Revista Venezolana de Análisis de Coyuntura, 2009, Vol. XV, No. 1 (ene-jun), pp. 219-240
recibido: 25-02-2009 / arbitrado: 09-02-2009

MODELO SISTÉMICO DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS UNIVERSIDADES

Orlando Viloria*
Walter Blanco**
USB

Resumen:

El siguiente artículo propone un modelo gerencial denominado Modelo Sistémico de la Seguridad de la Información en las Universidades, su objetivo es brindar un marco conceptual que contribuya a tratar esta situación en las universidades venezolanas. Destaca el Modelo Organizacional Dinámico de Leavitt como modelo de inspiración. El componente tecnología cambia por las TIC (intranet o extranet); la gente y la cultura, la estructura organizacional así como los procesos y las tareas están descritos bajo un enfoque de la seguridad informática. El modelo propuesto incorpora un quinto elemento, las disciplinas de las organizaciones inteligentes como factores críticos de éxito y elementos de orden en el caos generado por la adopción de las TIC. El modelo no es una panacea que resuelve el problema de inseguridad de la información que crea la adopción de las redes privadas, pero ayuda a los equipos y gerentes responsables a comprenderlo y a facilitarles la planificación estratégica y su ejecución bajo una perspectiva de la seguridad de la información.

Palabras Claves: Seguridad de la información, organizaciones inteligentes, modelo gerencial, trabajadores del conocimiento, SI, TIC.

INTRODUCCIÓN

Actualmente un plan estratégico bajo una perspectiva de la seguridad de la información (SIF) es un factor crítico de éxito para cualquier empresa madura en el uso y la adopción de los Sistemas de Información (SI) y las Tecnologías de la Información y la Comunicación (TIC). Este plan debe poseer un enfoque sistémico, ya que para ser completo abarca aspectos relacionados con: la seguridad lógica y la seguridad física, el factor humano, la gerencia, la cultura y la estructura organizacional. En este mismo orden de ideas, este trabajo propone un modelo organizacional denominado Modelo Sistémico de la Seguridad de la Información de las Universidades (MOSSIU), en especial las venezolanas. El modelo es una formulación teórica o una herramienta para aquellos trabajadores del conocimiento[1], encargados de la seguridad de la información ya que ayuda a comprender el problema en sus organizaciones y a bajar la incertidumbre.

* oviloria@usb.ve ** wblanco@usb.ve

[1] Son trabajadores que agregan valor al conocimiento que reciben y con él modifican sus rutinas. Según Laudon y Laudon (2002), los trabajadores del conocimiento, como ingenieros, arquitectos y científicos, diseñan productos o servicios y crean conocimientos.

Cabe destacar que las universidades venezolanas poseen diferentes culturas y profundas diferencias con respecto a la cultura informacional, incluso algunas instituciones superiores son más maduras que otras o poseen un mayor nivel de aprendizaje organizacional, además afrontan los problemas relacionados con la inseguridad de la información con más eficacia que otras. En consecuencia, cualquier plan estratégico bajo una perspectiva de la Seguridad de la Información a operacionalizar, depende de cómo ésta se encuentra hoy y de su nivel de aprendizaje en la adopción de los SI y las TIC. El MOSSIU es un modelo independiente de las discrepancias existentes en estas instituciones educativas, es un marco referencial, es una estructura, una guía para los encargados de la seguridad de la información.

Este trabajo presenta una descripción de los subsistemas que integran al MOSSIU, las relaciones sistémicas entre ellas, la sinergia, las barreras de aprendizaje necesarias para garantizar el éxito en la elaboración e instrumentación de cualquier plan de seguridad de la información. Además, es importante señalar que el modelo se describe bajo un enfoque de una organización aprendiente y tiene como base el modelo dinámico organizacional de Leavitt (1965), también conocido como el diamante de Leavitt.

BASES TEÓRICAS

En esta sección es importante precisar algunos conceptos claves manejados en el desarrollo de este trabajo.

Concepto de Seguridad de la Información

El concepto de Seguridad de la Información considerado en este estudio es el de Aceituno (2006), él señala que deben cumplirse los siguientes requerimientos de seguridad en los activos de una organización:

- Confidencialidad, consiste en dar acceso a la información sólo a los usuarios autorizados.
- Control de acceso, consiste en controlar y restringir el acceso a la información a determinados usuarios.
- Disponibilidad, consiste en la posibilidad de acceder a la información o utilizar un servicio siempre que se necesite.
- No repudio, consiste en la imposibilidad de negar la autoría de un mensaje o información del que alguien es autor.

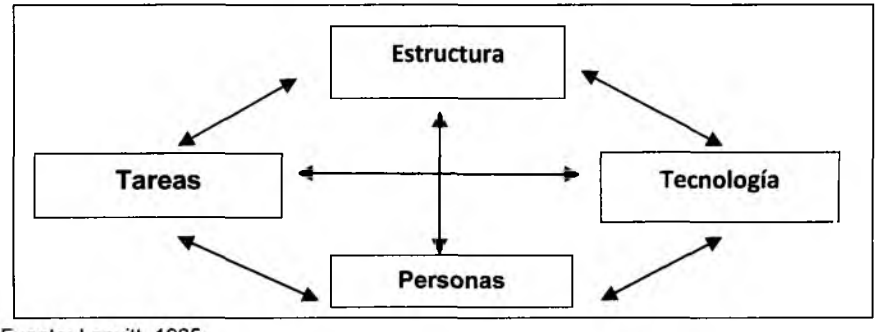
- Integridad, consiste en garantizar la no manipulación de una información o mensaje.

El Modelo Dinámico Organizacional (MDO) de Leavitt

En el MDO destacan 4 componentes o subsistemas relacionados entre si: los procesos y las tareas, la gente y la cultura, la tecnología y la estructura organizacional. La esencia de este modelo subyace en la relación sistémica de sus partes y los cambios que ocurren en cada componente cuando la organización adopta una nueva tecnología que afecta la curva de aprendizaje organizacional, la aleja del equilibrio y aumenta su complejidad e incertidumbre. Dada la interrelación y la dependencia entre los componentes del MDO, la entropía los domina y se presenta el caos, esto amerita la instrumentación de una serie de acciones autorreguladoras, orientadas a reducir el desorden en cada uno de estos subsistemas y en consecuencia en toda la organización, para evolucionar a otro estado más complejo. Cabe destacar que adquirir una tecnología es un curso de acción formulado en los planes estratégicos de la organización en la búsqueda de impactar su competitividad y sus procesos críticos. Pero operacionalizar esta estrategia es un punto de bifurcación que dispara la entropía en todos los subsistemas del MDO.

Por lo tanto, el modelo de Leavitt contribuye a la disminución de la complejidad de la gestión del proceso de implantación de una tecnología. Facilita la identificación sistémica de los componentes afectados por la decisión estratégica de adoptar la nueva tecnología, en consecuencia contribuye a la formulación de estrategias o lazos retroalimentadores negativos necesarios para bajar la entropía en los componentes del diamante de Leavitt (1965) (ver Gráfico 1), en otras palabras el MDO es como un vórtice (Briggs y Peat, 1999) en la organización.

Gráfico 1. El Diamante de Leavitt



Fuente: Leavitt, 1965.

Las Disciplinas de las Organizaciones Inteligentes

El Dominio Personal (DP)

En resumen, respecto a esta disciplina señalan Senge (1992) y Senge et al (2004) que:

- Trasciende la competencia y las habilidades, aunque se basa en ellas.
- Trasciende la apertura espiritual, aunque requiere del crecimiento espiritual.
- Significa abordar la vida como una tarea creativa, vivirla desde una perspectiva creativa y no meramente reactiva.
- Su esencia es aprender a generar la tensión creativa en la vida.
- Su aprendizaje no significa adquirir más información, sino expandir la aptitud para producir los resultados deseados (aprendizaje generativo).
- La gente con alto nivel de dominio personal tiene un sentido especial del propósito que subyace en sus metas y visiones, viven en una continua modalidad de aprendizaje.
- Es un proceso, es una disciplina que dura toda la vida.
- Un trabajador con un alto DP es consciente de su ignorancia, incompetencia y de sus zonas de crecimiento, es más comprometido, posee mayor iniciativa y es responsable.
- Una organización que la aplique alienta el desarrollo de los trabajadores.

Los Modelos Mentales (MM)

Respecto a los MM, señala Senge (1992) y Senge et al (2004) que:

- Son supuestos hondamente arraigados, generalizaciones e imágenes que influyen sobre el modo de actuar de las personas. Son las imágenes, supuestos e historias que llevan en la mente acerca de ellos, los demás, las instituciones y todos los aspectos del mundo.
- Son tácitos, direccionan las conductas y decisiones en la vida. En las organizaciones también están intensamente arraigados, tanto que influyen las decisiones gerenciales.
- El desarrollo de su disciplina necesita del Dominio Personal, pues ésta representa las aptitudes y las actitudes de la gerencia estratégica y de los

equipos existentes en la organización. Al final, los MM ayudarán a impulsar el DP y el aprendizaje en equipo para lograr la visión compartida.

- Dos aptitudes esenciales para adecuarlos son: la reflexión que consiste en disminuir el ritmo de los procesos mentales para concienciar la formación de nuestros MM; y la indagación, que consiste en realizar conversaciones para compartir en forma abierta los puntos de vista y procurar conocer las premisas y opiniones de los otros.
- Su definición potencia el proceso de aprendizaje de los trabajadores, se toman decisiones más ajustadas a la realidad.

Visión Compartida (VC)

Con relación a la VC señala Senge (1992) y Senge et al (2004) que:

- Es una fuerza en el corazón de la gente, una fuerza de impresionante poder. Puede estar inspirada por una idea, pero si es tan convincente como para poder lograr el respaldo de más de una persona cesa de ser una abstracción.
- Es un conjunto de imágenes que lleva la gente de la empresa, crea una sensación de atadura común que impregna la organización y brinda coherencia a actividades dispares.
- Es vital para la organización inteligente, porque brinda concentración y voluntad para el aprendizaje. En el aprendizaje adaptativo, el de más bajo nivel, no existe VC.
- Para crearla en las organizaciones se necesitan actitudes y conocimiento (Disciplina del DP). Entre la VC y el DP se establece una relación sistémica generadora de sinergia que modifica la relación de la gente con la empresa.
- Cuando hay visión genuina, la gente no sobresale ni aprende por que se le ordene sino porque lo desea.

El Aprendizaje en Equipo (AE)

Respecto a esta disciplina, según Senge (1992) y Senge et al (2004):

- Cuando los equipos aprenden de veras, no sólo generan resultados extraordinarios sino que sus integrantes crecen con mayor rapidez.
- La clave es la comunicación, las relaciones entre los diferentes componentes del equipo o sistema para diseñar las estrategias o cursos de acción coordinadas con el fin de lograr los objetivos comunes.

- Comienza con el diálogo, la capacidad de los miembros del equipo para suspender e ingresar en un auténtico pensamiento en conjunto.
- Los equipos que la practican tienen las siguientes características: (a) son sistemas dinámicos, evolucionan continuamente e intercambian energía con su entorno, (b) existen relaciones cualitativas entre la visión de equipo y su dominio personal; (c) el conocimiento individual se transmite entre ellos y a otros equipos y; (d) establecen los modelos mentales por consenso.

Pensamiento Sistémico (PS)

Es la integración de las cuatro disciplinas anteriores llamada también la quinta disciplina, se fusionan en un cuerpo coherente de teoría y práctica (Senge, 1992).

En síntesis, según Senge (1992) y Senge et al (2004):

- El pensamiento sistémico está presente en cada una de las disciplinas, pues cada una de ellas no se desarrolla individualmente, ya que no habría sinergia.
- Los trabajadores del conocimiento se deben centrar en el paradigma orientado a procesos y no en el de tareas.
- Se debe pensar en sistemas, y preguntarse sobre las consecuencias de sus errores en otra unidad organizacional o en el mismo departamento.

Sin embargo, deben identificarse las barreras de aprendizaje de Senge (1992) y las de Argyris (1990) las cuales atentan contra el pensamiento sistémico.

METODOLOGÍA

Introducción

Este artículo muestra los resultados parciales de un macroproyecto de planificación estratégica bajo un enfoque de los Sistemas de Información (SI) y la Tecnología de la Información (TI) en las universidades venezolanas, el primer estudio se realizó en el Núcleo de la Universidad Simón Bolívar (USB), ubicado en el Estado Vargas en el año 1997, abarcó: (a) el diseño de la metodología, (b) el diagnóstico y, (c) la propuesta, la recolección de datos culminó en el año 1999. A partir del año 2000, el proyecto macro sufre cambios en sus objetivos, es más ambicioso, la planificación estratégica se extiende hacia las redes privadas y se orienta hacia los SI y las TIC. En este período genera varias líneas de investigación con algunos resultados: trabajos de ascenso, tesis de maestría, artículos publicados y ponencias en congresos.

Posteriormente en el año 2002, el plan de trabajo evoluciona y cambian los objetivos del proyecto, ahora es Planificación estratégica bajo una perspectiva de los SI, las TIC y la SIF, la visión es sistémica y adecuada a los cambios tecnológicos que ocurren en nuestro entorno y sus efectos colaterales, como la inseguridad de la información (Viloria y Blanco, 2006c). Asimismo, la muestra en estudio no se limita a la USB, sino a otras universidades. Las distintas etapas de desarrollo del Plan Estratégico de los SI, las TIC y la SIF, consistió en la recolección de datos e información, al final ayudó a la identificación de variables y sus relaciones para dar origen al MOSSIU.

Descripción de la Metodología

El tipo de estudio realizado fue longitudinal, pues la recolección de datos se hace en un periodo extendido de tiempo. En efecto, en las diversas investigaciones alineadas con el proyecto de Planificación Estratégica se aplicaron una variedad de metodologías, métodos y técnicas para recolección de datos e información, en donde destacan la encuesta de opinión, los cuestionarios, las entrevistas estructuradas, semiestructuradas o abiertas, la observación directa y la investigación-acción. En efecto, la investigación de Morales (2004) sobre los servicios de información y su seguridad fue realizada en tres universidades públicas nacionales: Universidad Central de Venezuela, Universidad del Zulia y la Universidad Simón Bolívar, instrumentó una metodología cualitativa y aplicó entrevistas; Villegas (2008) creó un modelo de madurez sistémico con cinco niveles de aprendizaje de la gestión de la seguridad de la información, abarcó 11 universidades de una población de 14 ubicadas en el Distrito Capital, incluyó instituciones públicas y privadas; Mayorca (2007), para describir la presencia de las 7 dimensiones del aprendizaje de una organización aprendiente de Watkins y Marsick, aplicó entrevistas y cuestionarios en la Universidad Católica Andrés Bello y la Universidad Simón Bolívar y; Romero (2008) enfocó su investigación al análisis y gestión de riesgo de activos informáticos, su contexto fue la USB.

Por otro lado, el estudio de campo realizado por Villegas (2008), presentó la oportunidad a los autores de este artículo de aplicar entrevistas abiertas a trabajadores del conocimiento encargados de la seguridad de la información en universidades, y así evaluar su nivel de aprendizaje bajo una perspectiva de una organización aprendiente.

Asimismo, esta investigación es un estudio de campo de tipo exploratoria, pues se revisaron una serie de trabajos relacionados con gerencia, aprendizaje organizacional, gestión tecnológica en las universidades y la seguridad de la informática en donde los autores de este artículo son coautores, tales como: Viloria y Blanco (1999, 2000, 2001, 2004a, 2004b, 2006a; 2006b, 2006c); Blanco

y Viloria (1999a; 1999b, 2001, 2006); Morales et al (2000); Morales y Torrealba (2004); Torrealba (2004); Torrealba y Morales (2004, 2005). Todos estos trabajos de investigación contribuyeron a establecer los bases necesarias para la identificación de variables, tendencias y estructurar el problema planteado, tal como lo recomiendan Hernández, Fernández y Baptista (1998) para esta modalidad de investigación. Además se identifican las relaciones entre las variables tales como los valores éticos, la actitud, la aptitud, las políticas de seguridad informática, el cooperativismo, la estructura organizacional, los procesos y tareas, la visión y la cultura de la SIF. Estas variables ayudaron a inferir la aplicación de las disciplinas de una organización aprendiente como: el aprendizaje en equipo, los modelos mentales, el dominio personal, la visión compartida y el pensamiento sistémico.

En este mismo orden de ideas, la observación facilitó la recolección de información efectiva, con el establecimiento de conversaciones y un estrecho contacto con los gerentes y empleados claves encargados de la seguridad. En tal sentido, los autores se sometieron a las reglas formales e informales del grupo encargado de la SIF, para que fluyera el curso natural de los acontecimientos sin alterarlo, tal como lo recomienda (Pérez, 1998).

Las entrevistas abiertas fueron aplicadas a especialistas del área de SIF a nivel técnico y gerencial, se comparó con la información recabada en las observaciones y se identificaron otras dimensiones de las variables estudiadas. Cabe destacar que la información suministrada por los trabajadores claves del conocimiento (gerentes y empleados) fue de suma importancia, permitió recopilar datos importantes para la conformación del modelo.

SITUACIÓN DE LA INSEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES VENEZOLANAS BAJO UNA PERSPECTIVA DE UNA ORGANIZACIÓN APRENDIENTE

En Venezuela la situación de la Seguridad de la Información (SIF), particularmente en instituciones educativas a nivel superior es improvisado y sólo unas pocas universidades se involucran con profundidad en el proceso investigativo de este nuevo horizonte (Morales, 2004), ninguna posee un departamento o equipo formal que se encargue únicamente de la SIF, la seguridad es delegada a los administradores de las redes (Morales, 2004; Viloria y Blanco, 2006c). A continuación, Viloria y Blanco (2006c) destacan los factores más importantes que contribuyen a crear un clima de inseguridad de la información:

- Falta una cultura de la seguridad de la información, de códigos deontológicos en el uso de la información y las TIC, de políticas de seguridad, de modelos mentales bajo una perspectiva de la seguridad y alineados con las discipli-

nas de Senge (1992). Según Vargas (2001) "la inercia de los modelos mentales puede impedir el aprendizaje organizacional, sin embargo, al moldearlos podemos lograr que en vez de atacarlos aceleren el aprendizaje". Esta situación trae como consecuencia que la SIF no se asuma como un valor agregado y no exista una visión compartida para afrontar la inseguridad; en efecto, tampoco habrá tensión creativa en los trabajadores del conocimiento, esencia del domino personal. La tensión creativa para Senge (1992) es la yuxtaposición entre la situación actual y la visión compartida, interpretada en este contexto como la fuerza que atrae y presiona al trabajador del conocimiento para adquirir el dominio cognoscitivo necesario para lograr la visión compartida bajo una perspectiva de la SIF.

- No hay aprendizaje en equipo, situación que afecta la creación de una visión compartida y de modelos mentales alineados con las disciplinas de las organizaciones inteligentes, es por ello que no existe la fuerza para desarrollar las actitudes y las aptitudes para afrontar el problema de la inseguridad. Por lo tanto, la organización no aprende, pues las mismas aprenden a través de sus trabajadores (Senge, 1992).
- Falta de un pensamiento sistémico para afrontar los problemas de la inseguridad, quinta disciplina de las organizaciones inteligentes. Se evidencia en la falta de promoción y apoyo por parte de la gerencia alta y media, ven la situación como un problema meramente técnico, descuidan el factor humano, el contexto organizacional. Las instituciones se enfocan a buscar únicamente protección de ataques externos. En resumen, el problema de la inseguridad de la información es un problema de todos, no solamente de los administradores de las redes. Aquí nuevamente se evidencia la falta de una visión compartida bajo una perspectiva de la SIF.
- Los administradores de las redes operan en sus parcelas, Torrealba y Morales (2005) señalan que mantienen una visión asistémica del problema de la seguridad y un enfoque estrictamente técnico, además sus actitudes son reactivas. Por otro lado, Viloria y Blanco (2006c) señalan que los encargados de la seguridad de la información en las organizaciones deben poseer un alto dominio personal, actualizándose permanentemente en la información publicada en organismos públicos y privados sobre nuevas modalidades de ataques y de vulnerabilidades en los sistemas.

Todo lo expuesto evidencia que las universidades venezolanas tienen características que las clasifican como organizaciones con un nivel de aprendizaje de primer ciclo. Los Modelos Mentales como por ejemplo, la seguridad es un problema que lo resuelven los técnicos de computación; impiden el aprendizaje organizacional generativo. Al respecto, Senge (1992) señala que estancan a las compañías e industrias en prácticas anticuadas. Igualmente, Blanco y Viloria (2006c) opinan que contribuyen a mantener a las organizaciones en los ciclos de

aprendizaje más bajos, el de primer ciclo de Argyris y Schon (1978) y el de aprendizaje 0 de Bateson (Cozzi, 2003).

A continuación, la descripción de las características del modelo:

ORIGEN DEL MOSSIU

La propuesta partió del Modelo Dinámico Organizacional de Harold Leavitt (Lucas, 1997, Blanco y Viloria, 1999a; Viloria y Blanco, 2006c) como base de inspiración para crear el MOSSIU, pero bajo una perspectiva de la SIF en el contexto de una organización aprendiente.

MODELO SISTÉMICO

El modelo es sistémico y dinámico, considera a las universidades como sistemas alejados del equilibrio, las propiedades de este sistema no pueden ser explicadas por la suma de sus subsistemas o por uno de ellos, el todo se comporta diferente. En efecto, es importante comprender bajo un enfoque holístico las relaciones de las partes del MOSSIU para entender el problema de la inseguridad de la información en las universidades y lograr la sinergia deseada. El análisis se lleva a cabo en función de los problemas de inseguridad informática generados al adoptar una Intranet o Extranet en las universidades.

EL MOSSIU BAJO UNA PERSPECTIVA DE LA SEGURIDAD DE LA INFORMACIÓN

El MOSSIU tiene cambios con respecto al modelo base de Leavitt, su componente tecnología está representado por las TIC, la cultura está representada por la cultura de la SIF. Las TIC en el MOSSIU están constituidas por la intranet o la extranet universitaria, estas redes privadas son vistas por los autores de este trabajo como estructuras meramente técnicas, pero con un gran impacto en la conducta humana, la cultura, las tareas y los procesos así como en la estructura organizacional. Estas redes privadas sirven de plataforma para la implantación de los sistemas y su integración, sus aplicaciones y bases de datos como la esencia del componente técnico, los usuarios y los operadores representan el factor humano. En efecto, en el MOSSIU, el componente técnico de un SI está en el componente tecnológico y el factor humano está presente en los subsistemas: (a) la gente y cultura y, (b) las tareas y procesos.

Estas redes soportan los Sistemas de Información Gerencial, consideradas en este estudio como "sistemas sociotécnicos; porque además de la tecnología nece-

sitan del factor humano" (Kosciuk, 2006; Blanco y Viloria, 1999). En resumen, el MOSSIU es el modelo extendido del MDO de Leavitt pero bajo un enfoque de la Seguridad de la Información en el contexto de una organización inteligente.

LAS DISCIPLINAS DE LAS ORGANIZACIONES INTELIGENTES EN EL MOSSIU

Así como sucede en los sistemas caóticos (Briggs y Peat, 1999), en una organización los cambios en la estructura, en la cultura organizacional, en las tareas y los procesos, por la adopción de una nueva tecnología, generan desajustes en los subsistemas sociotécnicos y un aumento del desorden. De la misma manera, como en los sistemas caóticos surgen elementos de orden, en el MOSSIU, las herramientas de las organizaciones inteligentes de Senge (1992) y Senge et al (2004c), representan un vórtice más en una organización, pues su aplicación constante contribuye significativamente a reducir la entropía que producen los cambios en el modelo dinámico de Leavitt. Igualmente, las herramientas de Senge son un factor crítico de éxito que contribuyen a reducir los potenciales problemas de inseguridad generados por la adopción de los SI y las TIC, a continuación la descripción de su integración en el MOSSIU.

El Pensamiento Sistémico en el MOSSIU

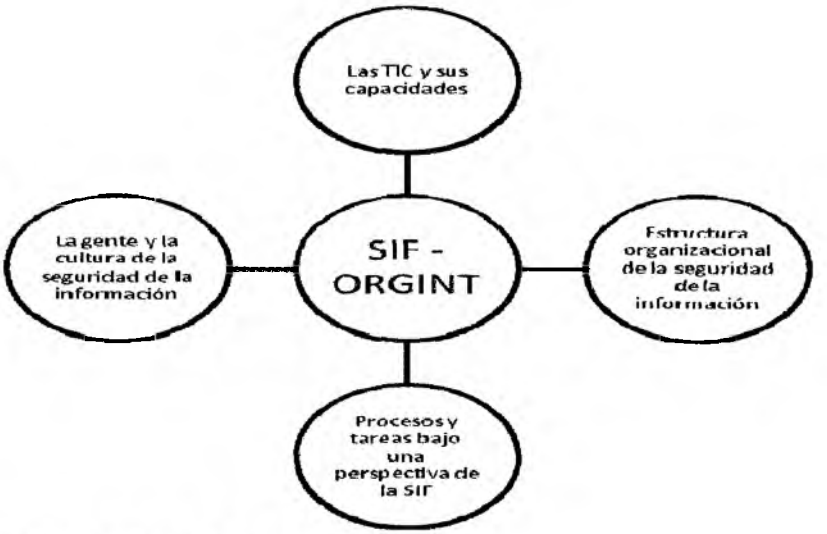
El gráfico 2 visualiza al MOSSIU con su componente de Seguridad de la Información bajo el contexto de las organizaciones inteligentes. Cabe destacar que este elemento no presente en el MDO de Leavitt es un sistema, pues los modelos mentales, el dominio personal, el aprendizaje en equipo y la visión compartida están integrados sistémicamente, por eso la quinta disciplina es el pensamiento sistémico Senge (1992) y Senge et al (2004). Además, señala que esta disciplina integra a las demás, fusionándolas en un cuerpo coherente de teoría y práctica, en donde el todo supera la suma de las partes.

La seguridad en el MOSSIU, bajo una perspectiva de las organizaciones inteligentes, basado en el MDO, significa que las disciplinas propuestas por Senge están presentes o se aplican en cada uno de los componentes del modelo, de esta forma puede garantizarse un mayor nivel de aprendizaje y de progreso en la institución. Por ello la relación del componente SIF-ORGINT con cada uno de los elementos del MOSSIU, ver gráfico 2. En efecto, en el MOSSIU las disciplinas de las organizaciones inteligentes no están separadas del resto de los componentes, todo está conectado y cada elemento influye sobre el otro.

Es importante pensar en sistemas para afrontar los problemas (Checkland, 1981), al considerar la seguridad en los procesos y tareas, en la cultura y la gen-

te, en las TIC y sus capacidades (Torrealba y Morales, 2005). Al respecto, Cano (2005) señala que el concepto de seguridad informática "siempre ha estado en las organizaciones desde hace mucho tiempo, sólo que disociado y especializado en los profesionales de tecnología, y en algunas comunidades de negocio o militares en el tema de procesos organizacionales".En otras palabras, mientras no se comprendan las relaciones existentes entre estos componentes que intervienen en la seguridad, no habrá valor agregado en la organización y no será de utilidad el modelo propuesto.

Gráfico 2. Modelo Sistémico de la Seguridad de la Información en Universidades



Fuente: Leyenda Seguridad de la Información SIF.

La Gente y la Cultura de la Seguridad de la Información

La cultura de la seguridad de la información es una subcultura de la cultura organizacional, puede definirse como: el conjunto de valores éticos y actitudes, las tradiciones, creencias, hábitos, modelos mentales, la visión, las normas, los procedimientos, todo lo que permita identificar la madurez de la institución en la administración de la seguridad de la información y, sobre todo, alcanzar los objetivos, la misión y la visión de la institución bajo una perspectiva de la seguridad de todos sus bienes informáticos.

En este subsistema los trabajadores del conocimiento cuya función es la de garantizar la SIF, observan la problemática de la inseguridad bajo una perspectiva sistémica, igualmente poseen un alto dominio personal. Los equipos de desa-

rrollo de software y de soporte técnico participan, colaboran, dan valor agregado al conocimiento, redefinen tareas, y asumen responsabilidades para alcanzar la visión enmarcada en la SIF. En resumen, la visión compartida enfocada en la SIF es notoria, es una fuerza que estimula a todos los trabajadores del conocimiento y de oficina a crear nuevas actitudes y aptitudes (Dominio Personal) para afrontar y reducir los problemas de inseguridad de la información en la organización, en efecto, es un proceso de aprendizaje continuo. En la cultura de la SIF del MOSSIU, la disciplina del dominio personal es un proceso que permanece en el tiempo, el conocimiento se expande siempre para alcanzar los objetivos.

Las Políticas de la Seguridad Informática (PSI) y los valores éticos son insumos básicos para crear la cultura de la SIF en las universidades, son las condiciones iniciales que facilitan la protección de los activos de una universidad, especialmente la información Factor Crítico de Éxito (FCE), por ello la SIF se orienta a mantener su confidencialidad, su integridad y su disponibilidad (Cano, 2005). La seguridad informática depende de la articulación sistémica de varios factores, uno de ellos lo representa las PSI que simbolizan el marco normativo para el establecimiento de cualquier solución de seguridad en las organizaciones (Viloria y Blanco, 2006c). En las universidades, las PSI se publican en su sitio Web y el responsable de administrarlas es el encargado de monitorear su operacionalización, además de velar por su difusión y promoción continua.

En este subsistema también destaca la disciplina del aprendizaje en equipo, herramienta FCE. Senge (1992) opina que: "Cuando los equipos aprenden de veras, no sólo generan trabajos extraordinarios sino que sus integrantes crecen con mayor rapidez". Sin las disciplinas de Senge es casi imposible realizar un análisis de riesgo efectivo que genere sinergia (Viloria y Blanco, 2006c). En tal sentido, los procedimientos más idóneos y las mejores herramientas de protección establecidas en la institución, son consecuencia del alto nivel de experticia técnica y del proceso dinámico de actualización del conocimiento de los trabajadores encargados de la seguridad, por ello se requiere de un elevado dominio personal individual y colectivo, pues hay que expandir las capacidades y las aptitudes para lograr la disciplina del aprendizaje en equipo y el crecimiento de la institución.

Es primordial que los trabajadores del conocimiento dedicados a la seguridad de la informática trabajen en conjunto para generar sinergia, ya que adquirir el conocimiento en la seguridad requiere de mucha dedicación y colaboración por parte de todos sus miembros. En otras palabras, el equipo es la célula principal del desarrollo de una empresa, así como lo es la familia para la sociedad, por ello su existencia debe estar implícitamente en la cultura de la seguridad.

Cabe destacar que un equipo de seguridad, tal como lo indica su nombre debe aprender a trabajar en conjunto alineado al pensamiento sistémico, poseer las destrezas cognoscitivas y las actitudes proactivas y reactivas para resolver los problemas presentados, el diálogo y la discusión deben estar permanentemente presentes, todos estos atributos determinan un perfil que genera sinergia. En este mismo orden de ideas las disciplinas de Senge (1992) resultan ser las herramientas FCE de las universidades para alcanzar un buen nivel de SIF, así como de los SI y TIC.

Las TIC y sus capacidades

Las TIC forman parte de los sistemas de información de las universidades, sus herramientas son usadas para desarrollar aplicaciones, almacenar datos e información, proteger los bienes informáticos, además poseen capacidades computacionales y de comunicación, un ejemplo es toda la infraestructura tecnológica que soporta a una intranet o extranet universitaria.

Por otra parte, la adopción de una red privada como una intranet o extranet universitaria o la implantación de un sistema de información, trastoca el equilibrio aparente de una institución, aumenta la entropía en todos los subsistemas que integran el MDO de Leavitt, por ello es necesario implementar una serie de estrategias en cada elemento de este modelo, así el sistema se autoorganiza y evoluciona a otra estructura más compleja. Adicionalmente aparecen otros problemas, no contemplados en el modelo de Leavitt que exigen la instrumentación de otros cursos de acción para tratar de controlarlos y minimizarlos, este escenario lo contempla el MOSSIU, este modelo abarca las redes privadas, los servicios de salvaguarda, los mecanismos y herramientas de seguridad y sus capacidades.

La intranet o la extranet universitaria son herederas de los mismos problemas de la Internet, la inseguridad informática (Viloria y Blanco, 2006c). Un ataque desde la Internet o desde el interior de la institución que comprometa la seguridad de un activo informático crítico, desencadena a la vez un ataque a una serie de recursos asociados al árbol de activos de este bien informático. Por ello, este componente del MOSSIU, contempla las metodologías estratégicas bajo una perspectiva de la SIF que integren el análisis y gestión del riesgo entre sus procesos.

Las herramientas de protección de hardware y software así como las capacidades computacionales y de comunicación las identifica este proceso. Los mecanismos de seguridad en el MOSSIU se utilizan para garantizar los servicios de seguridad como: la integridad, la autenticación, la disponibilidad, el no repudio, el control de acceso y la confidencialidad necesarios que emergen de la aplicación de alguna metodología. Entre los mecanismos de seguridad se tienen:

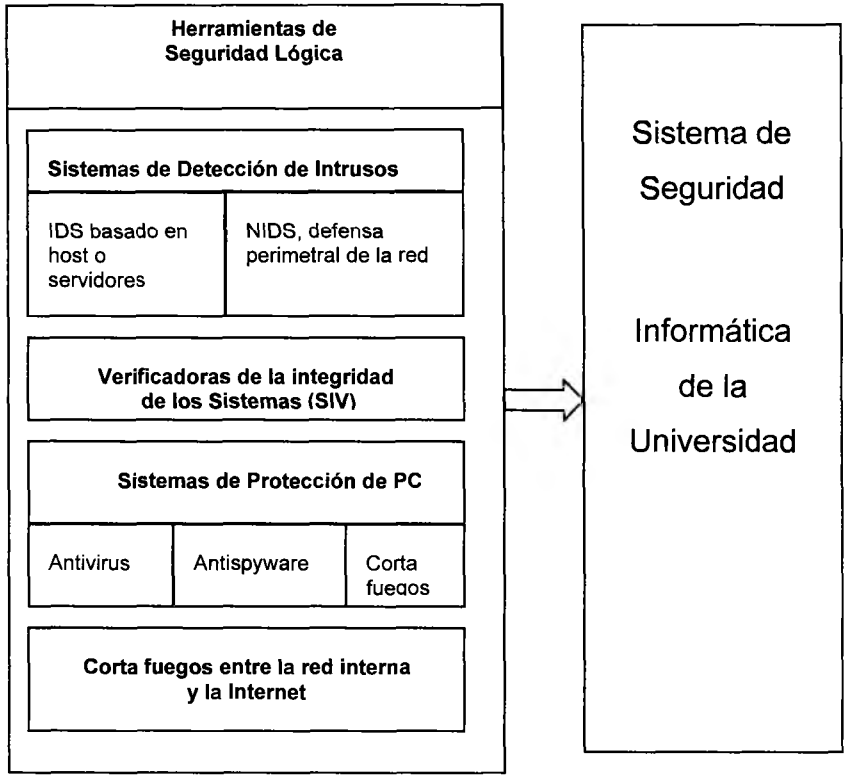
el cifrado, la firma digital, el intercambio de autenticación y el relleno de tráfico, entre otros.

Cabe destacar que la seguridad de la informática no termina con la implementación de estas herramientas. En efecto, en el subsistema de las TIC y sus capacidades del MOSSIU, los equipos de seguridad monitorean los cambios que ocurren en el entorno interno y externo, por ejemplo, las nuevas modalidades de ataque o las diversas variaciones de la ingeniería social, por ello existe una fuerte influencia de la disciplina del dominio personal en este subsistema.

En este subsistema se identifican, sin restricción, las medidas de protección de los activos informáticos con la intención de reducir el riesgo intrínseco, se instrumentan metodologías para identificar las funciones y los servicios de seguridad, se agrupan activos y sus amenazas, se determina el riesgo, y se proponen herramientas y mecanismos de seguridad. Todas las actividades señaladas nunca terminan, son repetitivas e iterativas, debido a los nuevos activos informáticos que deben ser protegidos y los diversos cambios del contexto organizacional, lo que induce a que aparezcan nuevas amenazas y modalidades de ataques.

El gráfico 3 presenta un resumen de las herramientas de seguridad lógica enmarcado en el subsistema de las TIC y sus capacidades que deben incluirse en un sistema de seguridad de una universidad.

Grafico 3: Herramientas de Seguridad Lógica



La Estructura Organizacional de la Seguridad de la Información

La Estructura Organizacional en el MOSSIU, al igual que en el MDO de Leavitt, cambia. En el MOSSIU evoluciona la estructura interna con la finalidad de que los trabajadores del conocimiento y de oficina se acoplen con las formas de realizar las tareas y los procesos como consecuencia de los desajustes producidos por adoptar la tecnología. Es importante destacar que este esquema separa las TIC de otras tecnologías existentes en la organización, ya que las TIC son el eje central que enlaza a todo la empresa (Viloria y Blanco, 2006c). Esta característica de las TIC, en especial de las redes privadas dispara la entropía en la universidad, pues los efectos colaterales afloran en cualquier momento y algunos permanecen ocultos después de adquirir la tecnología, surgen nuevas vulnerabilidades y aumenta la inseguridad de la información. Por ello en este subsistema es importante la existencia de una unidad organizacional de la SIF que abarque la seguridad física y lógica. Asimismo, en este componente del MOSSIU entra en

juego nuevamente la disciplina del aprendizaje en equipo y evidentemente para comprender la situación que es compleja, el pensamiento sistémico.

Esta unidad organizacional posee una visión compartida bajo una perspectiva de la SIF, pero creada por los equipos de trabajo, encargados de la seguridad, por ejemplo parte de la visión puede ser: convertir a la universidad en una de las más seguras de país pero bajo un enfoque de la seguridad de los activos informáticos. Por otro lado, debe prevalecer la disciplina de los modelos mentales, las decisiones que se tomen deben apartar las consideraciones personales, los juicios de valor, los supuestos y todo aquello que conlleve a la gerencia o a los equipos establecidos a cometer errores. Los modelos mentales en este departamento afloran, son revisados y sometidos a una rigurosa revisión para verificar si son fiables y adecuados a la realidad y si es necesario cambiarlos, un ejemplo alineado a las disciplinas de las organizaciones inteligentes puede ser: el trabajo en equipo es un factor crítico de éxito de la SIF, este modelo le da impulso y potencia al dominio personal y al trabajo en conjunto para lograr la visión compartida.

Por otro lado, en este componente existen los códigos de cargos administrativos asociados al rol que cumplen los encargados de la SIF, un ejemplo puede ser: un encargado de la seguridad lógica I o un encargado de la seguridad física II, denominaciones que dependen del dominio personal logrado por los trabajadores del conocimiento en la SIF. Deben incluirse los programas de incentivos socio económicos, pues los empleados con una alta experticia en SIF son muy bien remunerados en el mercado laboral, de esta manera se podría contribuir a mantenerlos en la institución.

En resumen, todo lo señalado en el subsistema de la Estructura Organizacional bajo una perspectiva de la SIF evidenció la gran influencia del subsistema de las herramientas de las organizaciones inteligentes.

Procesos y Tareas bajo una Perspectiva de la SIF

Los procesos pueden estar integrados por varias unidades organizacionales que interactúan a través de la información, asimismo por la propiedad de recursividad de los sistemas, sus componentes son otros subsistemas, en donde aparecen otros elementos, como personas, computadoras, redes, bases de datos, aplicaciones, entre otros. Bajo otra perspectiva, un proceso es la ejecución de un conjunto de tareas en donde se manejan datos e información con la finalidad de lograr un objetivo. Esta teorización conceptual evidencia que el componente Procesos y Tareas tiene una fuerte relación con los otros elementos del

MDO de Leavitt, como la Cultura y la Gente, las TIC y sus Capacidades, y la Estructura Organizacional.

En el componente: los Procesos y las Tareas bajo una perspectiva de la SIF del MOSSIU, la aplicación de procedimientos de seguridad son vitales para blindar a los procesos y las tareas FCE y proteger la información y los datos, se definen de acuerdo a las características del negocio y las tecnologías (TIC) necesarias para instrumentar las PSI (Viloria y Blanco, 2006c), por ello existe una fuerte relación sistémica con los otros componentes del modelo, la cultura por las PSI, las TIC por las herramientas y mecanismos de seguridad y sus capacidades así como la estructura organizacional por el rol que juega la unidad organizacional de la SIF para proteger los activos informáticos involucrados en los procesos. En tal sentido, en este modelo se asume que los equipos de trabajo tienen bien definida la visión compartida y poseen un alto dominio personal, además los modelos mentales se alinean con las disciplinas de las organizaciones inteligentes y el problema de la inseguridad informática se analiza bajo el pensamiento sistémico.

En el caso de las universidades, los procesos y las tareas manejan información crítica como la concerniente a estudiantes, a nómina y a presupuesto, entre otras, que puede ser confidencial, y estar propensa a amenazas de alteración, divulgación no autorizada y sustracción. Asimismo, las redes privadas son la plataforma que soportan a los sistemas de información; en otras palabras, a los procesos críticos que manejan información. El riesgo de materializarse un ataque que provenga de la Internet o desde el interior de la misma institución aumenta, si no se aplican los correctivos a tiempo, hace que participen los procedimientos de seguridad, que es la instrumentación de las PSI, asociados a las características de la universidad, a las TIC y, en consecuencia, a los procesos y tareas. Estos procedimientos son una serie de pasos que al ejecutarse disminuyen la ocurrencia de eventos que afectan la seguridad de la información en la organización. En resumen, los procedimientos de seguridad quedan integrados a los procesos y a sus tareas como parte de ellos, lo que produce un mayor valor agregado y, en consecuencia, mayor sinergia.

Por otro lado, los equipos de trabajo encargados de la SIF no son sus únicos responsables, los trabajadores del conocimiento de otras áreas de especialización y de oficina tienen la responsabilidad de cumplir con las PSI de la organización, por ello deben operacionalizar los procedimientos de SIF de la organización de manera de proteger, reducir y minimizar las amenazas y vulnerabilidades que se ciernen sobre la información y otros activos informáticos que manejan, procesan, almacenan, recuperan y distribuyen información crítica de la institución. Aquí se observa la relación sistémica entre el subsistema de los procesos y las tareas con el de la cultura de la seguridad.

Por último, los procedimientos que ejecutan los trabajadores son para proteger los recursos informáticos, activos de la organización, y son diseñados en función de las TIC y de los sistemas existentes, ya que los procesos están sumergidos en las relaciones entre los tres componentes de un modelo básico de seguridad: procedimientos, personas y la tecnología, pues la integran personas, aplicaciones y las TIC (Blanco y Viloria, 1999a). El éxito depende de la aplicación de las disciplinas de las organizaciones inteligentes, manifiesta en una gestión de la SIF eficiente y efectiva, sistémica que cubra las aplicaciones clave del negocio, la seguridad física y ambiental, una plataforma tecnológica y arquitectura de comunicaciones y la seguridad para terceros. De la misma manera, se deben incluir el código de ética, las PSI, los procedimientos y los estándares adecuados a la institución y a la tecnología, componente de la cultura de la seguridad del MOSSIU, todo enmarcado en un efectivo proceso de gestión de riesgo.

CONCLUSIONES

El MOSSIU, modelo propuesto de gerencia de la seguridad de la información en las universidades, no es una panacea, representa una formulación teórica y sistémica de la gestión de la seguridad de la información en las universidades venezolanas. En tal sentido, este modelo es un marco referencial, una aproximación que apoyará a los gerentes a elaborar planes estratégicos para abordar el problema de la inseguridad de la información en sus instituciones.

El modelo presentado incorpora herramientas de las organizaciones inteligentes presentes en cada subsistema, y la quinta disciplina, el pensamiento sistémico, es vital para comprender las interrelaciones existentes entre las diversas variables del modelo, además facilita la comprensión de la situación de la seguridad de la información en las universidades venezolanas.

Bajo el panorama descrito en este trabajo, la solución del problema de inseguridad de la información no es fácil de afrontar, requiere de mucha experticia técnica y sobre todo gerencial. En el caso de las universidades venezolanas, no están exentas a este problema a pesar de la calidad de los profesionales que laboran en estas organizaciones, pues estas instituciones son sistemas muy complejos con una diversidad de problemas que mantienen permanentemente un alto grado de entropía, la incorporación de la intranet o extranet son factores tecnológicos que contribuyen con este desorden y aumentan la complejidad de estas instituciones.

REFERENCIAS BIBLIOGRÁFICAS

Aceituno (2006), *Seguridad de la información: expectativas, riesgos y técnicas de protección*, Limusa, México.

Argyris C. (1990), *Overcoming Organizacional Defense: Facilitating Organizational Learning*, Needham, MA: Allyn & Bacon, USA.

Argyris, Chris and Schon, Donald (1978), *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley, Massachusetts.

Blanco, W. y Viloria, O. (1999a), *Análisis y Diagnóstico de la Situación Actual en Sistemas y Tecnologías de la Información y una Propuesta de Acciones estratégicas para la USB – Sede del Litoral*, Trabajo de ascenso para optar a la categoría de Asociado, Universidad Simón Bolívar, Venezuela.

— (1999b), "Aspectos Organizacionales a Considerar en el Desarrollo de un Sistema de Información Universitario para la Universidad Simón Bolívar Sede del Litoral", *Revista VI de Investigación*, Vol. 6, Número Único, Caracas.

— (2001), "Propuesta de un Plan Estratégico de Desarrollo de Sistemas y Tecnologías de la Información para el Decanato de Estudios Tecnológicos de la USB Litoral (Fase II)", *Revista Perfiles*, Año 22, No.2, Caracas.

— (2006), "Modelos mentales de la USB y su influencia en el retorno al Litoral Central", *Revista Venezolana de Análisis de Coyuntura*, Vol. 12, Numero 2, Caracas.

Briggs, J. & Peat, F. D. (1999). Las Siete Leyes del Caos. Las ventajas de una vida caótica, Grijalbo, Barcelona, España.

Cano, J. (2005), "Concepto Extendido de la Mente Segura: Pensamiento Sistémico en Seguridad Informática", *Universidad de los Andes*, Colombia. Disponible: http://www.criptored.upm.es/guiateoria/gt_m142x.htm (Consulta 2008, Noviembre 26).

Checkland, P. (1981), Systems Thinking Systems Practice, Jhon Wiley, Chichester.

Cozzi, Enzo (2003), "Cambiando hacia la Sabiduría y los Niveles de Perfección", *Ecovisiones*, mayor/abril, Nª 7, Santiago, Chile. Disponible: http://www.ecovisiones.cl/revista/7/bateson.pdf.

Hernández, R.; Fernández, C. y Baptista, P. (1998), Metodología de la Investigación, MacGraw-Hill, México.

Kosciuk, N. (2006), *Sistemas de Información Gerencial, Copyleft c 2004*, 2005 Alfa Epsilon. Disponible: http://sigfacaunmsm.files.wordpress.com/2008/03/separata-laudon.pdf. (Consulta: 2008, mayo 14).

Laudon, K. y Laudon, J. (2002), *Sistemas de Información Gerencial*, 6da. Edición, Prentice Hall, México.

Leavitt, Harold J. (1965), *Applied organizational change in industry: structural, technological and humanistic approaches in: Handbook of Organizations*, J. G. March (Ed.), Rand McNally, Chicago, IL, USA.

Lucas, H. (1997), *Information Technology for Management*, McGraw-Hill, Sixth Edition, USA.

Mayorca, R. (2007), *Dimensión del Aprendizaje Organizacional de la Universidad Venezolana*, Trabajo Especial de Grado de Magíster en Gerencia Empresarial, Universidad Simón Bolívar, Caracas.

Morales, M. (2004), *Intranet Académica: Modelo del Sistema de Seguridad para un Servicio de Publicaciones*, Trabajo de grado de Magíster en Ciencias de la Computación: Mención Comunicación y Redes, Facultad de Ciencias, Escuela de Computación, Universidad Central de Venezuela, Caracas.

Morales M., Viloria O., Torrealba M. & Isern G. (2000), "Intranet Service Security System Design: Venezuelan Public Universities, a Case Study", *4th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2000) Proceeding Comunications Systems and Networks*, Volumen IV, Orlando-Florida.

Morales M. y Torrealba M. (2004), "Desarrollo de un Modelo de Seguridad para Publicaciones Académicas en el Web mediante UML", *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*, Orlando-Florida.

Pérez, G. (1998), *Investigación Cualitativa. Retos e Interrogantes*, 2da edición, La Muralla, Madrid.

Romero, B. (2008), *Valoración de Activos en el Riesgo para Aplicaciones Web Universitarias. Estudio de Caso: USB*, Tesis para optar al grado de Magíster en Ingeniería de Sistemas. Mención Sistemas de Información, Coordinación de Postgrado de Ingeniería de Sistemas, Universidad Simón Bolívar, Caracas.

Senge, Peter (1992), *La Quinta Disciplina*, Granica, Barcelona, España.

Senge, P., Ross R., Smith B., Roberts Ch. y Kleiner A. (2004), *La Quinta Disciplina en la Práctica*, Granica, Buenos Aires.

Torrealba, M. (2004), *Desarrollo de un Sistema de Apoyo de Redes TCP/IP que Detecta Ataques que se realizan a la Seguridad a través de la Técnica de Covert Channels Sobre ICMP*, Tesis para optar al grado de Magíster en Ciencias de la Computación, Mención Comunicación y Redes, Facultad de Ciencias, Escuela de Computación, Universidad Central de Venezuela, Caracas.

Torrealba, M. y Morales, M. (2004), "Modelo de un IDS para Proteger Sistemas del Tráfico ICMP: Caso del Ataque Loki", *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*, Orlando-Florida.

— (2005), "La Quinta Disciplina como Alternativa Estratégica en la Administración de la Seguridad Telemática", *LIV Convención Anual de la ASOVAC*, Universidad Central de Venezuela, Facultad de Ciencias, Caracas.

Vargas, J. (2001), "La Organización Aprendiente", *Hitos de Ciencias Económico Administrativas*, Año 7, Número 19, México.

Villegas, M. (2008), *Modelo de Madurez para la Gestión de la Seguridad Informática en las Organizaciones*, Tesis para optar al grado de Magíster en Ingeniería de Sistemas, Mención Sistemas de Información, Coordinación de Postgrado de Ingeniería de Sistemas, Universidad Simón Bolívar, Caracas.

Viloria, O y Blanco, W. (1999), "Propuesta de un Plan Estratégico para un Departamento de Computación", *Lumen XXI*, VII, No. 2, Universidad Rómulo Gallegos, San Juan de Los Morros, Estado Guárico.

— (2000), "Evaluación de la Calidad del Servicio del Departamento de Admisión y Control de Estudios de la Universidad Simón Bolívar - Sede del Litoral bajo una perspectiva de Sistemas y Tecnologías de la Información", *Revista Perfiles*, Año 21, No. 1, Universidad Simón Bolívar, Caracas.

— (2001), "Análisis de la Situación Actual del Decanato de Estudios Tecnológicos de la Universidad Simón Bolívar - Sede del Litoral desde una Perspectiva de Sistemas y Tecnologías de la Información (Fase I)", *Revista Perfiles*, Año 22, No. 1, Caracas.

— (2004a), "Aspectos a considerar en una Metodología de Planificación Estratégica de Sistemas y Tecnologías de la Información para el Contexto Universitario Venezolano", *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*, Orlando-Florida.

— (2004b), "Análisis Sistémico del Proceso DDD Bajo una Perspectiva de las Cinco Disciplinas de las Organizaciones Inteligentes: Caso USB – NUL", *Revista Iberoamericana de Sistemas, Informática y Cibernética*, (ISSN: 1690-8627), Vol. 2, No. 1, Florida. Disponible: http://www.iiisci.org/Journal/riSCI/ (Consulta: 2005, Noviembre 11).

— (2006a), "Factores que Bloquean la Aplicación de las Disciplinas de las Organizaciones Inteligentes en el Núcleo del Litoral de la Universidad Simón Bolívar", *Revista Espacios*, Vol. 27, No. 3, Caracas.

— (2006b), "El Sistema DDD y el Proceso de Estimación de la Oferta Académica Bajo una Perspectiva de la Teoría del Caos: Caso USB-NUL", *Revista Perfiles*, Número Único, año 27, Caracas.

— (2006c), *Propuesta Metodológica de Planificación Estratégica de los Sistemas de Información y las TIC bajo el Contexto de las Organizaciones Inteligentes para el Sector Universitario*, Trabajo de ascenso para optar a la categoría de Titular, Universidad Simón Bolívar, Venezuela.