DESARROLLO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN EN AMBIENTES EDUCATIVOS VIRTUALES

Por: Victor Hugo Chavez Salazar
Postulante a Doctor en Educación Superior
CEPIES - UMSA
vicocba@gmail.com
La Paz - Bolivia

DESARROLLO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN EN AMBIENTES EDUCATIVOS VIRTUALES

INFORMATION SECURITY MODEL DEVELOPMENT IN VIRTUAL EDUCATIVE ENVIRONMENT

Por: Victor Hugo Chavez Salazar
Doctorante CEPIES UMSA

Abstract

The field of the security of the information is a discipline that is responsible for protecting the integrity and privacy of information stored on a computer medium that is why there are various components, standards, controls, and procedures internationally recognized. The model identifies six phases where to apply techniques, methods, criteria and fit components, standards, stages, controls and implementing procedures to optimize the security of the information in educational virtual environments.

This work presents the process of developing a model of information security in educational virtual environments of higher education which is an analysis of security of information, and other concepts that predominate in the analysis and design of the model.

Key words

Information security, components, standards, controls, procedures, methods, virtual learning environments.

Resumen

El campo de la seguridad de la información es una disciplina que se encarga de proteger la integridad y privacidad de la información almacenada en un medio informático, por esa razón existen diversos componentes, estándares, controles y procedimientos reconocidos internacionalmente. El modelo identifica seis fases donde se aplican técnicas, métodos, criterios y se adecuan componentes, estándares, fases, controles y procedimientos de implementación para optimizar la seguridad de la información en ambientes educativos virtuales.

Este trabajo presenta el proceso de elaboración de un modelo de Seguridad de la Información en Ambientes Educativos Virtuales de Educación Superior que se constituye en un análisis de estándares de seguridad de la información, y otros conceptos que predominan en el análisis y diseño del modelo

Palabras clave

Seguridad de la información, componentes, estándares, controles, procedimientos, métodos, ambientes educativos virtuales.

1. Introducción

La seguridad de la información en ambientes educativos virtuales de educación superior es un área clave en la responsabilidad del manejo de la información tanto por parte del docente y del estudiante para que administren, desarrollen y culminen un curso virtual de manera exitosa. El desarrollo de ambientes educativos virtuales en los últimos años ha sido importante en todas las universidades y es una forma de aprendizaje colaborativo[1] que merece el apoyo de la alta dirección. Asimismo, las funciones de seguridad de la información y continuidad operativa deben tener el apoyo de las altas autoridades para el desarrollo y para que los ambientes educativos virtuales que se diseñen cuenten con los recursos tecnológicos necesarios [Del Carpio, 2011].

Los niveles de seguridad establecidos en los instructivos de seguridad de cada universidad deben estar enmarcados en los intereses y los objetivos de cada ambiente educativo virtual [Calvo, 2010], y deberían tener las siguientes características:

a) Nivel de protección para el hardware y software
b) Identificación de usuarios en el ambiente educativo virtual.
c) Derecho de acceso a programas e información para cada estudiante.
d) Características adicionales que crean un ambiente educativo virtual de acceso controlado.
e) Capacidad de restringir a los usuarios no autorizados para que formen parte de un entono de educación virtual.

Por todo lo anterior, el presente trabajo se enmarca en el desarrollo de un Modelo de Seguridad de la Información en Ambientes Educativos Virtuales (MSIAEV) que se implemente en una universidad.

2. Seguridad de la información en ambientes educativos virtuales

Entendemos por ambiente educativo virtual al espacio físico donde las nuevas tecnologías tales como los sistemas satelitales, el Internet, la multimedia, y la televisión interactiva entre otros, se han potencializado rebasando al entorno universitario tradicional que favorece al conocimiento y a la apropiación de contenidos, experiencias y procesos pedagógico-comunicacionales de una manera más integral y eficiente.

En un ambiente educativo virtual intervienen los estudiantes, el docente, los contenidos educativos, la evaluación y los medios de información y comunicación. Los ambientes de aprendizaje no se circunscriben a la educación universitaria tradicional, ni tampoco a una modalidad educativa particular, se trata de aquellos espacios en donde se crean las condiciones para que el estudiante se apropie de nuevos conocimientos, de nuevas experiencias, de nuevos elementos que le generen procesos de análisis, reflexión y apropiación, reciben el nombre de “virtuales” en el sentido que no se llevan a cabo en un lugar predeterminado y porque el elemento a distancia está presente [Daltabuit, 2011].

La UNESCO[2] en su informe mundial de la educación, señala que los entornos de aprendizaje virtuales constituyen una nueva forma de tecnología educativa y ofrecen una serie de ventajas para impartir

[1] Sistema de interacciones cuidadosamente diseñado que organiza e induce la influencia recíproca entre los integrantes de un equipo.
[2] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, que contribuye a la paz y a la seguridad en el mundo mediante la educación, la cultura y las comunicaciones.

cursos dentro de las universidades de todo el mundo.

El entorno de aprendizaje virtual es definido como un programa informático interactivo de carácter pedagógico que posee una capacidad de comunicación integrada, es decir, que está asociado a las nuevas tecnologías de información y comunicación, estos nuevos entornos de aprendizaje favorecidos con la incorporación de las tecnologías se potencian en la Educación a Distancia por ser un modelo donde la no presencia física entre quien enseña y quien aprende es su principal característica.

Muchos ambientes educativos virtuales no son diseñados para ser seguros, la seguridad que se logra a través de los medios técnicos es limitada y está condicionada a realizar una buena gestión supervisada por procedimientos apropiados. La identificación de los controles que se deben establecer requiere planificación y una atención cuidadosa a los detalles (*Cardenas*, 2012).

Un "Modelo de Seguridad de la Información en Ambientes Educativos Virtuales" es una herramienta de gestión que permite conocer, gestionar y minimizar los riesgos que atentan contra la seguridad de la información de un curso virtual que imparte una universidad, también nos permite analizar y ordenar la estructura del ambiente educativo virtual, así como facilitar la definición de procedimientos de trabajo para mantener la integridad de la información. La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad de los cursos virtuales, minimizar el riesgo y maximizar el retorno de inversiones. La seguridad de la información se logra implementando un conjunto apropiado de controles incluyendo políticas, procesos, procedimientos, estructuras y funciones de software y hardware. Los controles deben ser establecidos, implementados, monitoreados, revisados y mejorados, para asegurar que se cumplan los objetivos específicos de seguridad de un curso virtual impartido por una universidad (*Herrera*, 2010).

Para este autor, la gestión de la seguridad de la información requiere, la participación de todos los docentes y estudiantes de la universidad, accionistas, proveedores, terceras partes, clientes y partes externas para que el Modelo de Seguridad de la Información en Ambientes Educativos Virtuales resulte exitoso y cumpla los objetivos de una universidad.

2.1. Estándares de seguridad de la información en ambientes educativos virtuales

Las normas que nos interesan para el presente trabajo son las normas ISO/IEC 27000 creadas para facilitar la implantación de la Seguridad de la Información en Ambientes Educativos Virtuales de Educación Superior (*Whitman*, 2010).

a) La primera norma, la ISO/IEC 27000, recoge los términos y definiciones empleados en el resto de normas de la serie. Con ello se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de toda la norma.

Además, incluye una visión general de la familia de normas en esta área, una introducción a la seguridad de la información en ambientes educativos virtuales y una descripción del ciclo de mejora continua.

b) La norma principal de la serie es la ISO/IEC 27001, se aplica

a cualquier tipo de universidad, independientemente de la magnitud y los cursos virtuales que imparte. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la Seguridad de la Información en Ambientes Educativos Virtuales. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del curso virtual. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada universidad.

c) La norma ISO/IEC 27002 es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar la seguridad de la información en cursos virtuales de una universidad. Para ello describe 11 dominios, es decir áreas de actuación, 39 objetivos de control o aspectos a asegurar dentro de cada área, y 133 controles o mecanismos para asegurar los distintos objetivos de control.

La familia de normas ISO/IEC 27000 contiene otras normas destacables. Como por ejemplo, la norma sobre requisitos para la acreditación de las entidades de auditoría y certificación, es decir, de aquellas entidades que acudirán a cada universidad para certificar que el sistema está correctamente implementado.

2.2. Árbol general de requerimientos de seguridad de la información

Un aspecto muy importante es determinar un árbol estándar para analizar, evaluar y comparar los diferentes controles que existen en el desarrollo de un MSIAEV en base a características, comportamientos y atributos (Figura 1).

El modelo de este árbol se basa en los conceptos definidos en los estándares ISO 27001 e ISO/IEC 27000 [ISO/IEC, 2011], aplicados y adecuados a los objetivos del presente trabajo.

Figura 1. Árbol general de requerimientos de seguridad de la información

CARACTERISTICAS	COMPORTAMIENTOS	TRIBUTOS
POLITICA DE SEGURIDAD EN AMBIENTES EDUCATIVOS VIRTUALES (1)	(1.1) Política de Seguridad de la información	1.1.1 Documento de política de seguridad en ambientes educativos virtuales 1.1.2 Revisión de la política de seguridad en ambientes educativos virtuales
ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA (2)	(2.1) Organización interna	(2.1.1) Compromiso de la dirección con la seguridad de la información en ambientes educativos virtuales (2.1.2) Coordinación de la seguridad de la información (2.1.3) Asignación de responsabilidades para la seguridad de la información (2.1.4) Proceso de autorización para los servicios de procesamiento de información (2.1.5) Aspectos sobre confidencialidad
SEGURIDAD FÍSICA Y DEL ENTORNO DE EDUCACIÓN VIRUTAL (3)	(3.1) Áreas seguras del entorno de educación virtual	(3.1.1) Seguridad física (3.1.2) Operaciones de acceso físico (3.1.3) Seguridad de oficinas, recintos e instalaciones (3.1.4) Protección contra amenazas externas y ambientales
	(3.2) Seguridad de los equipos	(3.2.1) Ubicación y protección de los equipos (3.2.2) Seguridad del cableado (3.2.3) Mantenimiento de los equipos
GESTIÓN DE COMUNICACIONES Y OPERACIONES (4)	(4.1) Procedimientos operacionales y responsabilidades	(4.1.1) Documentación de los procedimientos de operación (4.1.2) Distribución (segregación) de funciones (4.1.3) Separación de instalaciones de desarrollo, ensayo y operación
	(4.2) Protección contra códigos maliciosos	(4.2.1) Controles contra códigos maliciosos
	(4.3) Copias de respaldo	(4.3.1) Respaldo de la información
	(4.4) Gestión de la seguridad de las redes	(4.4.1) Controles de las redes (4.4.2) Seguridad de los servicios de la red
	(4.5) Manejo de los medios	(4.5.1) Gestión de los medios removiles (4.5.2) Procedimientos para el manejo de la información (4.5.3) Seguridad de la documentación del sistema
CONTROL DEL ACCESO (5)	(5.1) Requisitos de la universidad para el control de acceso	(5.1.1) Política de control de acceso
	(5.2) Gestión del acceso de docentes y estudiantes	(5.2.1) Registro de docentes y estudiantes (5.2.2) Gestión de privilegios
	(5.3) Responsabilidades de los docentes y estudiantes	(5.3.3) Gestión de contraseñas para docentes y estudiantes
	(5.4) Control de acceso a las redes	(5.4.1) Políticas de uso de los servicios en red (5.4.2) Control de conexión a las redes
	(5.5) Control de acceso al sistema operativo	(5.5.1) Procedimientos de registro de inicio seguro (5.5.2) Identificación y autentificación de estudiantes (5.5.3) Sistema de gestión de contraseñas
	(5.6) Control de acceso al entorno virtual y a la información	(5.6.1) Restricción del acceso a la información
DESARROLLO Y MANTENIMIENTO DE PLATAFORMAS VIRTUALES (6)	(6.1) Requisitos de seguridad de los ambientes virtuales	(6.1.1) Análisis y especifición de los requisitos de seguridad
	(6.2) Procesamiento correcto en las plataformas virtuales	(6.2.1) Validación de los datos de entrada (6.2.2) Control de procesamiento interno (6.2.3) Validación de los datos de salida
	(6.3) Seguridad en los procesos de desarrollo y soporte	(6.3.2) Revisión técnica de las aplicaciones después de los cambios en el sistema operativo
Nivel de Abstracción		
Nivel 1	Nivel 2	Nivel 3

Fuente: Elaboración propia

3. Desarrollo del modelo

3.1. Cualidades del modelo

El modelo es integral, es decir, es un conjunto definido de estrategias, métodos y técnicas que, aplicados sistemáticamente a las distintas fases del modelo producen un indicador esperado. El modelo es robusto, porque, permite procesos con resultados repetibles y reproducibles en el tiempo. Finalmente, el modelo es flexible, porque permite agregar o sacar características, comportamientos y atributos de manera modular (con la idea de alta cohesión y mínimo acoplamiento), conforme a las necesidades específicas del perfil de los estudiantes y docentes.

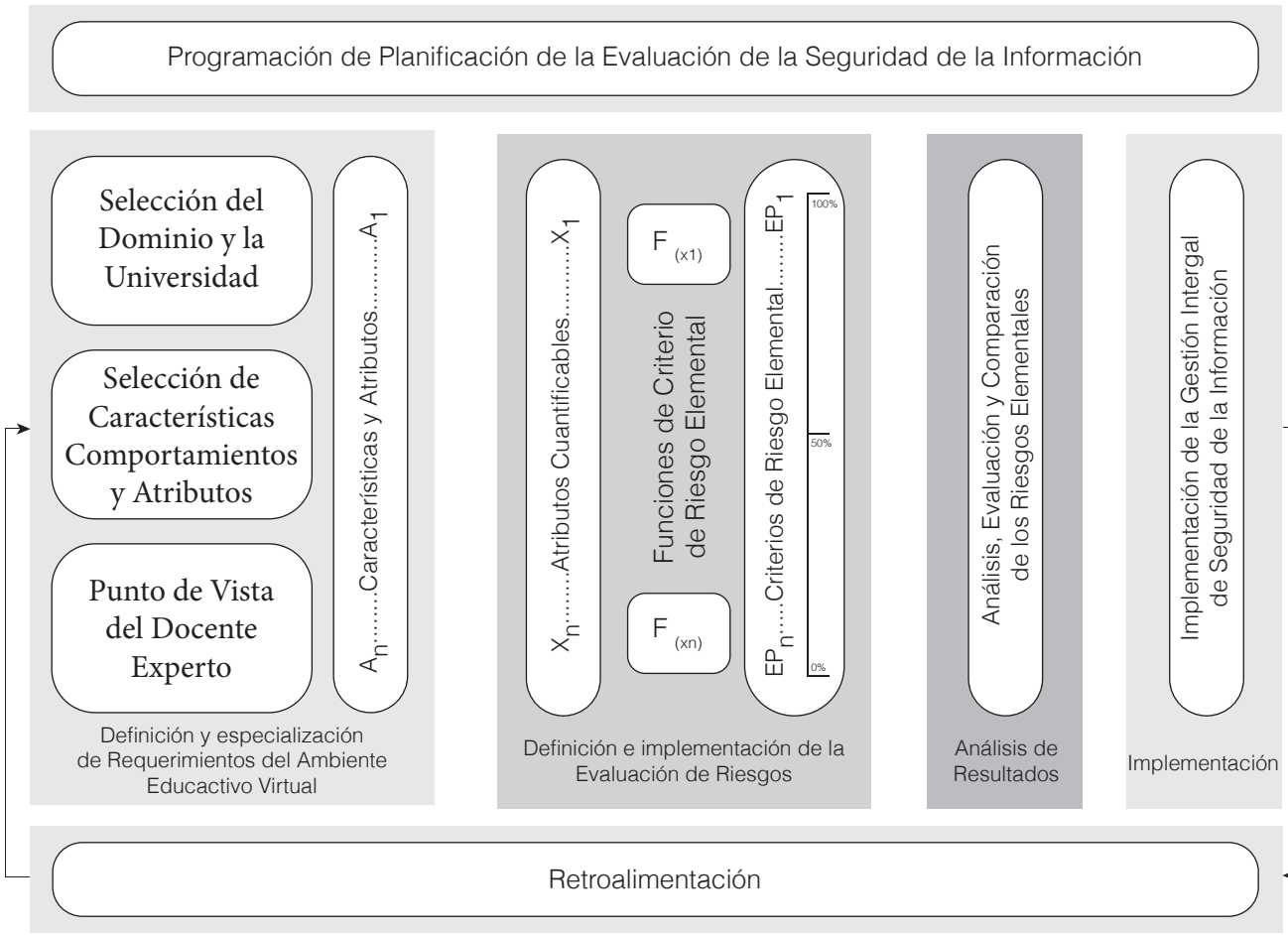
3.2. Fases principales

Las fases principales del modelo son las siguientes:

- **FASE 1.-** Programación y planificación de la evaluación en el MSIAEV
- **FASE 2.-** Definición y especificación de requerimientos del ambiente educativo virtual
- **FASE 3.-** Definición e implementación de la evaluación de riesgos
- **FASE 4.-** Análisis de resultados
- **FASE 5.-** Implementación
- **FASE 6.-** Retroalimentación

Una representación gráfica (Figura 2) del modelo donde se muestran las relaciones entre cada una de las fases es la siguiente:

Figura 2. Fases del modelo de seguridad de la información en ambientes educativos virtuales



Fuente: Elaboración propia

3.2.1. Fase de programación y planificación de la evaluación de la seguridad de la información en el ambiente educativo virtual

3.2.1.1 Definición del dominio y universidades de evaluación

Se 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 aplicando el modelo de Seguridad de la Información en Ambientes Educativos Virtuales.

3.2.1.2 Definición del objetivo y cronograma de evaluación

El objetivo representa los propósitos que se debe alcanzar en el dominio a ser evaluado, aplicando las fases del MSIAEV 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.

3.2.2 Fase de definición y especificación de requerimientos del ambiente educativo virtual

3.2.2.1 Perfil de usuario

Para la elaboración del modelo se definen los siguientes perfiles de usuario:

- "Docente", por la estrecha relación que tiene en la parte de enseñanza en ambientes educativos virtuales. La visión del docente considera el conocimiento y dominio de las principales características, comportamientos y atributos de la seguridad de la información en ambientes educativos virtuales.

- "Estudiante", por la participación indirecta como parte de un ambiente educativo virtual. La visión del estudiante considera el conocimiento superficial de las principales características, comportamientos y atributos de la seguridad de la información en ambientes educativos virtuales.

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.

- El Docente Casual, se define como la audiencia que utiliza un ambiente educativo virtual por azar, y donde la implementación está pensada para ser usada una sola vez.

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

El Docente Experto, se define como a la audiencia que es especialista para crear, manejar y administrar un ambiente educativo virtual, y forman parte de este grupo los administradores de seguridad de la información, docentes programadores, analistas de sistemas, entre otros.

3.2.2.2 Selección de técnicas para recopilar datos

a) Entrevistas

Los docentes que sean sujetos a la entrevista deben tener el perfil de Docentes Expertos. El evaluador debe entrevistar a los Docentes Expertos de forma individual o en grupos. La información cualitativa será relacionada con opiniones y descripciones narrativas de actividades o problemas que el "Docente Experto" tuvo al crear un ambiente educativo virtual, mientras que las descripciones cuantitativas serán relacionadas con números, frecuencias o cantidades de mantenimientos o situaciones en las cuales el entrevistado haya resuelto una contingencia en un ambiente educativo virtual en una universidad. Las entrevistas descubren rápidamente malos entendidos, falsas expectativas o incluso resistencia potencial a la ejecución de las fases del modelo de Seguridad de la Información en Ambientes Educativos Virtuales. La estructura de las entrevistas será diseñada para obtener datos específicos sobre las características, comportamientos y atributos que el "Docente Experto" requiere en la implantación de la Seguridad de la Información en Ambientes Educativos Virtuales asegurando una alta confiabilidad en todas las respuestas obtenidas.

b) Encuestas

Para los evaluadores las encuestas son la única forma posible de relacionarse con un gran número de "Docentes Expertos" con la finalidad de conocer varios aspectos del MSIAEV. En la mayor parte de los casos, el evaluador no conocerá ni tendrá relación directa con los docentes que respondan (evaluación por ciego); no obstante, está situación será también una ventaja ya que el aplicar las encuestas de manera simultánea asegurará que el docente cuente con mayor anonimato y de esta manera las respuestas brindadas tendrán mayor confiabilidad.

3.2.3 Fase de definición e implementación de la evaluación de riesgos

En esta fase se consideran diferentes tipos de escalas de riesgo, funciones, valores y rangos críticos para determinar el indicador de riesgo para cada atributo cuantificable para realizar el proceso de medición de cada característica, comportamiento y atributo del MSIAEV.

3.2.3.1 Criterio de riesgo elemental

El criterio de riesgo[3] 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 trabajo, se tomó en cuenta el criterio de riesgo elemental para medir todas las características, comportamientos y atributos del MSIAEV.

Para cada atributo cuantificable Ai, se debe asociar y determinar una variable Xi que procede a tomar un valor real a partir de un proceso de medición. Además, para cada variable Xi computada, por medio de un criterio elemental, se producirá un indicador de riesgo elemental por cada sección en el diseño del modelo ***(EPi)***, el

[3] Un factor que podría resultar en futuras consecuencias negativas, usualmente expresado como impacto y probabilidad

resultado final obtenido se interpreta como el grado o porcentaje del requerimiento del Docente Experto satisfecho para el atributo ***Ai*** [Fenton et al, 2007].

En cada variable medida X_i, donde $i = 1,\ldots\ldots, n$, se define una función que representa al criterio elemental. Un criterio elemental está definido como una correspondencia del valor de la variable de uso X_i, con el valor de riesgo elemental (EP_i). En términos generales, el valor medido de la variable es un número real [Fenton et al, 2007]:

$$X_i \in R_i \subset R;$$
donde R representa a los números reales

El valor de riesgo elemental (EP_i) es también un número real perteneciente al intervalo I = [0, 1] entonces [Fenton et al, 2007]:

$$EP_i \in I_i \text{ ; donde } i = 1,\ldots, n$$

Con frecuencia, en vez de usar el intervalo unitario es beneficioso emplear la escala porcentual de 1% a 100%. En este sentido se interpreta al indicador de riesgo como el porcentaje del requerimiento insatisfecho. Desde un punto de vista analítico, el criterio elemental ***(CrE)***, se define como la función:

$F_i : R_i \rightarrow I$ *Donde:* $EP_i = F_i(x_i)$;

Además: $X_{imin} \leq Xi \leq X_{imax}$

Entonces, sea X_i el valor que se le asigna a un atributo A_i, donde, el criterio elemental para dicho atributo es definido como [Fenton et al, 2007]:

X_{imin} *es el menor valor que toma X;*
X_{imax} *es el mayor valor que toma X*

Entonces:

$$\text{Si: } X_i \leq X_{i\,min} \quad \text{CrE } (X_i) = \text{Si: } \begin{cases} EP_i = 0 \cong 1\,\% \\ X_i \geq X_{i\,max} \rightarrow EP_i = 1 \cong 100\,\% \end{cases}$$

$$\text{Si: } X_{i\,min} \leq X_i \leq X_{i\,max} \rightarrow EP_i = \frac{X_i - X_{i\,min}}{X_{i\,max} - X_{i\,min}}$$

Según lo formulado, el criterio declara que el grado de satisfacción del Docente Experto se encuentra en:

- Un nivel satisfactorio si el atributo A_i es mayor o igual, al mayor $X_{i\,max}$, es decir EP_i es igual a 100%.
- Un nivel insatisfactorio si el atributo A_i es menor o igual, al mayor $X_{i\,min}$, es decir EP_i es igual a 1%.

3.2.3.2 Representación de notación de criterios

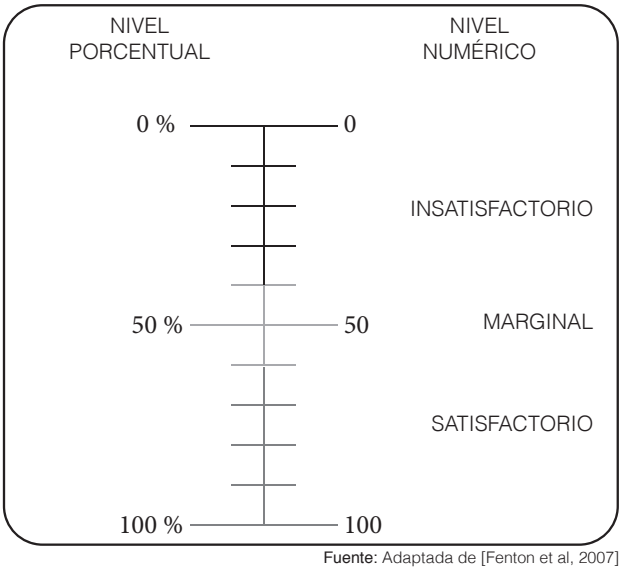
Se utilizara el siguiente tipo de notación para representar a los criterios elementales del presente trabajo.

a) Tipos de criterio de riesgo elemental

Muchas veces, una notación reducida tiene una escala de riesgos (Figura 3), en esta se muestran los niveles de riesgo correspondientes y los puntos que se consideran de mayor interés[Fenton et al, 2007]:

$$\text{CrE (Xi)} = \begin{cases} \text{Si: } X_{i\,min} = 1 \rightarrow EP_i = 1 \cong 1\% \\ \text{Si: } X_{i\,max} = 100 \rightarrow EP_i = 100 \cong 100\,\% \end{cases}$$

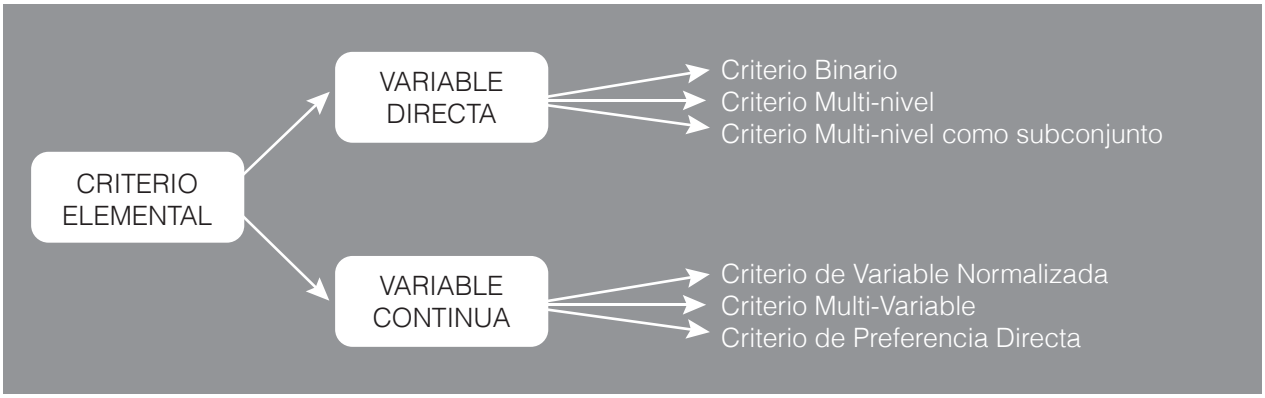
Figura 3. Escala de riesgo elemental



Fuente: Adaptada de [Fenton et al, 2007]

Dos tipos importantes de criterios elementales (Figura 4) son los criterios con variables continuas[4], y criterios con variables discretas[5] [Fenton et al, 2007].

Figura 4. Tipos de criterios de riesgo elemental



Fuente: Adaptada de [Fenton et al, 2007]

3.2.4 Fase de análisis de resultados

En la fase de análisis de resultados se realizan actividades de análisis y comparación de riesgos de las características definidas en el árbol general de requerimientos de seguridad de la información (Figura 1) consolidando los datos generados por cada característica con datos obtenidos de las entrevistas y cuestionarios realizadas a los docentes expertos, justificando cada resultado mediante el empleo de tablas que se describen a continuación.

3.2.4.1 Empleo de tablas

En la Tabla 1 se deben mostrar los resultados de los valores de los riesgos de la universidad para las características de la seguridad de la información en ambientes educativos virtuales. Los valores finales serán muy útiles para realizar la comparación, el análisis, la justificación y las recomendaciones de la implementación del modelo.

[4] Son aquellas que asumen cualquier valor dentro de un intervalo, por lo cual tiene un número infinito de valores posibles.
[5] Son aquellas que se cuentan, es decir, tienen un número finito de valores posibles, tanto las variables discretas como las continuas se agrupan construyendo intervalos.

Tabla 1. Tabla de resultados para obtener la evaluación de riesgos

CÓDIGO	NOMBRE	CRITERIO	PARÁMETROS Y VALORES	EVALUACIÓN DE RIESGO
1	CARACTERÍSTICA 1	E_i.....n = EP_n	V_1	R_1
1.1	COMPORTAMIENTO 1	...		
1.1.1	ATRIBUTOS 1.1	CrE (X_i) = EP_i		
1.1.2	...n	...		
...	...	...		
2	CARACTERÍSTICA 2	E_i.....n = EP_m	V_2	R_2
2.1	COMPORTAMIENTO 2	...		
2.1.1	ATRIBUTOS 2.1	CrE (X_i) = EP_i		
2.1.2	...m	...		
...		...		
3	CARACTERÍSTICA 3	E_i.....n = EP_k	V_n	R_n
3.1	COMPORTAMIENTO 3	...		
3.1.1	ATRIBUTOS 3.1	CrE (X_i) = EP_i		
3.1.2	...k	...		
..	...	...		

Fuente: Elaboración propia

En la Tabla 2, se debe mostrar el resultado del Indicador Global de Riesgo Controlado Total (IGRCT) que muestra el porcentaje de controles de riesgo por cada característica implementados en un ambiente educativo virtual de una universidad y se sitúa en cualquiera de los siguientes intervalos:

a) Insatisfactorio (1% a 40%)
b) Marginal (41% a 60%)
c) Satisfactorio (61% a 100%)

Tabla 2. Tabla de resultado para obtener el nivel de seguridad de la información

ENTIDAD EVALUADA	INDICADOR GLOBAL DE RIESGO CONTROLADO TOTAL (IGRCT)	NIVEL DE SEGURIDAD DE LA INFORMACIÓN		
		Insatisfactorio (1 - 40)	Marginal (41 – 60)	Satisfactorio (61 - 100)
NOMBRE DE LA UNIVERSIDAD	VALOR DE IGRT			

Fuente: Elaboración propia

3.2.5 Fase de implementación

En esta fase de implementación, se definen objetivos, controles y procedimientos de implementación para cada de 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 adecuados a los objetivos del presente trabajo.

- POLÍTICA DE SEGURIDAD EN AMBIENTES EDUCATIVOS VIRTUALES

a) Objetivo

Brindar apoyo y orientación a la alta dirección respecto a la seguridad de la información, de acuerdo con los requisitos y reglamentos del ambiente educativo virtual de la universidad

b) Control

El presente documento declara el apoyo de la dirección ejecutiva compuesta por el Rector, Vicerrector, Directores de Carrera y otros que apoyen a la gestión de la seguridad de la información de acuerdo a los objetivos estratégicos de cada universidad.

c) Procedimiento de implementación

El documento de la política de seguridad de la información debe contener declaraciones relacionadas con:

1. La definición de la seguridad de la información, objetivos generales y el alcance e importancia de la seguridad como mecanismo que garantice la calidad de la información.
2. La declaración de la intención de la dirección ejecutiva, que apoya las metas y los principios de seguridad de la información en los ambientes educativos virtuales, de acuerdo con la estrategia y los objetivos de la universidad.

- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a) Objetivo

Permitir gestionar la seguridad de la información, estableciendo una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de los ambientes educativos virtuales de la universidad

b) Control

Se deben definir claramente las responsabilidades de la seguridad de la información por cada empleado encargado de los ambientes educativos virtuales de la universidad.

c) Procedimiento de implementación

1. La asignación de responsabilidades para la seguridad de la información se debe realizar cumpliendo la política de seguridad de la información de la universidad.
2. Se deben definir las responsabilidades para la protección de hardware y software para la ejecución de procesos específicos del ambiente educativo virtual dentro de la universidad.

- SEGURIDAD FÍSICA Y DEL ENTORNO DE EDUCACIÓN VIRTUAL

a) Objetivo

Evitar la pérdida, daño, robo o puesta en peligro de la información de los ambientes educativos virtuales de la universidad, los equipos y la infraestructura deben estar protegidos contra amenazas físicas y ambientales

b) Control

Las áreas de procesamiento de los ambientes educativos virtuales deben estar protegidas con números de identificación personal (PIN) para asegurar que sólo se permite el acceso a personal autorizado.

c) Procedimiento de implementación

1. Se debe registrar la fecha y la hora de entrada y salida de personas ajenas al ambiente educativo virtual y todos los visitantes deben tener acceso solo a las salas de clase autorizadas.

2. Se debe controlar el acceso a áreas en donde se procesa y almacena información de los ambientes educativos virtuales y se deben utilizar controles de autenticación basadas en números de identificación personal (PIN) para autorizar y validar el acceso de cualquier docente y/o estudiante.

- GESTIÓN DE COMUNICACIONES Y OPERACIONES

a) Objetivo

Asegurar la operación correcta de los servicios de procesamiento de información en ambientes educativos virtuales estableciendo las responsabilidades y los procedimientos para la gestión y operación de todos los servicios

b) Control

Se debe detectar, prevenir y proteger la integridad del software y la información contra códigos maliciosos.

c) Procedimiento de implementación

1. Se deben llevar a cabo revisiones regulares del software del ambiente educativo virtual.
2. Se debe tener instalado un software corporativo para la detección de códigos maliciosos para explorar todos los computadores y los medios que acceden a ambientes educativos virtuales de la universidad diariamente, los controles de verificación deben:
   - Verificar la presencia de códigos maliciosos en todos los archivos en medios ópticos o electrónicos y archivos recibidos de las redes.
   - Verificar la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico.
   - Verificar las páginas web a las que se acceden a través de un curso virtual para comprobar la presencia de códigos maliciosos.

- CONTROL DEL ACCESO

a) Objetivo

Controlar el acceso a la información a los servicios de procesamiento de información y a los procesos de negocios sobre la base de los requisitos de seguridad de ambientes educativos virtuales

b) Control

Se controla el registro y suspensión de docentes y/o estudiantes con el fin de verificar y revocar el acceso a los ambientes educativos virtuales de la universidad.

c) Procedimiento de implementación

1. Se debe aplicar una identificación única de usuario para que los estudiantes y/o docentes queden registrados y sean responsables de las acciones que realizan en cada ambiente educativo virtual
2. Se debe brindar una declaración escrita de todos los derechos y obligaciones de cada estudiante y/o docente que tiene acceso a algún ambiente educativo virtual de la universidad.
3. Se debe contar con un historial de registro formal de todos los estudiantes y/o docentes que accedieron alguna vez un ambiente educativo virtual
4. Se debe retirar y bloquear de inmediato los derechos de acceso de los estudiantes y/o docentes que han cambiado de curso o que han dejado la universidad.

- DESARROLLO Y MANTENIMIENTO DE PLATAFORMAS VIRTUALES

a) Objetivo

Garantizar que la seguridad es parte integral antes y durante el desarrollo de un ambiente educativo virtual así como en la implementación del producto final en el ambiente de producción

b) Control

Se deben tener incorporados controles de validación en los ambientes educativos virtuales para detectar cualquier modificación de la información por errores de procesamiento o actos deliberados.

c) Procedimiento de Implementación

El diseño y la implementación de las plataformas de cursos virtuales deben garantizar que se minimizan los riesgos de falla en el almacenamiento y procesamiento de la información. Los temas específicos que se deben considerar son:

1. Implementación de programas decuados para la recuperación de servidores después de fallas en el ambiente educativo virtual con el fin de garantizar la integridad de los datos.
2. Se deben elaborarlas siguientes listas de verificación:

    - Verificaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o actualizado entre un computador central y remoto.
    - Verificación para garantizar que los programas de aplicación del ambiente educativo virtual se ejecutan en el momento correcto.
    - Verificaciones para garantizar que los programas se ejecutan en el orden correcto y terminan en caso de falla, y que el procesamiento posterior se detiene hasta resolver el problema.

3.2.6 Fase de retroalimentación

Es un proceso interactivo 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 ambientes 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 de Seguridad de la Información en Ambientes Educativos Virtuales para medir el nivel de minimización de riesgo antes y después de la implementación del modelo.

La retroalimentación es una fase importante ya que vuelve a iniciar el proceso de la "Definición e Implementación de la Evaluación de Riesgos" y el "Análisis de Resultados" cuantas veces sea necesario hasta que el Indicador Global de Riesgo Controlado Total (IGRCT) se encuentre en el intervalo de Satisfactorio (61% a 100%) (Tabla 2).

4. Conclusiones

- Se desarrolló el MSIAEV el cual tiene seis fases donde se aplican técnicas, métodos, criterios y se adecuan componentes, estándares, fases, controles y procedimientos de implementación que optimizan la seguridad de la información en ambientes educativos virtuales de una universidad.
- Se determinó el árbol general de requerimientos, adecuado en base el estándar ISO 27001 e ISO/IEC 27000 [ISO/IEC, 2011], y que toma en cuenta las siguientes características: política de seguridad en ambientes educativos virtuales; organización de la seguridad informática; seguridad física y del entorno de educación virtual; gestión de comunicaciones y operaciones, control del acceso; y el desarrollo y mantenimiento de plataformas virtuales.
- Se establecieron seis fases principales

en el desarrollo del modelo que son la programación y planificación de la evaluación de la seguridad de la información en el ambiente educativo virtual, definición y especificación de requerimientos del ambiente educativo virtual, definición e implementación de la evaluación de riesgos, el análisis de resultados, la implementación y la retroalimentación.

- Se estableció el Indicador Global de Riesgo Controlado Total (IGRCT) que muestra el porcentaje de riesgo por cada característica, comportamiento y atributos definidos en el árbol general de requerimientos antes y después de la implementación del modelo en un ambiente educativo virtual de una universidad.
- En la fase de implementación del modelo se definieron objetivos, controles y procedimientos de implementación que ayudan a que la seguridad de la información en ambientes educativos virtuales dentro de una universidad sea confiable y toda la información este resguardada de forma segura.

5. Limitaciones del trabajo

- Si bien el presente trabajo se limita a usar el estándar ISO 27001 e ISO/IEC 27000 [ISO/IEC, 2011], existen otros estándares de seguridad que se podrían tomar en cuenta en futuros trabajos. Estos podrían ofrecer una serie de nuevos resultados en los ámbitos de la seguridad de información dentro de un ambiente educativo virtual.

6. Recomendaciones

- Podría ampliarse el estudio tomando en cuenta los nuevos estándares de seguridad de la información y adicionando nuevas características de seguridad de la información para minimizar de mejor manera el nivel de riesgo en una organización.
- Se podrían plantear nuevos indicadores de riesgo por cada fase para controlar el nivel de riesgo en cada característica, comportamiento y atributo definido en el árbol general de requerimientos.

BIBLIOGRAFÍA

- Calvo E., 2010. Administración de Sistemas de Información. 2da. Edición Thomson Learning, México.
- Cardenas J., 2012. Alcaldía de Santiago de Cali-Colombia: “Seguridad de la Información, un nuevo reto para las universidades” Disponible en:http://www.cali.gov.co/publicaciones.php?id=1210, Visitado [15/Julio/2012]
- Daltabuit H., 2011. La seguridad de la información. 2da. Edición, Thomson Learning, Mexico.
- Del Carpio J., 2011. Análisis del riesgo en la administración de proyectos de tecnología de información, 2da. Edición, Prentice-Hall, México.
- Fenton C. 2007. Software Metrics: A Rigorous and Practical Approach. PWS Publishing Company, 2nd. Edition.
- Herrera G., 2010. El libro de los virus y de la seguridad informática, 1era. Edición, Addison-Wesley.
- ISO/IEC, 2011. Norma técnica de tecnología de la información 27000-27001.
  Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
- Whitman M., 2010. Management of Information Security, 2nd.Edition, Addison- Wesl.