Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009)
"Energy and Technology for the Americas: Education, Innovation, Technology and Practice"
June 2-5, 2009, San Cristóbal, Venezuela.

Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizaciones Inteligentes

Marianella Villegas
Universidad Simón Bolívar, Caracas, Venezuela, nellavillegas@usb.ve

Orlando Viloria
Universidad Simón Bolívar, Caracas, Venezuela, oviloria@usb.ve

Walter Blanco
Universidad Simón Bolívar, Caracas, Venezuela, wblanco@usb.ve

RESUMEN

Esta investigación presenta una propuesta de un Modelo de Madurez de la Gestión de la Seguridad Informática (MMAGSI) en el contexto de las cinco disciplinas de las organizaciones inteligentes de Peter Senge: el dominio personal, los modelos mentales, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico. La metodología fue una investigación de campo de tipo exploratoria, abarcó las siguientes actividades: (a) aplicación de entrevistas estructuradas a personal experto en el área, asesores de empresas y profesores y, (b) se recopiló y categorizó la información obtenida en investigaciones previas de la seguridad informática y aprendizaje organizacional. Las organizaciones que aprenden tienen institucionalizados procesos de reflexión y aprendizaje en la planificación y evaluación de sus acciones, adquiriendo una nueva competencia (aprender a cómo aprender); lo que implica transformar los modelos mentales vigentes, así como generar visiones compartidas. En tal sentido, bajo esta perspectiva, el MMAGSI es un marco conceptual, que ayuda a los gerentes y trabajadores a comprender la situación de la inseguridad de la información en las organizaciones, además de facilitar el proceso de diagnosticar, bajo un enfoque sistémico, cómo se encuentra hoy una organización, y abarcar todos los aspectos involucrados en el problema.

Palabras Claves: organizaciones inteligentes, seguridad de la información, madurez organizacional, tecnologías de la información y de la comunicación.

ABSTRACT

This research presents an Information Security Maturity Management Model (ISMMM) proposal in the context Senge's smart organizations five disciplines: personal command, mental models, shared vision, team learning and systemic thought. The methodology was a field exploratory research which encompassed the following activities: (a) structured interviews to area expert personnel, companies' advisers and teachers and, (b) the data obtained from previous researches about information security and organizational learning was compiled and categorized. Learning organizations have institutionalized reflection and learning processes for planning and evaluating in order to acquire a new competence (to learn how to learn); which implies transforming present mental models, as well as generating shared visions. In that sense, under this perspective, the ISMMM is a conceptual frame, which helps organizations managers and employees to understand information insecurity situations, in addition to it facilitates the diagnosis process under a systemic approach on how an organization is today, so that it includes all the aspects involved in the problem.

Keywords: smart organizations, information security, organizational maturity, information and communication technologies.

1. INTRODUCIÓN

Actualmente, la adopción de las Tecnologías de la Información y de la Comunicación (TIC) y la implantación de los Sistemas de Información (SI) representan un factor crítico de éxito que impacta la competitividad, e impulsa a las comunicaciones y a la integración de los SI, optimizan radicalmente la eficiencia de los procesos administrativos que manejan datos, en consecuencia, disminuyen los costos asociados a estos sistemas y mejoran la calidad de vida de los trabajadores del conocimiento y de oficina en el sitio de trabajo, afectan positivamente la estrategia corporativa de las organizaciones. Sin embargo, con las innovaciones tecnológicas, la adquisición de las TIC y la implantación de los SI, vienen otros problemas que contribuyen aumentar la entropía en los sistemas sociotécnicos de las organizaciones, tales como las vulnerabilidades, las amenazas y a los ataques informáticos.

Además, la situación se complica con el crecimiento descontrolado de la Internet, la proliferación de redes corporativas como las intranets y las extranets, entre otros; conforman el escenario ideal para la actuación de personas inescrupulosas, delincuentes del ciberespacio que, apoyados en el anonimato, intentan acceder a la información privada existente en los SI de las organizaciones. En efecto, a medida que las organizaciones adquieren nuevas tecnologías, se expanden y diversifican, la situación de la gerencia de los procesos relacionados con la seguridad de la información se hace más compleja.

En este mismo orden de ideas, es necesaria, la ejecución de un plan estratégico en el contexto de la Seguridad de la Información (SIF), que evolucione dinámicamente según los cambios en el entorno, en especial aquellos que trastocan la SIF en las empresas. En virtud de todo lo expuesto, las organizaciones no están exentas de situaciones de riesgo que afecten su equilibrio dinámico organizacional (Leavitt, 1965), por lo que requieren comprender el problema, e instrumentar algún esquema de SIF alineado a un plan estratégico que permita a la institución defenderse de eventuales ataques, proteger las vulnerabilidades de los sistemas y reducir el riesgo. La instrumentación de un esquema de seguridad bajo una visión meramente técnica, sin considerar el factor humano, la cultura organizacional, los procesos y tareas críticas y la estructura organizacional, es equivalente a ver la problemática de la inseguridad de una ciudad suramericana como un problema exclusivamente de los cuerpos policiales.

En virtud de todo lo expuesto, este trabajo propone un modelo, cuyo objetivo es disminuir la complejidad y la incertidumbre en la gestión de la SIF en las organizaciones, el modelo es denominado Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizaciones Inteligentes. La asimilación cognoscitiva de este modelo contribuye a la realización de cualquier diagnóstico de la situación en que se encuentra la SIF en las organizaciones, actividad neurálgica de la planificación estratégica bajo esta perspectiva, que facilitaría la identificación de las herramientas de hardware y software necesarias para proteger los activos informáticos.

2. ORGANIZACIONES INTELIGENTES

En esta sección se definen algunos conceptos con la finalidad de facilitar al lector su comprensión. Al respecto existen muchos conceptos de organizaciones inteligentes u organizaciones que aprenden a aprender, a continuación se plantean las consideraciones más adecuadas en esta investigación.

Las organizaciones inteligentes según Senge (1992), son los espacios o lugares "donde las personas continuamente expanden su capacidad para crear los resultados que verdaderamente quieren, donde se cultivan nuevas maneras de pensar, donde la aspiración colectiva queda en libertad así como las personas continuamente aprenden a aprender juntas". Asimismo, Garvin (2003) expresa que en ese tipo de organización existe la capacidad de crear, adquirir, transferir el conocimiento y modificar actitudes y formas de hacer sobre la base de un nuevo conocimiento.

Por otra parte, Choo (2002) define la organización inteligente como aquella que es capaz de integrar eficazmente la percepción, la creación del conocimiento y la toma de decisiones, pero según Nonaka (2008) la manera de crear nuevo conocimiento en las organizaciones y compartirlo no es una mera actividad sino más bien una forma de comportarse, de ser o actuar en donde todos los individuos son trabajadores del conocimiento.

Las disciplinas de las organizaciones inteligentes según Senge (1992) y Senge et al (2004), son cinco que convergen para innovar y resultan decisivas para el éxito de las demás organizaciones, a saber:

2.1 DOMINIO PERSONAL

Representa la disciplina del crecimiento individual, la misma permite ahondar continuamente en la visión personal, concentrar las energías, desarrollar paciencia, ver la realidad con objetividad y conectar el aprendizaje personal al colectivo, es decir, es la ampliación de la capacidad personal para producir los resultados deseados. En esta disciplina existe una fuerte relación entre aprendizaje personal y organizacional, así como compromisos mutuos, los trabajadores son capaces de aprender, alentados y apoyados por la gerencia.

2.2 MODELOS MENTALES

Son supuestos hondamente arraigados, generalizados e imágenes que influyen en nuestro modo de pensar, comprender y actuar, es decir, son nuestros mapas mentales. Esta disciplina apunta a concienciar nuestros modelos mentales internos, y con la realidad para que jueguen a favor de nuestros objetivos. Senge (1992) y Senge et al (2004), expresan que las organizaciones y las personas, al volver el espejo hacia adentro, aprenden a exhumar las imágenes preconcebidas del mundo para llevarlas a la superficie y someterlas a un riguroso escrutinio. Dentro de esta reinvención, también se incluye la aptitud para entablar conversaciones abiertas donde se equilibre la indagación con la persuasión. Sólo allí la gente podrá manifestar sus pensamientos libremente para exponerlos a la influencia de otros.

2.3 VISIÓN COMPARTIDA

La visión, cuando es compartida, establece un lazo afectivo entre las personas, proporciona una sensación de propósito y coherencia en todas las actividades que realiza la empresa, con ella se supone el desarrollo de aptitudes para configurar visiones del futuro comunes que propicien compromisos reales antes que el acatamiento de un conjunto de normas y prácticas dirigidas. En fin, se refiere a la construcción de una visión de futuro compartida y estimulante para los miembros de la organización que estimula un proceso de aprendizaje continuo basado en la esencia del dominio personal que es la tensión creativa.

2.4 APRENDIZAJE EN EQUIPO

El aprendizaje en equipo según Senge (1992), es una disciplina que comienza con el diálogo y la capacidad de los miembros para anular los supuestos y dejar de asumir, para así iniciar un verdadero proceso de pensamiento en conjunto. Implica aprender a reconocer los patrones de interacción que erosionan el aprendizaje en equipo para hacerlos aflorar creativamente y acelerar este proceso. Si los equipos no aprenden, la organización no puede aprender. Este aprendizaje es desarrollar la creatividad, la flexibilidad y el diálogo al interior de los equipos de trabajo, que resulta fundamental para determinar la capacidad que tiene la organización de aprender.

2.5 PENSAMIENTO SISTÉMICO

Es un marco conceptual, es decir, un conjunto de conocimientos y herramientas que se han desarrollado para que los patrones totales resulten más claros y para ayudarnos a modificarlos, en este pensamiento se posee una visión global y de la interrelación de sus partes.

3. METODOLOGÍA

Para lograr el objetivo de este trabajo se realizó una investigación de tipo exploratorio (Hernández et al, 1998), ya que se realizaron entrevistas estructuradas a personal experto, asesores de empresa y profesores del área de seguridad, se recopiló y categorizó información obtenida en investigaciones previas, así como una revisión de textos y sitios Web. Entre las referencias más importantes de este trabajo que brindaron un mayor aporte destacan: Blanco y Viloria (1999), Choo (2002); Garvin (2003); Nonaka (2008); Senge (1992); Senge et al (2004), Villegas (2008); Viloria y Blanco (2006). En todos estos trabajos se aplicaron metodologías formales,

desde estudios exploratorios y descriptivos hasta proyectos factibles. Por otra parte, el modelo MMAGSI está compuesto de niveles y a su vez de características que fueron sometidas a juicios de expertos y adaptadas a las organizaciones inteligentes.

4. EL MMAGSI EN EL CONTEXTO DE LAS ORGANIZACIONES INTELIGENTES

El modelo MMAGSI lo integran cinco niveles de madurez: inicio, crecimiento, desarrollo, madurez e inteligencia organizacional, cada uno posee características que lo definen, las mismas se construyeron con aspectos relacionados con la planificación estratégica, la cultura organizacional y los miembros de la organización, la gerencia, la estructura organizacional así como los procesos y tareas (Leavitt, 1965; Blanco y Viloria, 1999). El objetivo del modelo MMAGSI es contribuir en la gestión de la seguridad informática por lo que adaptarlo al contexto de las organizaciones inteligentes proporcionará un factor crítico de éxito en las empresas. (Villegas, 2008). (Ver Figura 1). A continuación la descripción de cada uno de los niveles:

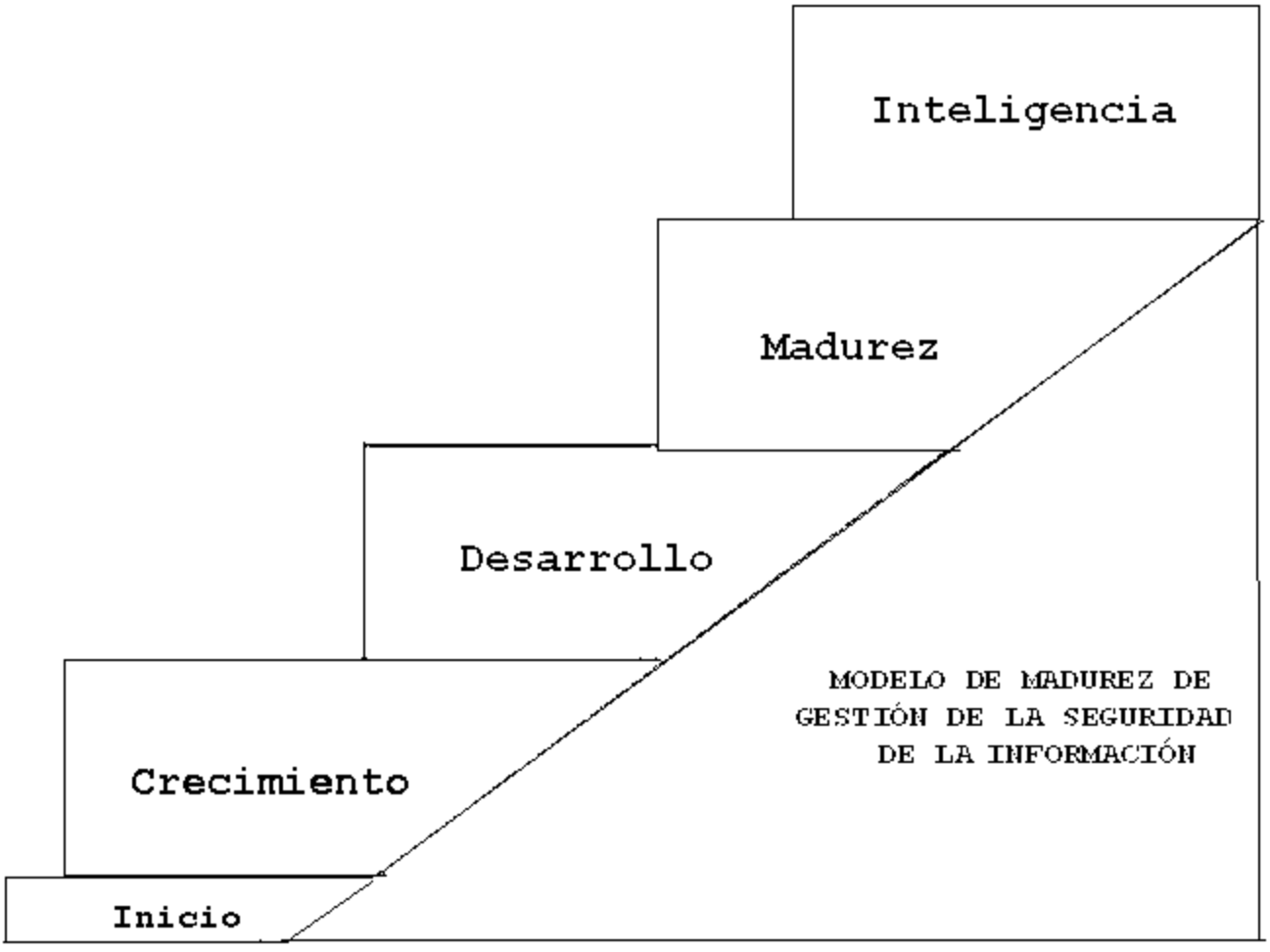

FIGURA 1: MODELO DE MADUREZ DE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA (MMAGSI) TOMADO DE VILLEGAS (2008)

4.1 NIVEL DE INICIO

Es el primer nivel del modelo MMAGSI, en donde las organizaciones no producen las acciones necesarias y suficientes para proporcionar un aprendizaje bajo un sentido de la SIF. Existen altos niveles de anarquía en la

adopción de medidas básicas de seguridad, cada usuario instala herramientas de software y hardware en su computadora, sin estar alineado a ningún plan de seguridad.

Los modelos mentales que sesgan las decisiones y producen soluciones erróneas predominan entre los encargados de la Seguridad de la Información, un ejemplo es considerar al personal técnico como el único responsable de la seguridad (Morales, 2004; Viloria y Blanco, 2006).

Conclusión: no hay actitudes proactivas sino reactivas, por lo tanto no se aplica la disciplina del dominio personal, tampoco hay presencia de las otras disciplinas de las organizaciones inteligentes.

4.2 NIVEL DE CRECIMIENTO

Es el segundo nivel del modelo MMAGSI, todavía no se han superado muchos de los problemas y situaciones presentes en el nivel de inicio; aún existe una barrera en la comunicación entre la alta gerencia y los departamentos de sistemas o afines. Destacan los siguientes indicadores:

4.2.1 ENCARGADO DE LA SEGURIDAD DE LA INFORMACIÓN

Es el responsable de todas las acciones que se deben realizar para mejorar la gestión de la SIF, generalmente uno o dos trabajadores.

4.2.2 MEDIDAS DE SEGURIDAD BÁSICAS

Empieza a tomarse conciencia de que el factor humano también es responsable de muchos de los ataques hacia los activos informáticos, en especial, los trabajadores de la organización.

4.2.3 HERRAMIENTAS BÁSICAS DE HARDWARE Y SOFTWARE

Comienza a aparecer una actitud proactiva ante situaciones de inseguridad de la Información, así como la instalación de software y hardware de seguridad con un mayor nivel de formalidad.

4.2.4 BACKUPS Y RECUPERACIÓN DE DATOS

En esta característica se ejecutan procedimientos de respaldo y recuperación de datos (backups) y su verificación**.** Los respaldos se realizan dentro de la organización y pueden salvaguardarse en un servidor fuera del país.

Conclusión: Surge la preocupación de que la seguridad es un problema de todos, que amerita atención. Se toma conciencia de las debilidades aptitudinales y de las incompetencias de los trabajadores de la seguridad, en otras palabras, comienza a desarrollarse el dominio personal. Por otro lado, persiste cierto ambiente de anarquía, por la instalación del software propietario y libre, sin estar enmarcado en ningún plan de de seguridad.

4.3 NIVEL DE DESARROLLO

Es el tercer nivel del MMAGSI, existe una visión más amplia y sistémica de la SIF, aumenta la preocupación por el problema de la inseguridad de los activos informáticos. Cambia la estructura organizacional, se crea el departamento o unidad encargada de la gestión de la SIF con sus respectivos gerentes y personal adscrito con experticia en el área, dedicados exclusivamente a las actividades concernientes a la seguridad física o lógica. Destacan las siguientes características:

4.3.1 UNIDAD ORGANIZACIONAL O DEPARTAMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Existe un departamento de seguridad de la información cuya misión está orientada a salvaguardar los bienes informáticos, aparecen los equipos de trabajo encargados de la seguridad con experticia en el área, tanto en la seguridad física como en la lógica.

4.3.2 DOCUMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Se crea y se cumple con un documento de la SIF que contiene: los procedimientos de seguridad en los procesos factores críticos de éxito, las funciones, medidas, normas, políticas, los responsables del hardware, software y de la información; así como las obligaciones de cada uno de los miembros de la organización.

4.3.3 VALORES Y CONDUCTAS ÉTICAS

Se definen y difunden los valores éticos que contribuyan con la seguridad de la información. También, se incentivan y crean conductas que favorezcan los valores éticos con respecto al manejo de la información a través de charlas, cursos y seminarios para toda la organización así como en las reuniones departamentales con el fin de crear la cultura de la SIF.

4.3.4 MEDIDAS DE SEGURIDAD INTERMEDIAS

En esta característica existe una actitud proactiva ante situaciones de inseguridad, se elaboran y ejecutan planes de contingencia en caso de ocurrir un ataque. Se implementan procedimientos y controles de detección y respuesta ante los incidentes. Se establecen controles a los usuarios que acceden a los datos y a la información.

4.3.5 DIFUSIÓN DE LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

En esta actividad se difunden las políticas de SIF, ya que no es suficiente desarrollarlas si no van a ser conocidas y ejecutadas por toda la organización.

4.3.6 REGISTRO DE EVENTOS

Se llevan registros de la ocurrencia de los eventos de inseguridad, se activan los procesos de verificación periódica de la base de datos donde están los registros de las incidencias ocurridas, con la finalidad de planificar el mantenimiento correctivo y estimar el preventivo de la SIF.

4.3.7 IMPLANTACIÓN DE LA SEGURIDAD LÓGICA

Corresponde al aseguramiento del software y los SI construidos e instalados en la organización, la protección de las bases de datos, los procesos y cualquier programa, así como el acceso ordenado y autorizado de los usuarios a la información. También, se establecen medidas para la administración de los usuarios y los recursos de las TIC, para así minimizar los riesgos de seguridad asociados con sus operaciones cotidianas.

4.3.8 SEGURIDAD FÍSICA

Se ejecutan planes para la protección de la información en cada una de las áreas de los SI y las TIC y se establecen los controles físicos para los sitios correspondientes, los cuales incluyen el control de acceso al personal autorizado y la prohibición de entrada a personal no autorizado, la protección contra incendios, control de la humedad, de la temperatura, del polvo, respaldo físico (backups) de todo los datos en lugares distantes, entre otros.

Conclusión: Predomina la actitud proactiva ante la reactiva, el dominio personal se fortalece, se instauran grupos consolidados de seguridad con una visión compartida.

4.4 NIVEL DE MADUREZ

Es el cuarto nivel del modelo MMAGSI se caracteriza por tener los siguientes indicadores:

4.4.1 SISTEMA DE ACTIVOS INFORMÁTICOS

Revisión, registro y control de los activos informáticos de la organización (usuarios, ubicación y costo) a través de una base de datos, se lleva un inventario.

4.4.2 ADOPCIÓN DE LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN (PSI)

Protección de la información y de los activos informáticos, garantizar la: confidencialidad, integridad, disponibilidad, autenticación, no repudio, control de acceso, consistencia y auditoría. Creación y ejecución de programas de concienciación para el cumplimiento de las políticas de la seguridad, así como la revisión y actualización de las PSI (Amendolia y Cendagorta, 2004).

4.4.3 DESARROLLO DE UN PLAN ESTRATÉGICO

Construir un plan estratégico el cual debe considerar las características representativas de la organización, en cuanto a sus activos de información y requerimientos de seguridad.

4.4.4 AUDITORÍAS INTERNAS Y EXTERNAS

Ejecución de auditorías externas e internas periódicamente, definiendo el ámbito y los objetivos perseguidos, así se validan y recomiendan cambios en función de los resultados obtenidos. Adopción de medidas correctivas para superar las deficiencias detectadas en la auditoría de seguridad.

4.4.5 MEDIDAS DE SEGURIDAD AVANZADAS

Entre las medidas se tiene el desarrollo de capacidades y destrezas relativas a la seguridad de la información, las mismas son promovidas en la organización, existen controles de acceso en el software para los usuarios que accedan a los datos, recursos en el desarrollo de sus funciones y se implanta un mecanismo de identificación de usuarios con el establecimiento de niveles de usuarios y claves o combinación de éstas.

4.4.6 ADOPCIÓN DE LOS VALORES ÉTICOS

Los valores éticos de la seguridad de la información forman parte de la cultura de la seguridad, a través de sus acciones ante las eventualidades ocurridas en la gestión de la seguridad. La diferencia de esta característica es que en este nivel se cumplen los valores éticos, no sólo se crean y conocen como en el nivel anterior.

4.4.7 VISIÓN COMPARTIDA

Existe una visión compartida bajo una perspectiva de la SIF, donde la misión, visión, objetivos y estrategias incluyen la seguridad y se promueve entre el grupo encargado en la organización.

4.4.8 TRABAJO EN EQUIPO

Las organizaciones ubicadas en este nivel, trabajan en equipo y existen grupos encargados de la seguridad de la información, asimismo promueven la capacitación del personal encargado de la seguridad y la comunicación entre los grupos de trabajo.

Conclusión: Los equipos de trabajo de la SIF trabajan en conjunto, generan sinergia y están bajo una visión común de ésta, estimulados por la aceptación colectiva de modelos mentales compartidos. La organización resalta muchas características que le permite generar conocimiento.

4.5 NIVEL DE INTELIGENCIA ORGANIZACIONAL

Este nivel se caracteriza por tener los siguientes indicadores:

4.5.1 CULTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

Se instaura una cultura de la SIF en la organización, se conocen, aceptan, comparten y cumplen los valores éticos y las políticas de seguridad informática. Existe un compromiso de la alta gerencia en la ejecución de los planes estratégicos de seguridad, así como se participa activamente en la promoción de los valores éticos. La misión bajo una perspectiva de la seguridad está bien planteada. Igualmente, la visión es compartida e influye significativamente en el desarrollo del dominio personal.

4.5.2 DESARROLLO DE APTITUDES Y ACTITUDES

Se desarrollan las aptitudes y actitudes de todos los miembros de la organización con respecto a la seguridad de la información, ya que los usuarios son los mayores responsables de los problemas de inseguridad.

4.5.3 ANÁLISIS Y GESTIÓN DE RIESGO

Se aplican metodologías de análisis y gestión de riesgo con cierta frecuencia, a toda la plataforma tecnológica existente, las TIC y los SI, así como a los nuevos activos informáticos. Se sugiere seleccionar la metodología más adecuada que se adapte a los requerimientos de la organización y se ajusta a las especificaciones del negocio (definición de las amenazas, de las categorías de los activos, de los criterios de evaluación de riesgo, entre otros). Además se realizan análisis y gestión de riesgo de los nuevos activos incorporados a la institución, éstos pueden ser hardware o software.

4.5.4 EJECUCIÓN DEL PLAN ESTRATÉGICO

En esta característica la gerencia monitorea la operacionalización de los planes estratégicos establecidos en el nivel anterior enfocados a la SIF.

4.5.5 MONITOREO PERMANENTE A LOS ACTIVOS INFORMÁTICOS

Existe un monitoreo permanentemente en la red y control de los registros de ataques y eventos ocurridos en la organización. En consecuencia, se realizan estadísticas, gráficos de ellos para realimentar la planificación estratégica y adecuarla a la realidad, así como para establecer las medidas preventivas y correctivas necesarias a futuro.

4.5.6 RESPONSABLE DE LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La institución, a través de la unidad organizacional encargada de la SIF, designa a un grupo del conocimiento (con alto dominio personal) con un líder (gerente) como responsables del conocimiento y cumplimiento de las políticas de seguridad de la información por todo el personal de la organización. Asimismo, éstas políticas pueden adaptarse a alguna norma internacional reconocida aunque la institución puede instaurar sus propias políticas.

Conclusión: en virtud de los indicadores descritos, la empresa alcanzó su máximo nivel de madurez, es una organización que aprende a aprender, la cultura de la seguridad está arraigada, las disciplinas de las organizaciones inteligentes son aplicadas en el ámbito organizacional de la seguridad de la información. La relación sistémica entre las disciplinas se encuentra en un nivel que genera sinergia, la cual se manifiesta en los procesos que se activan a raíz de ataques hacia los activos informáticos. Estos procesos están sustentados en todo el conocimiento producido por la organización, ya que los grupos encargados de la seguridad por trabajar en equipo y poseer un alto dominio personal, manifiestan que les permite tomar decisiones proactivas. En otras palabras, la organización responde con más eficiencia y efectividad a los embates del medio interno y externo que trastocan el equilibrio dinámico de la organización (Leavitt, 1965, Blanco y Viloria, 1999) llevándolo a un estado de mucha entropía (Briggs y Peat, 1999) y por otro lado la lleva rápidamente a su equilibrio aparente (Viloria y Blanco, 2006).

El modelo MMAGSI en el contexto de las organizaciones inteligentes tendría como:

- Estrategia, una dirección y un equipo de empleados conscientes del problema de la inseguridad de la información, de sus fortalezas y debilidades; para definir una misión, visión y objetivos en términos de conocimiento previos de la SIF.
- Infraestructura, que incluye los procesos organizativos de la empresa y las TIC como mecanismos acordes para facilitar la creación y el intercambio del conocimiento.
- Gestión de personal, que es el pilar clave de toda la gestión del conocimiento y está ligado a los aspectos culturales de la organización.

5. CONCLUSIONES

El Modelo de Madurez de la Gestión de la Seguridad Informática bajo el contexto de una organización inteligente, tiene como objetivo la disminución de la incertidumbre y la complejidad en la situación en que se encuentra la seguridad de la información en una organización, los cinco niveles que lo integran no se limitan exclusivamente a describir factores que influyen sobre ella, como los gerenciales, el análisis de gestión de riesgo, la planificación estratégica y la cultura organizacional, entre otros. Este modelo incorpora herramientas de una organización aprendiente alineada con el concepto de Peter Senge, característica que permite derrumbar algunos mitos y creencias que afectan la instrumentación de acciones que reducen el riesgo potencial de materializarse una amenaza, dada una vulnerabilidad asociada a un activo informático. En efecto, las disciplinas de las organizaciones inteligentes le dan valor agregado al modelo propuesto, generan sinergia.

El problema de la inseguridad informática no se resuelve únicamente al identificar los servicios de seguridad a proteger, las herramientas de seguridad de las TIC, la operacionalización de las políticas de seguridad y las normas, la situación es compleja, trasciende los aspectos tecnológicos, involucra el trabajo en conjunto de los trabajadores encargados de la seguridad, el desarrollo continuo de nuevas actitudes y aptitudes, la aplicación del pensamiento sistémico, un factor crítico al incorporar el dogma de las organizaciones inteligentes, sus valores éticos, la visión compartida y los modelos mentales bajo una perspectiva de la seguridad de la información. Sin embargo, en muchas organizaciones, los gerentes y el personal encargado de la seguridad de la información poseen un modelo mental que impide a las organizaciones alcanzar un mayor nivel de madurez en el manejo de la situación, como: los problemas de inseguridad de la información solamente los resuelve el personal técnico de computación.

REFERENCIAS

Amendolia D. y Cendagorta J. (2004). Políticas de Seguridad Informáticas. http://www.criptored.upm.es/guiateoria/gt_m148q.htm, 01/20/09.

Blanco W. y Viloria, O. (2006). "Modelos Mentales de la USB y su Influencia en el Retorno al Litoral Central". *Revista Venezolana de Análisis de Coyuntura"*. Vol. 12, N° 2, pp. 225-243.

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

Choo, C. (2002). *Information Management for the Intelligent Organization*, Third Edition. Published by Information Today/Learned Information, pp 35.

Garvin, D. (2003). *Learning in Action: A Guide to Putting the Learning Organization to Work (Hardcover)*, Hardvard Business Publishing. HBS Press Book, pp 58-60.

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

Leavitt, H. (1965). *Appling Organizational Change in Industry: a structural, Technological and humanistic Approach*. En, J. G. March (ed.) Handbook of Organizations Chicago. Rand. McNally.

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 de la Universidad Central de Venezuela, Caracas, Venezuela.

Nonaka, I. (2008). *The Knowledge-Creating Company*. Harvard Business School Press Publishing, pp 9.

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

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

Villegas, M. (2008). “Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades”. Trabajo de Grado para optar a la Magíster en Ingeniería de Sistemas. Universidad Simón Bolívar. Caracas. Venezuela.

Viloria, O y Blanco W. (2006). “Propuesta Metodológica de Planificación Estratégica de los Sistemas de Información y las TIC bajo el Contexto de las Organizaciones Inteligentes para el Sector Universitario. Universidad Simón Bolívar”. Trabajo de Ascenso para optar a la categoría de Titular. Universidad Simón Bolívar. Caracas. Venezuela.

Autorización y Renuncia

Los autores autorizan a LACCEI para publicar el escrito en los procedimientos de la conferencia. LACCEI o los editores no son responsables ni por el contenido ni por las implicaciones de lo que esta expresado en el escrito

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.