo elemental se define como un "riesgo básico" que forma parte de un riesgo principal, es decir que el nivel de análisis de complejidad de un criterio de riesgo elemental es menor a un criterio de riesgo principal. Para el presente estudio, se tomará en cuenta el criterio de riesgo elemental para medir las características, comportamientos y atributos del modelo" (Chavez, 2016).

Según Chavez (2016) citando a Fenton et.al. (2007) "para cada atributo cuantificable $\boldsymbol{A_i}$, se debe asociar y determinar una variable $\boldsymbol{X_i}$ que procede a tomar un valor real a partir de un proceso de medición. Además, para cada variable $\boldsymbol{X_i}$ computada, por medio de un criterio elemental, se producirá un indicador de riesgo elemental por cada sección en el diseño del modelo $\boldsymbol{(EP_i)}$, el resultado final obtenido se interpreta como el grado o porcentaje del requerimiento del Docente Experto satisfecho para el atributo $\boldsymbol{A_i}$".

Análisis de Resultados

"En la fase de análisis de resultados se realizan actividades de análisis y comparación de riesgos con los datos obtenidos a través de las encuestas por cada característica, comportamiento y atributos del árbol general de requerimientos" (Figura 1) y justificando cada resultado mediante el empleo de tablas y figuras que muestren los datos consolidados obtenidos en la investigación" (Chavez, 2016).

Fase de Implementación

"En esta fase, se definen objetivos, controles y procedimientos de implementación para cada una de las características, comportamientos y atributos del árbol general de requerimientos (Figura 1) que se basan en los conceptos definidos en los estándares ISO 27001 e ISO/IEC 27000 (ISO/IEC, 2011) que fueron aplicados y adaptados a los objetivos del presente estudio" (Chavez, 2016).

Fase de Validación

Según Chavez (2016) "en esta fase, se realiza la validación de modelo en una universidad, tomando en cuenta los objetivos, controles y procedimientos de implementación para cada una de las características, comportamientos y atributos del árbol general de requerimientos" descritos en la Figura 1.

Fase de Retroalimentación

De acuerdo a Chavez (2016) "es un proceso iterativo del modelo que se realiza para la minimización de riesgos, por cada característica, comportamiento y atributo resultante de cambios en el contexto interno o externo en los entornos educativos virtuales de las universidades. En esta etapa se deben mantener los valores de los pesos que son obtenidos de la evaluación de riesgos por cada característica del modelo para medir el nivel de minimización de riesgo antes y después de la implementación del modelo. La retroalimentación es una fase importante del modelo ya que vuelve a iniciar el proceso de la Fase 1 a la Fase 6 hasta que el Indicador Global de Riesgo Controlado Total se encuentre en el intervalo de Satisfactorio (61% a 100%)".

DISCUSIÓN

El modelo es holístico e integral, abarcando un conjunto estructurado de estrategias, métodos y técnicas que, al aplicarse sistemáticamente en las distintas fases del modelo, permiten alcanzar un resultado deseado.

La solidez del modelo tiene gran importancia en su capacidad para facilitar procesos con resultados consistentes y replicables en el tiempo. Esto se debe

a su naturaleza sistemática y estructurada, que garantiza la coherencia de los resultados.

Asimismo, el modelo es flexible, ya que permite la incorporación o eliminación de características, comportamientos y atributos de forma modular. Esta modularidad, junto a la idea de alta cohesión y bajo acoplamiento, facilita la adaptación del enfoque a diferentes contextos y necesidades específicas para mejorar la seguridad informática minimizando los riesgos en ambientes educativos virtuales de una universidad.

En la era digital actual, la seguridad informática se ha convertido en una necesidad importante para una universidad por el manejo de información sensible. La proliferación de ciberataques, el robo de datos y las filtraciones de información ponen en riesgo la confidencialidad, integridad y disponibilidad de la información, lo que puede tener consecuencias graves para las universidades, es por ese motivo que el modelo planteado reduce las vulnerabilidades en los entornos educativos virtuales, dificultando el acceso no autorizado a la información sensible.

CONCLUSIONES

Se definió un árbol general de requerimientos clasificado y relacionado de acuerdo a la necesidad de un entorno educativo virtual de una universidad y que está basado en la definición de características, comportamientos y atributos que toma en cuenta los estándares ISO 27001 e ISO/IEC 27000 referidos a la seguridad informática.

Se diseñó un modelo de seguridad informática completo y adaptable a las necesidades de las universidades aplicando técnicas, métodos y criterios rigurosos, así como en la adecuada selección de componentes, estándares, fases, controles y procedimientos de implementación, de esta manera, se garantiza la protección de la información y la infraestructura tecnológica en entornos educativos virtuales.

Se evidenció que la gestión de riesgos informáticos debe ser un proceso continuo y cíclico dentro del modelo, ya que se debe evaluar periódicamente los riesgos a los que está expuesta una universidad para mantener la eficacia del modelo y garantizar que se adapta a nuevas amenazas informáticas y vulnerabilidades.

Se mostró que una parte importante del modelo para la minimización de los riesgos es que los docentes y estudiantes tomen consciencia de la importancia de saber cómo interactuar dentro de un ambiente educativo virtual de forma segura a través del cumplimiento de las políticas de seguridad informática establecidas por la universidad.

REFERENCIAS BIBLIOGRÁFICAS

Arango, S. (2019). *Seguridad Informática en la Universidad*. Editorial Universitaria.

Chavez V. (2016). Desarrollo de un Modelo de Seguridad de la Información en Ambientes Educativos Virtuales. *Revista Científica de Publicación del Centro Psicopedagógico y de Investigación en Educación Superior.* Vol. 1 N. 1, 15-30.

Fenton et al. (2007). *Software Metrics: A Rigorous and Practical Approach*. PWS Publishing Company, 2nd. Edition.

Fernández Calderón, J. C. (2018). *Entornos Virtuales de Aprendizaje en la Educación Superior Boliviana*. Editorial Universitaria Boliviana.

ISO/IEC, (2011). *Norma ttécnica de tecnología de la información 27000-27001*. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Velásquez M. (2009). *Ceros y unos: La economía de la información, 2da. Edición, Prentice Hall*.

Fecha de recepción: 31 de mayo, 2024

Fecha de aceptación: 20 de julio, 2024