



Universidad Autónoma Metropolitana

Unidad Xochimilco

**ASPECTOS DE LA GESTIÓN Y CAPACIDADES TECNOLÓGICAS
QUE INCIDEN EN LA SEGURIDAD DE LA INFORMACIÓN EN
MEDIOS DIGITALES (SIeMD) EN LA RED NACIONAL DE
SEGURIDAD EN COMPUTO (RENASEC) PERTENECIENTE A LA
ASOCIACIÓN NACIONAL DE UNIVERSIDADES E INSTITUCIONES
DE EDUCACIÓN SUPERIOR (ANUIES)**

**INVESTIGACIÓN PRESENTADA EN LA DIVISIÓN DE CIENCIAS
SOCIALES.**

Que para obtener el grado de:

**MAESTRO EN ECONOMÍA Y GESTIÓN DEL CAMBIO
TECNOLÓGICO.**

Por

JOSÉ ALBERTO SALDAÑA JUÁREZ

**Asesor de la investigación.
Dr. Manuel Soria López**

México D.F., Diciembre 2006

Dedico esta tesis:

A mi chiquita preciosa, amor de mi vida y esposa mía; no solo esta tesis, sino mi vida entera está dedicada a ti, gracias por más de 12 años de inmensa felicidad.

A Yolo y Pepe, amorcitos, hijos preciosos, regalos de Dios, les dedico esta pequeños y toda mi vida.

A mi familia, Yoy, Mamá, McClaus y Andru, ejemplos de amor y trabajo.

Al Dr Manuel Soria y familia, Gran Caballero, maestro admirado, amigo mío.

A Maru, porque mis hijos tienen mucha abuela... y dos.

Con mucha estima a Argel, Angélica y a los Doctores Francisco Ortiz, Laura Peñalva y Ángel Taboada Uribe

Agradecimientos:

Hay tanto y tanta gente a quien agradecer, y poco el espacio, pero hay que hacerlo.

Gracias:

A mi familia hermosa, Elena, Yolo y Pepe.

A la casa de mis papas, Yoy, Mamita y Claus, así como mis abuelitas: Abuelita Cata y Abuelita Magos QEPD.

A ti mi Dios.

A mi asesor: El Dr. Manuel Soria y su familia, hay muchos motivos para decir gracias, así que, gracias, gracias, muchas gracias por todo.

A mis ejemplos: El Dr. Jaime Aboites, la Dra Laura Peñalva y al Mtro Angel Taboada Uribe, gracias por sus comentarios y aportaciones pero sobre todo por ser lo que son, un ejemplo para mi, y tres personas extraordinarias, muchas gracias.

A mis profesores: Dr Manuel Soria, Dra. Laura Peñalva, Dr. Daniel Villavicencio, Dr. Jaime Aboites, Mtr Carlos Hernández, Dr Rysa Rozga, Mtr Roberto Constantino, Dra. Gabriela Dutrenit, Mtr Mario Capdeville, asimismo a Claudia, Berthita y Victor Manuel

A la ANUIES y sus agremiadas, pero sobre todo a las instituciones educativas que me han dado la oportunidad de dar cátedra y me han abierto las puertas de la docencia: Gracias UP, UNITEC y UPIICSA.

A Francisco Ortiz y a mis alumnos de la 1ª generación de Ingeniería Industrial en Gestión e Innovación Tecnológica de la Universidad Panamericana.

A mis alumnos de la Universidad Tecnológica de México y de UPIICSA.

A mis compañeros de la Maestría, especialmente les quiero agradecer a Argel y Angélica, gracias pero muchas gracias.

A mis familiares y amigos: Anvaas, Ivonne, Mario (Unitec), Kika, Meche y Lupita (Unitec), Paco, Oscar Amador, Erika y Ray (Compadres), A mi Tío Luís, A mis dos tías Margaritas, A mi tío Lalo, A mi tío Chilo (QEPD) Gracias pero muchas gracias.

A Carl Sagal y a Alberth Einstein QEPD culpables de que sea ingeniero.

A Debar Shalom, Shinemi Mahahuay, Kerigma y Le Ku, siempre les enciendo una vela.

No te he olvidado Jorge, amigo mío, mi hermano, que la fuerza te acompañe, nos vemos en el cielo.

- i. Portada**
 - ii. Dedicatoria**
 - iii. Introducción**

 - 1. Marco Teórico y Conceptos Básicos:**
 - 1.1. Introducción**
 - 1.2. Los medios digitales:**
 - 1.2.1. La información en los medios digitales:**
 - 1.2.2. El conocimiento en los medios digitales:**
 - 1.3. La seguridad y la información**
 - 1.4. La seguridad de la información**
 - 1.4.1. Seguridad y Tipos de ataque**
 - 1.4.2. Tipos de Tecnología**
 - 1.5. Las Capacidades de una organización**
 - 1.5.1. Las Capacidades:**
 - 1.5.2. Las Capacidades Tecnológicas:**
 - 1.6. Corriente Evolucionista, Trayectorias Tecnológicas y patentes**
 - 1.6.1. Corriente Evolucionista, Trayectorias Tecnológicas.**
 - 1.6.2. Estudio de patentes.**
 - 1.6.2.1.Desventajas del uso de patentes para un estudio de caso.**
 - 1.6.2.2.Convergencia, Divergencia y Patentes**
 - 1.6.2.3.Estudio de Patentes “Palabras Claves”**
 - 1.6.2.4.Estudio de Patentes “Clases de Patentes”**
 - 1.7. La gestión tecnológica en las organizaciones:**
 - 1.7.1. Gestión**
 - 1.7.2. Gestión Tecnológica**
 - 1.7.2.1.Vigilar y analizar:**
 - 1.7.2.2.Focalizar:**
 - 1.7.2.3.Capacitar**
 - 1.7.2.3.1. Generación interna de conocimiento mediante la realización de investigación y desarrollo.**
 - 1.7.2.3.2. Transferencia en un esquema comercial**
 - 1.7.2.4.Implantar**
 - 1.7.2.5.Aprender**
 - 1.8. Divergencia y convergencia tecnológica en las TIC’s**
 - 1.9. Los sistemas de gestión de seguridad de la información**
 - 1.10. Herramienta de medición de capacidades y gestión tecnológica.**
 - 1.11. Hallazgos y conclusión de capítulo**

 - 2. Metodología**
 - 2.1. Introducción**
 - 2.2. El Estudio de caso**
 - 2.3. Etapa Preliminar**
 - 2.3.1. Fuentes de Información**
 - 2.3.2. Encuestas y bibliografía especializada**
 - 2.4. Etapa 1:**
-

- 4.4. Evolución de las Capacidades Tecnológicas de seguridad en las IES y la RENASEC 1999-2006**
 - 4.4.1. Una ANUIES Insegura 1999 - 2000**
 - 4.4.2. LA RENASEC 2001-2002**
 - 4.4.3. 2003-2006 La gestión Tecnológica en la UNAM-RENASEC**
 - 4.4.3.1.Periodo de Gestión Tecnológica en seguridad de la Información UNAM-RENASEC**
 - 4.4.3.2.La exigencia de seguridad de calidad en la ANUIES y la RENASEC**
 - 4.5. Hallazgos y conclusiones del capítulo**
 - 5. Gestión tecnológica de seguridad de información en medios digitales. El caso de la RENASEC perteneciente a la ANUIES.**
 - 5.1. Introducción**
 - 5.2. Gestión Tecnológica**
 - 5.2.1. Vigilar y analizar el elemento Tecnológico (Trayectorias y Capacidades Tecnológicas)**
 - 5.2.1.1. Elementos empíricos de las encuestas realizadas en los años 2002, 2004 y 2006**
 - 5.2.1.2.Trayectorias Tecnológicas (Seguridad de la información) y su evolución**
 - 5.2.2. Focalización**
 - 5.2.2.1.Los Objetivos**
 - 5.2.2.2.La Dirección**
 - 5.2.3. Capacitación**
 - 5.2.3.1.Generación interna de conocimiento mediante la realización de investigación y desarrollo**
 - 5.2.3.2.Transferencia de capacidades en un esquema comercial**
 - 5.2.3.3.Transferencia en un esquema de acuerdo y cooperación**
 - 5.2.4. Implantación**
 - 5.2.5. Aprendizaje**
 - 5.3. Análisis de los resultados**
 - 5.4. Hallazgos y conclusiones del capítulo**
 - Conclusiones, Bibliografía**
 - Anexos**
-

Índice de Figuras y Cuadros:

Capítulo 1

Figura 1.1 Esquema de Capacidades, Realización Propia, Fuente: Teece y Pisano (1994), The dynamic capabilities of firms: an introduction, en Industrial and Corporate Change.

Figura 1.2 Elementos claves para la Gestión de tecnología Fuente Cotec (1999)

Capítulo 2

Figura 2.1 Matriz para la elección de un método de investigación social según las características del objeto de estudio y el problema de interés. Fuente Yin (1994)

Figura 2.2 Esquemmatización de las rutinas usada en la presente tesis, Realización propia.

Figura 2.3 Grafica propuesta para el tratamiento de datos de “Tipos de Tecnología usada en los ataques a la seguridad de la información en medios digitales”, Realización propia. Fuente de datos a interpretar: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática”

Figura 2.4 Grafica propuesta para el tratamiento de datos de “Clasificación por número de incidentes totales”, Realización propia. Fuente de datos a interpretar: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática

Figura 2.5 Modelo de Gráfica propuesta para medir la Evolución de las tecnologías usada en materia de seguridad por año, Realización propia, Fuente a usar: CSI/FBI (2002, 2003, 2004, 2005 y 2006), Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 2.6 Modelo de Gráfica de “Intensidad Inventiva” a través del tiempo

Figura 2.7 Grafica Cruzada evolutiva de capacidades tecnológicas y capacidades de gestión tecnológica a través del tiempo. Adecuación de modelo propuesto por Bell y Pavitt (2006),Fuente: Realización Propia

Tabla 2.1 Interpretación de la Evolución de los tipos de ataque, Fuente a usar: CSI/FBI (2002, 2003 y 2004) Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey.

Tabla 2.2 Tabla resultante para el análisis de pendientes, Realización Propia.

Capítulo 3

Figura 3.1 Evolución de los tipos de ataque, Realización propia, Fuente: Mancera & Young (1997 – 2004) “Encuesta Global de seguridad informática”

Figura 3.2 Evolución del # total de incidentes promedio por año, Realización propia, Fuente: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática”

Figura 3.3 Evolución del tipo de tecnología usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (2002, 2003, 2004, 2005 y 2006), Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 3.4 Evolución de las ID digitales usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 3.5 Evolución de “Monitoreo y detección de intrusos” usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 3.6 Evolución de “Desarrollo de tarjetas inteligentes” usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 3.7 Evolución de “Seguridad Física” usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Figura 3.8 “Clases de patentes” mas significativas en las TIC’s y los Sistemas de Seguridad de la Información en Medios Digitales obtenidas a partir de un estudio exploratorio de patentes denominada “Palabras Clave”. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

Figura 3.9 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con las clases de patentes G06F, H04, G11, H04K , tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

Tabla 3.1 Interpretación de la Evolución de los tipos de ataque, Realización propia, Fuente: Mancera Ernest Young (1997 – 2004) “Encuesta Global de seguridad informática”

Tabla 3.2 Interpretación de las “Tecnologías de Seguridad Usadas”, Realización propia, Fuente: Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Tabla 3.3 Concentrado de resultados en la medición de la intensidad inventiva de patentes por palabra clave entre los años 1980 a 1992 y 1993 a 2005 en Estados Unidos (USITO) y el Mundo (ESPaNET).

Capítulo 4

Figura 4.1 Conformación de las 6 regiones estratégicas de la ANUIES

Figura 4.2 Flujos de información de las 6 regiones estratégicas de la RENASEC-ANUIES

Capítulo 5

Figura 5.1 Comparación de la evolución de las capacidades tecnológicas y del nivel de gestión de seguridad en la ANUIES (Realización propia)

Figura 5.2 Comparación de la evolución de las capacidades tecnológicas y del nivel de gestión de seguridad en las IES (Realización propia)

Figura 5.3 Comparación de la evolución de las capacidades tecnológicas en las IES y en la RENASEC (Realización propia)

Figura 5.4 Comparación de la evolución del Nivel de Gestión Tecnológica entre las IES y en la RENASEC (Realización propia)

I
N
T
R
O
D
U
C
C
I
O
N

... uno necesita conocerse a sí mismo, además de conocer al enemigo para mantenerse exitoso, estar en posición de enfocar sus iniciativas de seguridad de la información en base a amenazas creíbles y no sobre estrategias reactivas. La sobrevivencia de una organización depende de su capacidad para adaptarse a los cambios en el entorno... posiblemente muchas de ellas (organizaciones) no se conocen a sí mismas ni a su enemigo tan bien como debieran hacerlo, lo que resulta en un enfoque no apropiado para el creciente número y variedad de amenazas.

Encuesta Global de seguridad de la Información 2004
Mancera Ernst & Young

i. Introducción

La trascendencia de este proyecto de tesis se manifiesta precisamente en la importancia de la información que maneja la ANUIES, ya que, como institución reguladora, concentra en ella los resultados (calificaciones) de todos los alumnos y exalumnos de educación superior tanto de universidades, públicas como privadas, adscritas a ella (cerca del 96% del total de las universidades del país); además está facultada para corroborar la autenticidad de nivel de estudio (Licenciatura y postgrado) de cualquier persona. En otras palabras, la ANUIES es una institución que concentra la información crítica de las universidades de todo el país, lo que obliga a tener dentro de ella una gestión tecnológica enfocada a la seguridad de la información, ya que cualquier indicio de inseguridad podría derivarse en un problema de magnitud a nivel nacional.

A nivel nacional e internacional el crecimiento y desarrollo de las TIC's ha sido extraordinario, los elementos tecnológicos aplicados, su dinámica y beneficio innovativo económico ha sido usado por muchos países que han aprovechado, de una forma u otra, la apertura hacia la era de la información (Castells, M. 1996-2000):

Esta revolución, también conocida como el nuevo paradigma socio tecnológico (Perez, C. 2000), tiene diversas características distintivas, entre las más importantes tenemos la de que nunca se había presentado antes una dinámica de cambio tecnológico e innovación tan intensivo y duradero. Este hecho podría suponer que, si bien los elementos informáticos, de comunicaciones e incluso electrónicos, se han acoplado a dicha dinámica, existen algunos otros elementos que, por su propia naturaleza, sus características

económico productivas, etc, no pueden seguir la dinámica de cambio tecnológico mostrado por las TIC's en general.

En las organizaciones, al no tener las capacidades de seguimiento o presentar una menor dinámica de cambio tecnológico, se han manifestado diversos problemas, dificultades, riesgos, etc. que inciden en consecuencias desde diferentes perspectivas: legal, organizacional, tecnológico, económica, etc.

Dichos problemas, dificultades y riesgos tienen un efecto de incertidumbre al momento de trabajar y usar información, sobre todo en esquemas donde la información es crítica.

En este ambiente de inseguridad en las fuentes de información, una primer aproximación para el control de la inseguridad sería un esquema de gestión tecnológico avanzado, sin embargo, los resultados negativos en este rubro nos hacen suponer que existen elementos fundamentales dentro de la gestión tecnológica que no han sido agotados y que pueden explicar los comportamientos de dicha inseguridad.

Dado lo anterior, el objetivo de estudio de la investigación de tesis consiste en analizar algunos de los elementos fundamentales en materia de gestión tecnológica y capacidades tecnológicas (de acuerdo al modelo Cotec¹) que inciden en la seguridad de la información en medios digitales (SIeMD); Identificando con ello, los mecanismos por los cuales el nivel de gestión y capacidad tecnológica evidencian el aumento o disminución de la seguridad de dicha información en medios digitales, la investigación se aplica a un caso de estudio en una institución nacional. Al respecto, el estudio de caso lo componen dos agentes: los miembros activos de la ANUIES² y que están adscritos en la RENASEC³ y la misma RENASEC

Preguntas de Investigación

En ésta investigación se plantean las siguientes preguntas:

Desde la perspectiva de capacidades y gestión de la tecnología en la seguridad de la información en medios digitales

¹ Cotec es una fundación de origen empresarial que tiene como misión contribuir al desarrollo del país mediante el fomento de la innovación tecnológica en la empresa y en la sociedad española.

² La ANUIES es la Asociación Nacional de Universidades e Institutos de Educación Superior.

³ La RENASEC es la Red Nacional de Seguridad en Computo

¿Cuáles son los factores, desde una perspectiva tecnológica, que provocan la inseguridad de la información en medios digitales?

Desde la perspectiva de la RENASEC

¿Son dichos factores fundamentales en el proceso de gestión tecnológica en seguridad de la información en ambientes digitales de la ANUIES, específicamente correspondiente a la RENASEC y sus asociados las Instituciones de Educación Superior (IES)?

Desde la perspectiva de la gestión tecnológica de la RENASEC

¿Es la RENASEC capaz de aplicar un modelo exitoso de gestión tecnológica de acuerdo a la evaluación de sus capacidades tecnológicas y los niveles de Gestión Tecnológica?

Objetivos Específicos

Para poder resolver las preguntas de investigación se plantean los siguientes objetivos específicos:

1. Hacer una revisión conceptual de los elementos más importantes sobre: gestión tecnológica, medios digitales, seguridad de la información.
2. Analizar las tendencias en la evolución de las trayectorias tecnológicas en materia de seguridad de la información en medios digitales.
3. Identificar las principales herramientas y metodologías usadas en la gestión tecnológica enfocada a la seguridad de la información en medios digitales
4. Analizar las trayectorias tecnológicas de las capacidades tanto de la RENASEC como de las IES asociadas a la ANUIES
5. Determinar los factores intrínsecos de la gestión tecnológica que crean inseguridad y riesgo en la información y que son usados por las IES y la RENASEC de forma conjunta

Hipótesis

Dado lo anterior, la **Hipótesis** específica de tesis también se divide en tres sentidos:

De la primer pregunta: los factores que provocan la inseguridad de la información en medios digitales van relacionados con elementos de tipo “gestión tecnológica” y no solamente de “capacidades tecnológicas”

De la segunda pregunta: la inseguridad de la información en ambientes digitales se debe principalmente a 3 elementos:

1. Retraso dinámico (divergencia tecnológica)
2. Elementos deficientes en la gestión tecnológica dentro de las organizaciones que utilizan medios digitales particularmente en el caso de la gestión tecnológica de la relación entre las IES y la RENASEC.
3. Capacidades tecnológicas limitadas

De la tercer pregunta: SI, la RENASEC es capaz de aplicar un modelo de “gestión tecnológica” exitoso.

La metodología utilizada para la investigación es la de estudio de caso. Las herramientas utilizadas fueron las entrevistas en profundidad, aplicación de encuestas nacionales, estudio de patentes, observación directa y análisis de resultados de encuestas en la materia de los últimos años, etc.

El presente documento está estructurado en cinco capítulos.

El primer capítulo presenta una revisión de la literatura (Marco conceptual) correspondiente al tema de estudio, donde se definen los conceptos principales que sirven de referencia para subsecuentes capítulos, haciendo énfasis en los siguientes temas: los medios digitales, las trayectorias tecnológicas, las capacidades tecnológicas y la gestión tecnológica en las organizaciones.

En el segundo capítulo se explica la metodología empleada, describiendo las herramientas a través de las cuales se obtuvo la información necesaria, evidenciando así las variables y los indicadores usados en el caso de estudio.

En el tercer capítulo se hace una revisión a nivel global de evidencia empírica sobre el tema específico de seguridad en medios digitales, procurando con ello abarcar 3 puntos: los tipos de ataques computacionales, las tecnologías desarrolladas para evitar los ataques computacionales y un estudio exploratorio de patentes que permita determinar elementos convergentes o divergentes en la intensidad inventiva.

En el cuarto capítulo se presenta la primer parte del caso de estudio, con una breve descripción de la ANUIES, la cual incluye los principales características específicamente en lo referente a la RENASEC, sus características estructurales y los elementos de gestión

tecnológica; se desarrollan asimismo la evolución y trayectorias tecnológicas tanto de las capacidades como de la gestión tecnológica tanto en la RENASEC como en las IES asociadas,

En el quinto capítulo se analiza la información descrita en el capítulo cuarto presentando los elementos de evidencia necesarios para poder determinar los niveles de capacidad tecnológica de la RENASEC y de las IES asociadas, concluyendo con esto cual es el estado actual de los niveles de gestión tecnológica de la RENASEC y si dicho nivel es suficiente para crear seguridad en la información de medios digitales en la relación con las IES.

Finalmente se dan las conclusiones de la presente investigación de tesis.

C
A
P
I
T
I
L
O

1

MARCO TEÓRICO Y CONCEPTOS BÁSICOS

1. Marco Teórico y Conceptos Básicos:

1.1. Introducción

El objetivo del presente capítulo es mostrar los insumos conceptuales que se usaran a lo largo de la tesis, la estructura básica propuesta está conformada de la siguiente manera:

Se empieza hablando de los medios digitales donde se definen 2 posturas que son punto de partida de nuestro estudio: una postura alentadora, que se podría traducir como positiva o sea “libre de inseguridad” y una catastrófica, donde dicha postura será, a la larga, la que nos dicte los elementos de inseguridad.

Posterior a ello, se introducen 2 elementos “fundamentales” en la tesis: la información y el conocimiento, poniendo especial énfasis en la tarea de los medios digitales en estos dos rubros, rematando en este espacio con la relación entre la seguridad y la información.

El siguiente elemento es precisamente el de las capacidades, haciendo una reflexión entre las distintas clases de capacidades y escogiendo a las capacidades tecnológicas como uno de los argumentos principales de la presente tesis.

Sin embargo, el tema de capacidades tecnológicas no es suficiente para poder explicar comportamientos en las trayectorias tecnológicas, por lo que se recurre a la teoría evolucionista para poder manifestar comportamientos y tendencias a través del tiempo.

Como una herramienta para poder determinar trayectorias evolutivas, se usará los estudios de patentes, por lo que el siguiente apartado habla precisamente de ello, discutiendo las ventajas, las desventajas y el uso que se le dará a ésta herramienta en la presente tesis.

Posterior a ello, se habla del tema de gestión, especialmente de gestión tecnológica, del modelo que se va a usar (modelo Cotec de gestión tecnológica) durante la investigación y de las características propias de un sistema de gestión de seguridad.

Como punto final se hablará del tema de convergencia y divergencia tecnológica, su discusión, sus características, sus efectos y del porqué de su gran importancia para la presente investigación.

1.2. Los medios digitales:

Podemos definir al medio digital como todo aquella vía donde pueden transportarse grandes cantidades de información en formatos electrónicos y donde se concentran codificaciones (información codificada) generada en diversos lugares, el ejemplo más evidente lo tenemos actualmente en la Internet, que no es otra cosa que grandes cantidades de información codificada en formato electrónico (En este caso en formato Web).

El medio digital toma importancia en los últimos 10 años ya que es considerado como el principal responsable del crecimiento y desarrollo de lo que conocemos como: “Tecnologías de Información y Comunicaciones” TIC’s mismas que descansan en los elementos tecnológicos y de innovación (Castells, M. 1996-2000), con estructuras complejas entre los que se tienen: capacidades tecnológicas, absorción de las mismas capacidades, procesos de aprendizaje, capacidades organizacionales, entre otros muchos, los cuales tratan de explicar, con diversas visiones y desde perspectivas en ocasiones opuestas, cual ha sido el proceso por el cual se ha llevado a cabo dicho crecimiento y desarrollo.

Existen, en este sentido, dos posturas genéricas:

- Una postura catastrófica que advierten los peligros de “adjudicar” a los medios digitales el título de “los nuevos canales tecnológicos” (Aibar, E. 2001) siendo que, a lo largo del tiempo se han registrado problemas derivados del uso de los mismos
- Una postura alentadora que proyecta a los medios digitales como los caminos naturales de los flujos de información eficiente que puede ayudar a los procesos de crecimiento en distintas áreas del conocimiento. (Castells, M. (1996-2000)

Sea cual fuere la postura es un hecho que, por sus propias características, las TIC’s deben parte importante de su alta dinámica de crecimiento a los flujos de información, y dichos flujos son sin duda piedra angular en los procesos de aprendizaje, las transformaciones tecnológicas, los procesos innovadores, etc. siendo la información, los datos y el conocimiento la materia prima fundamental para dichos procesos. (Sancho, J. M. 1992)

1.2.1. La información en los medios digitales:

En la presente tesis, entenderemos el término “información” como datos organizados en una forma que es útil para las personas que la reciban¹, y los datos como un conjunto de hechos discretos, objetivos, sobre ciertos eventos (Davenport, T.; Prusak, L. 1998), asimismo, el proceso mediante el cual los datos se transforman en información es a través de la agregación de valor², de hecho, las computadoras y cualquier otro medio electrónico de lectura y recepción de datos y agregan valor a los mismos y los transforman en información “digital”, muchas veces en formatos que pueden viajar por algún medio electrónico (también conocido como un proceso de digitalización), lo que hace de ello una ventaja al momento de transportarlos, consultarlos, analizarlos, modificarlos, etc.³

Es en este punto, donde los datos y la información quedan inmersos en un ambiente electrónico, se manifiesta una evidencia (llamado registro) en la cual los datos organizados en forma de información pasan de un estado inicial (físico, escrito, codificado, etc.) a un estado final digital por medio de un proceso de transformación (mediante un escáner, digitalización directa, fotografía, registro, transductores⁴, etc.).

Cabe recordar que la características más importantes de un medio digital, es que transforma a la información a un “paquete digital”, que generalmente toma la forma de un documento⁵.

Dicho documento puede ser visible, audible, tangible (incluso intangible) o virtual, explicando, el medio digital permite a la información en forma de archivo: seleccionar, clasificar, analizar, modificar y exhibir datos que se comunican a través de los medios electrónicos, en diferentes lugares (a través del mundo, de regiones o estados), en diversas presentaciones (imagen, sonido, video, archivo), en distintos dispositivos (como lo puede

¹ Dixon, N (2000) sostiene que la información tiene sentido solamente cuando significa algo o aporta conocimiento para la o las personas que la consultan, lo que en otras palabras es una manifestación de la capacidad de las personas que hacen la consulta de dicha información.

² Dicha agregación va de la mano con la capacidad de las personas para entender los datos, lo que convierte a los datos en información codificada.

³ Debemos tomar en cuenta que los procesos de transformación, transporte, consulta, etc. de datos estaba, antes de la era digital, sujeto a una apreciable cantidad de movimientos y transportes que entorpecían y retrasaban dichos procesos, cosa que al momento de digitalizar han desaparecido casi por completo

⁴ Un transductor es un aparato que convierte alguna manifestación de energía, movimiento o manifestación en un impulso electrónico que puede ser registrado.

⁵ Un documento en un Medio Digital es conocido como un “archivo electrónico” que puede ser de distintos tipos, una imagen, una hoja de cálculo, un documento, una base de datos, una página Web, un archivo multimedia, etc. N del Autor

ser una computadora, un monitor, un celular, un pad, una memory travel), y en diferentes espacios de tiempo (en forma programada o en forma inmediata conocida como “en línea” por ejemplo los chat’s y la Internet).

En otras palabras, la información es la presentación de los datos en formas que pueden ser utilizados por los usuarios desde distintas herramientas y con diferentes intenciones y perspectivas.

Ahora, la información por sí misma no es sino el punto de partida (insumo) de algo más importante en cualquier organización: el conocimiento. La base mediante la cual se puede conseguir una ventaja competitiva de la información es la posibilidad de usarla, procesarla, analizarla, discutirla, modificada, etc. en lo que es llamado un proceso de generación de conocimiento y aprendizaje.

1.2.2. El conocimiento en los medios digitales:

Dixon, N. (2000) define el conocimiento como las relaciones significativas que la gente realiza en su mente entre la información y su aplicación en la acción, con la aportación de un valor agregado, así (Fransman, M. 1994) identifica al conocimiento como la producción de información creíble.

Ambas posiciones nos ayudan a entender que en un medio digital se encuentran naturalmente las vías eficientes de flujos de información que ayudan a generar conocimiento a partir de información creíble.

Esto es sumamente importante, ya que las organizaciones basan sus estructuras productivas, administrativas, operativas, directivas, de acción y de decisión en los conocimientos adquiridos mediante la información creíble, y los medios digitales se han convertido, por sus propias características de transportación, análisis, estructuración, etc; en el medio más usado para fluir, canalizar, depositar y modificar el conocimiento, para así ayudar al proceso de aprendizaje.

Otro aspecto fundamental es entender que los medios digitales son “entes” sumamente dinámicos y evolutivos, así, Castells, M (1999 2a Ed) menciona al menos cinco características fundamentales que los distingue de casi cualquier otro ambiente:

- Facilita el acceso a la información, incluso en esquemas y vías no necesariamente presenciales.
- Es posible la disposición de la información en diferentes plataformas, modelos, estructuras.
- Es posible también la transformación de la información, mediante un sinnúmero de herramientas, dependiendo el tipo de información y el tipo de transformación que se quiera realizar.
- Es inevitable también la posibilidad de la destrucción de la información.

1.3. La seguridad y la información

Tenemos, a lo largo de la presente tesis, dos elementos interrelacionados fundamentales: la seguridad y la información.

Estudios hechos por la FBI y Mancera y Young (CSI/FBI 2003, 2004, 2005 y Mancera Ernst & Young 2002, 2003, 2004 y 2005) evidencian que la información esta sometida a riesgos de una gran variedad y contundencia, que pueden y han afectado de forma crítica a las organizaciones, las universidades, los institutos, las empresas, etc. Esto ha hecho que las organizaciones, instituciones y empresas empiecen a tomar conciencia del valor que tiene la información (y el conocimiento) y se preocupen cada vez más de la protección de la misma.

Algunos modelos empresariales, institucionales y organizacionales, que se han basado en la implantación de sistemas de información, han demostrado tener enormes beneficios para aumentar su nivel de competitividad, lo que ha convertido a la información y al conocimiento en piedra angular y de gran valor para la compañía y por lo tanto, también uno de los más importantes insumos o elementos a atender desde el punto de vista de la seguridad.⁶

Para proteger los sistemas de información, algunas organizaciones afrontaron proyectos de seguridad desde la perspectiva de la protección de elementos aislados en el mismo sistema de información, obviando el concepto de “Administración de los sistemas

⁶ Algunos de los ejemplos más representativos de los modelos económicos aplicados y que representan beneficios tangibles los ponemos encontrar en el libro de Chistopher Price: Los Conquistadores de Internet, batallas de un mundo globalizado

de gestión de seguridad de la información” y centrándose simplemente en el concepto “de seguridad”. Este punto de vista que consideraba “la seguridad” como partes aisladas y no como un todo relacionado, tuvo graves consecuencias para la mayoría de las organizaciones que acogieron este tipo de proyectos, ya que existieron diversas consecuencias⁷, por ejemplo:

- No cumplieron con sus objetivos de seguridad ni de estabilidad en sus sistemas de información
- Se creó un rechazo generalizado hacia los sistemas de seguridad por parte de los empleados, trabajadores y usuarios⁸.

Al no poseer un marco de gestión global de la seguridad que permitiera su estabilidad en el mediano y largo plazo se ocasionaron continuas fugas y pérdidas de información vital para las organizaciones, lo que evitó que éstas pudieran evolucionar de forma acorde al potencial que tenían.

Por otra parte, las organizaciones implantaban controles y programas de seguridad con una visión altamente técnica, considerando que el personal y la dirección debían ser ajenos a estos sistemas de seguridad, con el tiempo se demostró que un sistema de seguridad de la información basado en controles y programas de seguridad con una visión altamente técnica es por sí solo, ineficaz.

Así, Tsujii, S (2004) destaca que, para la construcción de un sistema de seguridad en medios digitales (SIeMD), no bastan los aspectos de transferencia y aplicabilidad tecnológicas, sino que también son necesarios tres aspectos relacionados:

1. La gestión tecnológica (Entendida por Tsujii como los elementos administrativos avanzados⁹)

⁷ Algo muy semejante se observó en los sistemas de calidad (Norma ISO 900:2001) donde los primeros esfuerzos fueron altamente caóticos, desorganizados y sin elementos de gestión adecuada que se manifestaron a la larga con inoperabilidad organizacional y el surgimiento de nuevos problemas operativos, productivos y organizacionales

⁸ De acuerdo con Mancera Ernst & Young 2002 Dichos usuarios terminaron viendo la seguridad de los sistemas de información como un problema que impedía y retrasaba el proceso, progreso y desarrollo evolutivo de la organización, en lugar de tomarlo como un mecanismo que ayudaba a la estabilidad de la misma.

⁹ Veremos posteriormente que un sistema de Gestión no es más que un sistema avanzado administrativo

2. La evolución de las trayectorias (de las cuales las tecnológicas son de nuestro principal interés) asociadas a las organizaciones y cuyo origen puede ser interno y/o externo.
3. Las capacidades propias de las organizaciones involucradas con el sistema de seguridad.

Como núcleo en esta nueva orientación de la seguridad (como un sistema de gestión, de capacidades y evolución de trayectorias), se han creado políticas y herramientas administrativas en materia que contienen el conjunto de reglas y regulaciones que determinan cómo debe protegerse una organización.

Al día de hoy, entre las normas y regulaciones más importantes encontramos:

- Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation)
- NIST (National Institute of Standards and Technology)
- AS/NZS (Australian/New Zealand Standard 4360:2004)
- La norma ISO 17799 y su equivalente británica
- La norma ISO 27000

Pese a lo anterior, no fue sino hasta acontecimientos recientes, derivados de la inseguridad de la información¹⁰, que las organizaciones empezaron a tener una conciencia real y mínima en materia de seguridad, y han asumido la necesidad de la misma, sin embargo, las mismas organizaciones se han encontrado con que no saben cómo salvaguardar sus sistemas de información¹¹.

La mayor parte de las organizaciones (empresas, instituciones, universidades, etc) tienen problemas en sus sistemas de seguridad (CSI/FBI 2003, 2004, 2005 y Mancera Ernst & Young 2002, 2003, 2004 y 2005). El origen de dichos problemas ha sido atribuido, entre muchas otras cosas, a la creación de sistemas de información sin guías adecuadas, sin la existencia de documentación y con recursos de operación insuficientes; así como aplicación de prácticas ineficientes de seguridad de la información (Mancera Ernst & Young 2002, 2003 y 2004).

¹⁰ Como los hechos ocurridos en Estados Unidos el 11 de septiembre de 2001, los atentados informacionales del 2000 y 2004 así como los fraudes multimillonarios del 2004

¹¹ Como veremos en el análisis de evidencia en el capítulo 3 de la presente tesis, es evidente un aumento en la preocupación de las organizaciones, sin embargo en los mismos análisis se han determinado capacidades limitadas y desconocimiento de los elementos mínimos de seguridad y salvaguarda de la información

Por otro lado, las herramientas de seguridad existentes en el mercado (aun las desarrolladas en el esquema de opensource¹²), ayudan a solucionar parte de los problemas de inseguridad computacional, pero solo ocasionalmente dichas herramientas proponen soluciones que inciden de una manera global e integrada a los sistemas informáticos, además, si agregamos el hecho de que las mismas tecnologías de información, como Internet, han puesto a disposición de cualquier persona una enorme diversidad de estas herramientas de seguridad (sin incidencia o capacidad de una aplicación de manera global e integrada a los sistemas informáticos), esto ha provocado a mediano plazo costos enormes en recursos económicos, humanos y estructurales, para poder gestionarlas de una manera adecuada, lo que crea elementos de inseguridad de la información (CSI/FBI 2003, 2004, 2005 y Mancera Ernst & Young 2002, 2003, 2004 y 2005)

Existen teorías (Aibar, E. 2001) donde se asegura que la mayor parte de las consecuencias de la inseguridad en medios digitales no se conocen, ya que la falta de controles adecuados para realizar el seguimiento de la información imposibilita a la organización conocer la existencia de fugas de información, y por lo tanto poder cuantificar el coste y la incidencia de las mismas¹³.

Debido a la inseguridad de la información mostrada, los usuarios de esquemas de seguridad (las instituciones, las escuelas, las universidades, los gobiernos, las empresas, las organizaciones, etc.), demandan actualmente a las empresas que brindan servicios de seguridad informática¹⁴ que sean capaces de garantizar que las tecnologías que usan realmente signifiquen mejoras en los sistemas de seguridad de la información, haciendo con ello que sus activos informáticos (la información y el conocimiento) sean seguros.

Así, para que las organizaciones puedan cumplir sus objetivos de seguridad, los responsables de sistemas de información de las mismas organizaciones se han encontrado

¹² Estas herramientas tienen la característica que pueden ser usadas libremente sin pagar por su uso, lo que en términos computacionales se le conoce como libres.

¹³ De la misma manera, se puede decir que los elementos intangibles de las organizaciones como pueden ser las patentes, los secretos industriales, los elementos de conocimiento tácito interno a la empresa, etc son los elementos más difíciles de poder medir y cuantificar y, en su momento, salvaguardar

¹⁴ Entiéndase una empresa que brinda servicios o insumos en seguridad de información como una organización o empresa con capacidades especiales que la hace proveedora de servicios de salvaguarda, monitorización, vigilancia, codificación, etc de la propia información, algunos ejemplos de éstas empresas son: Panda Antivirus, McAfee, Norton Asociation, SCA protection, etc.

con diversos problemas que, por su propia naturaleza, no tienen una solución única ni satisfactoria, entre ellos tenemos:

- La falta de herramientas accesibles que permitan afrontar la gestión de la seguridad de los sistemas de información de una forma centralizada, sencilla y dimensionada al tamaño de la organización
- La falta de guías de seguridad de la información (o bien el desconocimiento de la existencia de éstas) que respondan a las preguntas de ¿Dónde tengo que buscar? ¿Qué tengo que controlar? ¿Cómo tengo que controlarlo?, etc

1.4. La seguridad de la información

1.4.1. Seguridad y Tipos de ataque

Podemos entender como seguridad a una característica de cualquier sistema (informático o no) que nos indica que está libre de peligro, daño o riesgo, asimismo, se entiende como peligro o daño todo aquello que pueda afectar el funcionamiento directo del sistema o los resultados que se obtienen del mismo. Para la mayoría de los expertos, el concepto de seguridad en la informática es utópico, porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debemos de dotarlo de tres características¹⁵

- Integridad
- Confidencialidad
- Disponibilidad

Términos relacionados con la seguridad informática

- **Activo:** recurso del sistema de información, o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza:** es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto:** consecuencia de la materialización de una amenaza.

¹⁵ http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

- **Riesgo:** posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.
- **Vulnerabilidad:** posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.
- **Ataque:** evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Como se puede observar, un ataque es un evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema. En el mundo existen, cuando menos 3 organismos (RENASEC, CERT EU y CERT UE) que han identificado los tipos de ataque de acuerdo a su riesgo específico:

- **Riesgo tecnológico alto:** es aquel riesgo de origen tecnológico que supone capacidades tecnológicas considerables (tanto que superan las capacidades tecnológicas de las tecnologías de reacción y de prevención descritas anteriormente).
- **Riesgo Económico alto:** es aquel riesgo cuyo origen técnico puede no suponer capacidades tecnológicas considerables, pero cuyo riesgo económico puede ser considerable para la universidad, la empresa, la persona, etc.
- **Riesgo Estructural alto:** es aquel riesgo cuya acción ofensiva está destinada principalmente a la desestabilización estructural más que la económica o la tecnológica.

1.4.2. Tipos de Tecnología

CSI/FBI ha identificado 2 tipos generales de tecnologías en las TIC's y en relación con la SIeMD:

- Las tecnologías de reacción: las cuales esperan a que ocurra un evento de contingencia para así poder responder a el¹⁶.
- Las tecnologías de prevención: son tecnologías que se anticipan a las contingencias.

Estos dos tipos de tecnologías, en términos tecnológicos, son de suma importancia, de acuerdo a Hilbert, M. & Katz J.(2003), una tecnología de reacción supone capacidades tecnológicas y técnicas limitadas para poderse anticipar a las contingencias, por lo que suelen ofrecer “la mejor tecnología posible” (que en términos de capacidades es la tecnología limitada por la capacidad del creador de la misma) incluyendo un módulo que reacciona cuando la tecnología ha sido superada por algún factor de inseguridad¹⁷.

En este esquema explicativo, las tecnologías de prevención suponen tener las capacidades tecnológicas y técnicas necesarias para anticiparse a las contingencias y prevenir, en algunos casos mitigar, las acciones negativas y disminuir así los riesgos derivados.

1.5. Las Capacidades de una organización

1.5.1. Las Capacidades:

La información, el conocimiento y el aprendizaje se vuelven uno de los vehículos principales en la concepción y fortalecimiento de las organizaciones confiriéndoles una dimensión dinámica (Teece, D.J., Pisano, G., Shuen, A. 1997), dando así paso a un nuevo concepto: las capacidades

Podemos definir a las capacidades como aquellas cualidades que hacen distintiva, competitiva, exitosa, eficiente, etc., a alguna organización (Hitt, M., Ireland, D. y

¹⁶ La tecnología de reacción más representativa son los antivirus

¹⁷ Un factor de inseguridad es aquel que puede provocar un peligro o un riesgo a la información en cualquiera de sus presentaciones electrónicas (Imagen, sonido, video, documento, etc)

Hoskisson, R. 1999), sin embargo, dada su importancia y la gran cantidad de generación de conocimiento en la materia, encontramos literatura donde se definen distintos tipos de capacidades, que varían de acuerdo al modelo explicativo, las circunstancias en que se manifiestan, la escuela del conocimiento que da origen a su explicación, ejemplo de ello son:

- Las capacidades centrales (Porter, M. (1996) y Leonard-Barton, D. (1992)¹⁸
- Las capacidades distintivas¹⁹ (Barney, J. 1991)
- Las capacidades tecnológicas (Yoguel y Rabettino, 1999; Motta 1999; Teece y Pisano (1994))
- Las capacidades empresariales (COTEC 2005 a)
- Las capacidades innovadoras (Johannisson y Monsted, 1997) etc.

Todas ellas entendidas y vislumbradas a partir de distintos criterios, y con usos en ocasiones hasta contradictorios; sin embargo, y pese a la importancia de todas ellas, con base en sus características, retomaremos la visión de capacidades tecnológicas descrita por Teece y Pisano (1994) quienes definen a las capacidades en un contexto englobado en 3 partes fundamentales (Figura 1.1):

- 1) La construcción de estas capacidades dependen del contexto en que se desarrollan, lo que les da un carácter de dependencia interna (Endógeno) y externa (Exógeno) respecto a las circunstancias.
- 2) Los senderos y trayectorias de las organizaciones, donde lo imperante es entender que todas las organizaciones son diferentes, y en su diferencia tienen aspectos históricos y evolutivos, de hecho, las circunstancias y los cambios actuales deben ser entendidos y analizados en un contexto evolutivo donde el futuro debe ser función de la evolución del pasado. Aunque este aspecto no signifique necesariamente que las organizaciones

¹⁸ Que le dan estabilidad a la firma y son la columna vertebral de la organización

¹⁹ Que son aquellas que le dan un valor agregado a las organizaciones

estén ancladas a sus decisiones pasadas, éstas trascienden en las decisiones futuras y actuales.

- 3) Aspectos fundamentales estratégicos, donde se ven las capacidades como un resultado de organización y ejecución estratégica.

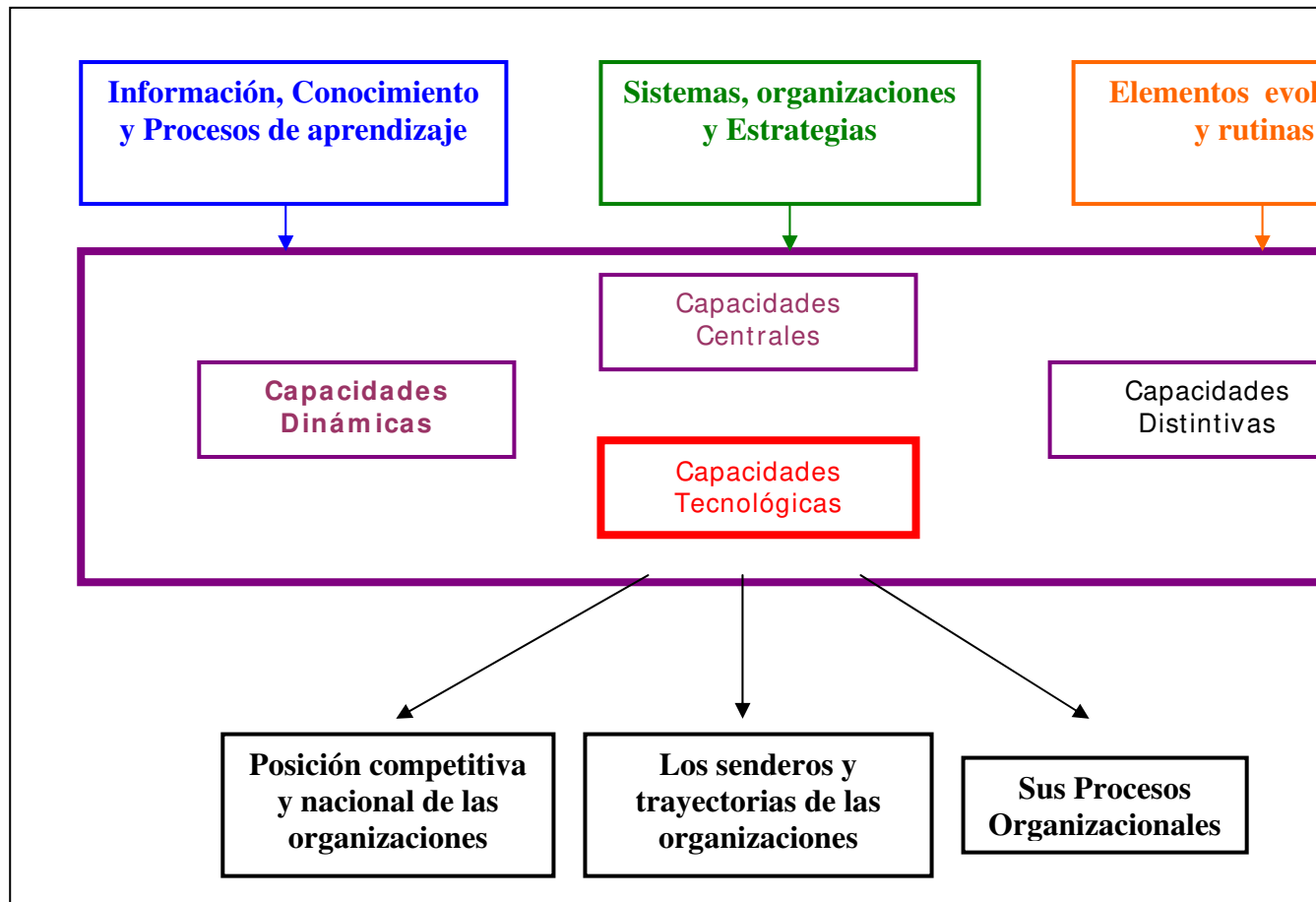


Figura 1.1 Esquema de Capacidades, Realización Propia, Fuente: Teece y Pisano (1994), The dynamic capabilities of firms: an introduction, en Ir

Como se puede observar en la figura 1.1 encontramos 3 elementos fundamentales que fundamentan y dan razón de ser a las capacidades:

- La información, el conocimiento y los procesos de aprendizaje:
 - Que son los activos más importantes en cualquier organización, ya que a partir de ellos se pueden fundamentar elementos complejos de decisión y de comprensión a nivel organizacional.
- Los elementos organizacionales y las estrategias
 - Que pueden resumirse como los objetivos y las formas de conseguir dichos objetivos por parte de las organizaciones y sus estructuras componentes.
- Elementos evolutivos y las rutinas
 - Que no son otra cosa más que las trayectorias y tendencias propias de cada una de las organizaciones.

Por otra parte, se puede asegurar que las capacidades descritas en la figura 1.1 tienen diferencias y coincidencias internas los cuales hacen que sus características internas cambien constantemente, lo que a su vez provoca que los componentes del sistema (subsistemas y organizaciones)²⁰ también cambien y sean diferentes entre sí. Dichas diferencias hacen que el elemento de capacidad sea:

- Diferente de organización a organización (incluso dentro de una misma empresa o corporativo)
- Evolutivo (ya que estamos considerando que siempre existirá la posibilidad de cambios dentro del sistema y de los componentes a través del tiempo.

Autores como Bell y Pavitt (1993), Lall (1995) y Kim (1995) han realizado importantes aportaciones teóricas al respecto, ellos han encontrado que las capacidades tienen su origen en el conocimiento que es creado a través de los procesos de aprendizaje, que a su vez es la consecuencia de la concepción y uso de flujos de información eficientes, esto hace empalmar los elementos de información, aprendizaje y conocimiento, vistos en el

²⁰ Una organización es el conjunto de personas que tienen un objetivo común y un subsistema es la parte fundamental de un sistema que no pierde las características propias del sistema que lo integra y que se compone esencialmente de organizaciones.

primer apartado de la presente tesis, con las capacidades (cambiantes y evolutivas) aquí descritas.

1.5.2. Las capacidades tecnológicas:

Como ya se mencionó, las capacidades que nos interesan en la presente tesis por su utilidad en un esquema de gestión tecnológica son precisamente las capacidades tecnológicas.

Kim (1997) define a las capacidades tecnológicas como “la habilidad para hacer un uso efectivo del conocimiento tecnológico y que le permite asimilar, usar, adaptar y cambiar las tecnologías existentes. Además, facilita la creación de nuevas tecnologías y el desarrollo de nuevos productos y procesos”. Bell y Pavitt (1993) consideran que las capacidades tecnológicas se refieren a “los recursos necesarios para generar y administrar el cambio técnico, incluyendo habilidades, conocimientos, experiencias y vínculos institucionales que poseen las organizaciones”.

De la misma manera, Cimoli, M y Della G. (2003) resaltan elementos de capacidades tecnológicas que otorgan ventajas en sus activos intangibles, esto es, la adquisición de conocimiento tecnológico de una forma tácita y cuya características principales se basan en: ser comerciales, difícilmente imitables y no sustituibles²¹.

En otro sentido, Bell, M (1984), separa a las capacidades tecnológicas en 2 aspectos esenciales:

1. Como procesos de adquisición de habilidades y conocimientos que depende de la experiencia (Learning by doing), todo bajo un proceso de retroalimentación bajo una actividad operativa.
2. Adquisición incremental de habilidades y conocimiento, esto es cuando en una organización es evidente el incremento de sus capacidades para la administración de la tecnología y para la implementación del cambio técnico/tecnológico.

²¹ Algunos ejemplos de lo anterior en las TIC's son: los programas computacionales protegidos por derechos de autor, la infraestructura lógica de los chip's, los modelos computacionales avanzados, etc

En materia de desarrollo organizacional, el crecimiento interno de las organizaciones es en realidad un proceso de exploración de las capacidades tecnológicas existentes y el desarrollo de nuevas capacidades Penrose (1959) y Teece (1980,1982) ; de la misma manera, en la estrategia de las organizaciones, e incorporando una visión dinámica de recursos, la acumulación de capacidades tecnológicas es una tarea importante para construir aceptables teorías descriptivas y normativas de estrategias enfocadas al crecimiento de las organizaciones Teece y Pisano (1994), asimismo, los autores hablan de la competencia de una organización como un conjunto de habilidades diferenciadas, recursos complementarios y rutinas que mantienen la base de las capacidades competitivas y tecnológicas de una organización.

Sin embargo, el concepto que más se acerca a nuestra investigación es el proporcionado por Ariffin y Figueiredo (2001) quienes, tomando como base la definición del Bell y Pavitt (1993) consideran que las capacidades tecnológicas son **“aquellos recursos necesarios para generar y administrar las mejoras en los procesos, la organización, los productos y servicios, el equipo, los proyectos de internos a la organización, etc.”**²² y que además mejoran y ayudan a fomentar los elementos de innovación, la activación productiva, los elementos de calidad, competitividad y rentabilidad desde una perspectiva organizacional (incluso empresarial)”. Dichas capacidades tecnológicas se dan a nivel individual (habilidades, conocimiento y experiencia), a nivel grupal e incluso a nivel de los sistemas organizacionales y de los sistemas directivos dentro de las empresas.”

Esta definición integra los conceptos antes mencionados de Teece y Pisano (1994), Penrose (1959), Bell y Pavitt (1993) y de Kim (1997).

1.6. Corriente evolucionista, trayectorias tecnológicas y patentes

1.6.1. Corriente evolucionista, trayectorias tecnológicas.

Podemos decir que los autores más destacados en materia de “teoría evolucionista y trayectorias tecnológicas” son Nelson y Winter (1977, 1982), Pavitt (1979, 1984), Freeman

²² Lo que poco a poco nos acerca más a un proceso de gestión tecnológica

(1982), Von Hippel (1976, 1988), Dosi (1982, 1988), Rosenberg (1976, 1982), Abernathy y Utterback (1975, 1978), quienes analizan el proceso evolutivo y de trayectoria en diversos entornos, así, explican la evolución de la tecnología a través del tiempo, e introducen varios rasgos y definiciones sumamente importantes para la óptima comprensión del proceso de desarrollo tecnológico y su evolución.

Elementos como: dependencia a la trayectoria, innovación, proceso de aprendizaje y de absorción, derramas tecnológicas, etc, son algunos de los ejemplos más destacados relacionados con las trayectorias tecnológicas y elementos evolutivos.

Las trayectorias tecnológicas configuran y expresan al conjunto de estándares tecnológicos durante un tiempo considerable. En palabras de Dosi “Trayectoria Tecnológica es el progreso tecnológico de las actividades mediante las cuales el comportamiento económico y tecnológico esta definido dentro del paradigma” (Dosi G. y Orsenigo L. 1988). Por otro lado, la evolución de dichas trayectorias explican los cambios, los efectos y los antecedentes del comportamiento de la trayectoria tecnológica; a esto se le llama: la dependencia de la trayectoria (path dependence).

El concepto de "dependencia de la trayectoria", se basa en el supuesto de que el punto donde puede ubicarse un sistema (organización, empresa, firma, corporativo, tecnología, capacidad, etc.) está una función directa, aunque pocas veces proporcional, según Teece (1994), de:

- su posición actual,
- de las trayectorias disponibles pero sobre todo de su trayectoria pasada
- de la propia evolución del mismo sistema.

Esto se traduce en que las condiciones internas y específicas de los sistemas ayudan a explicar, entre otras cosas, por qué los sistemas son diferentes, cómo cambian a lo largo del tiempo y si son capaces de permanecer competitivos. Asimismo, las estructuras formales e informales del sistema tienen una importancia destacada en la dirección de la innovación y en el desarrollo de capacidades tecnológicas y de gestión (Teece 1994).

Así, uniendo los elementos evolucionistas con los de trayectorias tecnológicas, se debe de considerar que, en principio, la trayectoria tiene una posición evolucionista, y que el término “evolución” se puede interpretar como “cambios incrementales” que se producen en los elementos componentes de los sistemas como función del tiempo.

Cabe recordar que la “innovación”, desde la perspectiva de Pérez C.(1982) y Freeman (1988), es producida, ya sea por elementos incrementales o por elementos radicales, existiendo siempre un periodo de tiempo para implementarlos, y por ende también un periodo de tiempo para adaptarse a ellos, lo que obliga a involucrar elementos de adaptación y supervivencia..

Asimismo, para poder tener un fundamento evolutivo debemos agregar varias consideraciones; en principio, los elementos evolutivos deben estar fundamentados en los siguientes aspectos Cimoli, M. y Della Giusta, M. (2003):

- Dinámicos
- Con supuestos fundamentados
- Racionalidad limitada y heterogeneidad entre agentes
- Novedad continua
- Interacciones colectivas como mecanismo de selección y
- La consideración de fenómenos agregados como características inesperadas

de naturaleza no estable

Es importante recordar que los elementos fundamentales en la concepción de una trayectoria tecnológica tienen la facultad de decirnos mucho acerca de las características propias de cada tecnología, esto es, las tendencias y las características de cualquier fenómeno tecnológico dependen de la trayectoria tecnológica de la misma tecnología, así, usando los elementos incrementales descritos por Perez C.(1982) y Freeman (1988), **el análisis de las trayectorias tecnológicas de distintas tecnologías en materia de seguridad (incluso en materia de gestión de la seguridad) puede ser una herramienta importante para determinar las tendencias representativas específicas a la seguridad (por ejemplo del presente caso de estudio), más aún, puede identificar los aspectos fundamentales relacionados a la misma trayectoria y evolución tecnológica.**²³

²³ Este comentario es de suma importancia en la fundamentación de la presente tesis, ya que es el punto de partida “conceptual” para considerar, tanto en el capítulo 3 como en el capítulo 5, elementos evolutivos y de dependencia a la trayectoria (path dependence) que nos ayudan a obtener información fundamental que apoya a la hipótesis de investigación, sin embargo, también este mismo argumento es suficiente para darnos cuenta que, pese al esmero en el trabajo de investigación, es una obligación el cuestionar continuamente nuestros resultados ya que, como se mencionó, estamos hablando de aspectos y elementos dinámicos y las

1.6.2. Estudio de patentes.

Una patente es un documento técnico con una estructura de contenido determinada, en el que se describe la invención que se pretende patentar y en el que se fundamentan las diferencias y mejoras respecto a las patentes que ya existen.²⁴

Por otro lado, debemos considerar que una patente constituye un contrato (social) establecido entre una persona física o moral y el Estado, y que en dicho contrato se establece que el inventor desarrolla un conocimiento materializado en un invento y, a cambio, el Estado le otorga el derecho de explotarlo comercialmente, creando con ello un monopolio.²⁵

Para que un invento pueda ser considerado para ser patentado debe cubrir 4 características esenciales, de acuerdo al Instituto Mexicano de Propiedad Intelectual IMPI:

- Novedad: Se considera nuevo, todo aquello que no se encuentre en el estado de la técnica, es decir, en el conjunto de conocimientos técnicos que se han hecho públicos mediante una descripción oral o escrita, por la explotación o por cualquier otro medio de difusión o información, en el país o en el extranjero.
- Actividad inventiva: Es el proceso creativo cuyos resultados no se deduzcan del estado de la técnica en forma evidente para un técnico en la materia.
- Aplicación industrial: Es la posibilidad de ser producido o utilizado en cualquier rama de la actividad económica.²⁶
- Debe de ser repetible, ya sea a nivel prototipo o a nivel industrial²⁷

A cambio, el Estado otorga 3 facultades a los inventos patentados:

condiciones de hoy pudieran ser diferentes a las de mañana, lo que provocaría asimismo cambios en las conclusiones. Nota del Autor

²⁴ http://innovacion.cicese.mx/pate_que.html

²⁵ <http://innovacion.cicese.mx/pi.html>

²⁶ http://www.impi.gob.mx/impi/docs/patentes/guia_patentes.pdf

²⁷ Esta característica nos fue explicada en una visita realizada en el Instituto Nacional de Propiedad Intelectual y se nos explico que era un elemento agregado a las 3 características y que daban una garantía de duplicación del conocimiento (Nota del autor)

- Exclusividad: de poder dar un uso comercial y exclusivo de la patente
- Temporalidad: gozar de un monopolio en un rango de tiempo
- Territorialidad: gozar de la protección del Estado en exclusividad y temporalidad en un límite de espacio, el cual depende dónde es solicitada y otorgada la patente, ya que ésta puede ser de carácter nacional e internacional.²⁸

Además de lo anterior, diferentes estudios han demostrado que el fortalecimiento y dinámica económica y tecnológica mundial ha sido motivada por el desarrollo, aplicación y difusión de las innovaciones tecnológicas (Romer, P. (1990), Kaldor y Mirrlees (1962), Solow (1957)), y que sin duda, la generación de innovaciones depende directamente, entre otras cosas, de las patentes.

Entonces, si la generación de innovaciones y tecnología son el motor del desarrollo y dinámica económica de los países, podemos asegurar que su estudio puede determinar, entre otras muchas cosas, la actividad inventiva de un fenómeno, área, sector económico, elemento específico, el fortalecimiento tecnológico de un país, la capacidad de desarrollo tecnológico de alguna región, etc.

Las preguntas lógicas podrían ser:

¿Cuáles son los indicadores, técnicas y/o metodologías adecuados para un adecuado estudio de patentes?, dicha pregunta se complementa haciendo una segunda pregunta ¿Qué es lo que buscamos realmente en el estudio de patentes en la presente tesis?

Resolviendo la segunda pregunta, lo que se busca es, esencialmente, observar la evolución de la trayectoria tecnológica de la seguridad de la información en medios digitales (SIeMD) respecto con las TIC's; esto es, se quiere ver si el comportamiento inventivo de las TIC's es semejante al comportamiento inventivo de los SIeMD, lo que, en principio podríamos considerar lógico ya que ambos conceptos están íntimamente relacionados.

²⁸ http://www.impi.gob.mx/impi/docs/patentes/guia_patentes.pdf

Ahora, resolviendo la primer pregunta, Spinak, E. (1996) define la existencia de diversas herramientas de indicación derivados de un estudio de patentes, en particular la intensidad inventiva, que no es otra cosa más que el porcentaje de desarrollo de patentes de un tema, área, sección, etc. que es específica y de interés para el estudio.²⁹

1.6.2.1. Desventajas del uso de patentes para un estudio de caso.

Se debe estar conciente que al hacer uso de patentes para realizar cualquier tipo de estudio tiene sus ventajas y desventajas, entre las cuales se pueden mencionar, de acuerdo a Archibugi y Pianta (1996), Pavitt, K; Patel, P. (1988) y Spinak, E. (1998). que:

- no todos los países dan la misma importancia al sistema de las patentes.
- existen evidentes diferencias entre países, relacionadas con los costes-beneficios de las patentes
- existen diferencias entre las tecnologías y sectores en la importancia de las patentes como sistema de protección
- existen diferencias evidentes entre las empresas respecto a la propensión a patentar especialmente en innovaciones novedosas que pueden ser protegidas bajo diferentes denominaciones
- no todas las patentes se convierten en innovaciones.
- no todas las leyes permiten que todas las innovaciones se puedan patentar.
- no todas las innovaciones de las empresas son patentadas, lo cual se muestra en que las diferentes industrias tienen diferentes propensiones hacia el patentamiento de innovaciones.
- existe un valor heterogéneo de las innovaciones individuales.
- es difícil evaluar la significatividad y representabilidad de cualquier muestra que se realice en las patentes

Sin embargo, Rodrigues, H (2001), asegura al respecto que un estudio de patentes se vuelve más significativo si, dentro de la metodología de investigación, se pueden realizar 2 acciones concretas:

²⁹ En nuestro caso la convergencia y/o divergencia de los inventos relacionados con la SIeMD con el desarrollo de las TIC's.

- cuidar que la muestra representativa sea numerosa, ya que mientras mayor número de patentes exista, mayor significatividad y representatividad tendrá dicho estudio
- si se cuenta con un número muy alto de patentes, tratar de hacer un ejercicio de clasificación para poder tener un estudio más consistente y mejor delimitado.

1.6.2.2. Convergencia, divergencia y patentes

Los estudios hechos por Castells (1998), la CEPAL (2003) y, anteriormente, Westphal, L. Kim y Dahlman, C (1985) muestran una tendencia a considerar que una de las fortalezas de las TIC's (tanto a nivel teórico como práctico) es la convergencia de sus componentes, esto es, las TIC's son un conjunto de diversas disciplinas que llegan, bajo una estructura dinámica, de innovación y tecnológica; a puntos de coincidencia, que son la base del desarrollo positivo de las TIC's

Sin embargo, resultados teóricos y empíricos Aibar, E. (2001), Macau, R (2004) y, más actualmente Lira A. (2005), revelan la posibilidad de que:

- No existe tal “convergencia” o “asociación” entre todos los componentes de las TIC's
- Sus elementos de convergencia son mucho más puntuales (solamente una parte del total) de lo que se presume.³⁰; esto es, que la “convergencia” de las componentes de las TIC's no es homogénea en todos los casos, sino que existen evidencias que podrían suponer elementos incluso divergentes o de desfase tecnológicos entre las tecnologías integrantes de las TIC's

Esta posibilidad, (que a mi juicio podría ser un hallazgo que puede dar nuevos componentes fundamentales a la investigación de tesis) nos hace proponer un estudio que nos pueda determinar si realmente existe dicha divergencia, en particular entre las TIC's y los Sistemas de seguridad de la información en medios digitales.

³⁰ Quiero hacer énfasis en un detalle, inicialmente el tema de tesis se centraba precisamente en determinar la no homogeneidad o no convergencia entre las TIC's y los SIeMD, en un fenómeno que en el último año se ha definido como la “divergencia tecnológica de las TIC's”, sin embargo algunas circunstancias generadas internamente en la RENASEC de la ANUIES me orillaron a cambiar el tema de tesis y hacer del tratamiento de este tema (divergencia tecnológica de las TIC's) solo un subtema importante para la presente investigación.

Una herramienta que se puede usar para poder determinar si una tecnología tiene un comportamiento convergente o divergente es precisamente la intensidad inventiva Spinak, E. (1996),³¹.

1.6.2.3. Estudio de patentes “palabras claves”

Castells (1998), Mancera Ernst & Young (2002, 2003, 2004 2005 y 2006), y varios autores más han evidenciado la existencia de “palabras claves” en temas de Tecnologías de Información, dichas “palabras” son consideradas por los autores como representativas de un tema en específico, en particular, del tema de las Tecnologías de Información y Comunicaciones.

Sin embargo, dichas palabras tienen algunas características que deben siempre tomarse en cuenta si es que son usadas en algún tipo de estudio:

- Cambian con respecto al lugar
- Dependen siempre de la perspectiva de quien las propone
- Son dinámicas
- Siempre existe la posibilidad de la aparición de nuevas “palabras clave” y la desaparición de palabras obsoletas con respecto al tiempo.

En materia de TIC´s Castells (1998), Topscot (2000), Macau, R (2004), la CEPAL (2003) entre otros, consideran las siguientes palabras como claves: “system”, “software”, “hardware”, “computer”, “computing”, “Internet”, “information”.

Dichas palabras son útiles en un estudio exploratorio de patentes, ya que se han desarrollado herramientas específicas informacionales de búsqueda de patentes que evidencian el uso e importancia de las palabras clave encontradas, una de dichas herramientas se llama “Matheo Patent”, la cual será explicada un poco más adelante.

³¹ A partir de este momento se definirá como intensidad inventiva a La relación cuantitativa entre las patentes específicas de un subcampo tecnológico y las patentes del campo tecnológico al que pertenecen.

1.6.2.4. Estudio de patentes “clases de patentes”

Una forma de poder realizar verificaciones de los experimentos y análisis realizados es precisamente repitiendo el experimento con algunas variantes, este es el caso.

Dadas las características de los estudios de patentes, se hace obligatorio hacer algún tipo de validación de resultados.

Existe una diferencia significativa entre una consideración de “palabras clave” con respecto a “clases de patentes”, ya que la primera es el resultado de consideraciones derivadas de la experiencia, y la otra es una forma de orden y clasificación.

Para entender el término de “clases de patentes”, se debe primero entender que las patentes están alojadas, en realidad, en un sistema de ordenamiento.

Dicho orden clasifica a las patentes en sectores técnicos previamente determinados; en particular la Clasificación Internacional de Patentes (CIP) divide el “saber técnico” o “patentes” en 8 secciones, 20 subsecciones, 118 clases, 624 subclases y más de 70.000 grupos y subgrupos, identificados por símbolos de clasificación.³²

Las ocho secciones generales son:

- a) Necesidades corrientes de la vida.
- b) Técnicas industriales diversas; transportes.
- c) Química, metalurgia.
- d) Textiles; papel.
- e) Construcciones fijas.
- f) Mecánica, iluminación, calefacción, armamento, voladura.
- g) Física.
- h) Electricidad.

Y las clases y subclases son elementos integrados en las ocho secciones generales descritas.

La forma de aplicar dicho estudio será semejante a lo que se realice con el estudio de “palabras clave”, esto es, haciendo uso de la herramienta computacional llamada Matheo Patent que será descrita posteriormente.

³² <http://www.wipo.int/classifications/ipc/es/>

1.7. La gestión tecnológica en las organizaciones:

1.7.1. Gestión

La palabra “gestión” encierra por si misma varios significados, dependiendo el uso específico al que se intente asociar; por ejemplo, para Faga, R (2000) es fundamental el aspecto administrativo en la gestión, desde una perspectiva sistémica donde cada uno de los departamentos interacciona entre sí y donde la gestión se encarga de la asignación eficiente de recurso para poder conseguir los objetivos de la organización. Para Davenport (1996), quien también define “gestión” como un proceso sistémico organizacional, es un proceso en el cual se busca, filtra, organiza y presenta la información (y el conocimiento) con el objetivo de mejorar los elementos humanos y las áreas de trabajo; en cambio, Malhotra, Y (1997) hace énfasis en la gestión vista como una combinación de sinergias entre los datos, la información, los sistemas y subsistemas integrantes, todo ello en busca de un equilibrio entre la organización y los activos existentes.

Sin embargo, el impacto que ha causado en las organizaciones la teoría del conocimiento ha cambiado un poco la perspectiva de “la gestión”, orillándola más al manejo y uso de elementos de flujos informativos, toma de decisiones y alta administración y calidad. Esto ha dado paso a definiciones de gestión como la propuesta por Nonaka y Takeuchi (1995) quienes resaltan el elemento de gestión como una capacidad (apartado 1.5.1) de la empresa para poder obtener, usar y generar conocimiento, incorporando dicho conocimiento a los productos, servicios y en general al sistema productivo o de servicios de la organización. En esta definición se ve implicado un elemento sistémico integrador complejo en el que se abarcan actividades clásicas, como lo son los elementos productivos, de servicio y administrativos que tiene toda organización, y elementos emergentes, como lo son: la creación y/o absorción del conocimiento, los elementos estructurales y obviamente los elementos estratégicos; sin olvidar que se parte de objetivos eminentemente organizacionales que se basan en la misión, visión y objetivos propios de la organización y/o sistema.

Dado lo anterior, el elemento de gestión que interesa a la presente tesis, más allá de la gestión del conocimiento, es la gestión tecnológica, la cual abarca:

- A la gestión clásica vista desde la perspectiva sistémica, los elementos administrativos y los elementos de producción o de servicio según sea el caso.
- A la gestión del conocimiento que conlleva a las consideraciones del manejo y flujo del conocimiento
- A los elementos estratégicos enfocados a características tecnológicas de la organización, como lo es la SIeMD.

1.7.2. Gestión tecnológica

Podemos encontrar en la literatura, diversas posiciones acerca de que es y como se maneja y estructura la gestión tecnológica dentro de las organizaciones.

Lo cierto es que, dentro de todas las posiciones, existen elementos de coincidencia importantes que deben ser tomados en cuenta. Por ejemplo, la fundación española COTEC (1999) considera que la gestión tecnológica es más que la administración de la información, más bien es el conocimiento organizado en diversas estructuras llamadas multisistemas cuyas actividades son enfocadas hacia las de sistema determinado; en otras palabras, es un sistema de conocimientos y prácticas, cuya relación con los procesos de innovación, desarrollo, transferencia tecnológica y uso de la tecnología son sumamente importantes.

Kanz y Lam (1996) agregan que la gestión tecnológica es una colección de procesos y metodologías sistematizadas que ayudan a la organización de procesos en la aplicación y creación de conocimientos, extendiendo así el rango específico de las actividades humanas para la óptima producción de bienes y servicios.

Asimismo, la gestión tecnológica se ve como una integración de “ingeniería, ciencias y disciplinas de gestión organizacional y económica” para planear, desarrollar e implementar capacidades tecnológicas, en vías de alcanzar los objetivos estratégicos de la organización. Khalil (1998), procurando con ello un proceso de homogenización y convergencia entre los elementos involucrados en la gestión tecnológica.

Existen en el mundo algunos modelos de gestión tecnológica, incluso México posee un modelo propuesto por el comité técnico del Premio Nacional de Tecnología³³, sin

³³ <http://www.pnt.org.mx/pdf/modelo2005.pdf>

embargo, dicha propuesta es limitada con respecto a otros modelos desarrollados en el mundo.

Uno de los modelos que más se aproxima a las definiciones de gestión mostradas por Faga, R (2000), Davenport (1996), Malhotra, Y (1997); pero sobre al concepto de gestión tecnológica descrito por Nonaka y Takeuchi (1995) y Kanz y Lam (1996), es el desarrollado y propuesto por la Fundación para la Innovación Tecnológica de España COTEC (2005 b), COTEC (2005 a) y COTEC (1999)

El modelo propuesto contempla 5 puntos mínimos necesarios (más nunca suficientes) para una eficiente gestión tecnológica y de innovación; son los siguientes COTEC (1999):

1.7.2.1.Vigilar y analizar:

El cual se refiere a la atención y análisis del entorno en busca de señales sobre la necesidad de innovar, en el caso de innovación, y de organizar y administrar, en el caso de gestión, en busca de oportunidades potenciales que puedan aparecer y ser utilizadas por las empresas o las instituciones que así lo necesiten. COTEC (2001)

El objeto de este apartado es el de preparar a la organización para afrontar los cambios que le puedan afectar en un futuro más o menos próximo y conseguir así su adaptación, ya sea en esquemas relativamente sencillos y personales así como esquemas más complejos que son conocidos como Sistemas Complejos Adaptables³⁴.

1.7.2.2.Focalizar:

Focalizar es poner especial atención y esfuerzo en alguna estrategia concreta para la mejora de la organización que se esté tratando (Industria, institución educativa, negocio, etc) esto con la intención de dar una solución específica a un problema.

De acuerdo a la fundación COTEC (1999), es necesaria aplicar de manera continua el proceso de focalización, ya que hasta las organizaciones mejor dotadas de recursos no pueden plantearse abarcar todas las oportunidades de innovación, crecimiento y gestión que

³⁴ Un sistema Complejo Adaptable es aquel en donde los elementos que lo integran poseen una interrelación dinámica cuya principal característica es la tendencia al equilibrio a través del tiempo, además de poder tener cambios naturales enfocados a un proceso de adaptación a las condiciones, internas y externas, que los caracteriza.

ofrece el entorno, y debe seleccionar aquellas que en mayor medida puedan contribuir al mantenimiento y mejora de su competitividad en el mercado.

1.7.2.3.Capacitar

Esta claro que, en un entorno de gestión tecnológica, y en búsqueda de un aumento en las capacidades de la organización involucrada, la estrategia principal elegida debe dedicar los recursos necesarios para un plan de capacitación oportuna, visionaria y constante.

La fundación COTEC y diversos esquemas de capacitación de la ONU (2004) demuestran que ésta, la capacitación, puede implicar desde la compra directa de una tecnología, la explotación de los resultados de una investigación existente, o bien la transferencia de conocimiento mediante esquemas de aprendizaje colectivo, de persona a persona o incluso por medio de algún tipo de tecnología de la información, cuyo análisis en el estudio de esta tesis es esencial.

Un enfoque adecuado para el uso y generación de nuevo conocimiento puede realizarse básicamente de tres formas COTEC (1999):

1. Generandola internamente mediante la realización de investigación y desarrollo.
2. Transfiriéndola en un esquema comercial
3. Transfiriéndola en un esquema de acuerdo y cooperación.

1.7.2.3.1. Generación interna de conocimiento mediante la realización de investigación y desarrollo.

La generación interna de conocimiento mediante investigación y desarrollo es una práctica que se ha vuelto común de una manera comercial, pero poco eficiente de una manera académica, esto es, evidentemente existe la generación de conocimiento en las universidades en materia de seguridad de la información en ambientes digitales, pero casi toda esta generación de conocimientos es experimental, y por el grado crítico de la información manejada en ambientes reales, existe un gran riesgo en el manejo de este tipo de información.

1.7.2.3.2. Transferencia en un esquema comercial

Este tipo de adquisición de capacidad es el más común de todos, la transferencia y absorción tecnológica viene dándose de manera natural al momento de “comprar” tecnología de seguridad, sin embargo esto ha creado un gran debate.³⁵

1.7.2.4. Implantar

La implantación es la aplicación directa de los elementos diseñados y concebidos dentro de la gestión, partiendo de la idea y siguiendo las distintas fases de su desarrollo hasta su lanzamiento final, ya sea de nuevos productos y servicios en el caso de innovación hasta elementos de desarrollos específicos como es el caso de gestión tecnológica.

1.7.2.5. Aprender

Sin lugar a duda y como ya se explicó, los procesos de aprendizaje son vitales para la gestión tecnológica, ya que sin ellos los elementos de información no tendrían sentido.

Los elementos que específicamente son esenciales en este rubro son los elementos codificados y los elementos tácitos de la información (llamada en cualquier organización “experiencia”), lo que supone fomentar la creación de análisis y reflexión (en un sentido evolutivo y de trayectoria tecnológica como se hace en esta tesis) y la revisión de la experiencias tanto de éxito como de fracaso, para así lograr un proceso de aprendizaje.

Otra fuente de aprendizaje es en sí la tecnología, donde los procesos de absorción del mismo conocimiento tecnológico, son fundamentales para la comprensión del proceso de aprendizaje en la organización. Un óptimo control de los elementos que ayudan al aprendizaje individual y colectivo de la organización ayudan, sin duda, a marcar directrices específicas en materia de gestión tecnológica.

³⁵ Al ser la seguridad un elemento crítico respecto a la información y al conocimiento en los medios digitales usados en las empresas e instituciones, se crea incertidumbre cuando el esquema de generación de conocimiento relacionado es, en su mayoría, de origen comercial.

La interacción de los 5 puntos anteriores nos da como resultado los elementos claves para una eficiente gestión de la tecnología, que puede ser representado gráficamente de la siguiente manera:

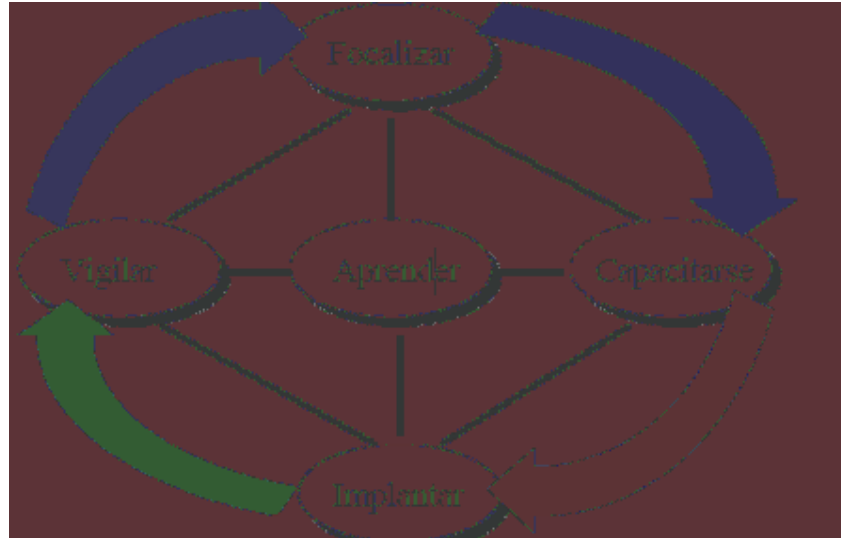


Figura 1.2 Elementos claves para la Gestión de tecnología Fuente Cotec (1999)

Del esquema de la figura 1.2, y de acuerdo con COTEC (1999), la dinámica a la que pueda moverse este ciclo determina la posibilidad de que organización tiene para poder hacer cambios estratégicos, y con ello, mejorar las condiciones específicas en sus metas, objetivos y planteamientos; tanto a nivel general como a nivel operativo, a nivel interno como a nivel de relación con el exterior.

Las fallas en la ejecución y aplicación de este esquema, o irregularidades con los elementos en los flujos de información, derivaran sin duda en pérdidas en la capacidad de desarrollo, control, administración y, sobre todo, deficiencias en la gestión tecnológica específica que se esté realizando.

1.8. Divergencia y convergencia tecnológica en las TIC's

Como ya se mencionó anteriormente, estudios hechos por Castells (1998), la CEPAL (2003) y, anteriormente, Westphal, L. Kim y Dahlman, C (1985); muestran una tendencia a considerar que una de las fortalezas de las TIC's es la convergencia de sus componentes, esto es, las TIC's son un conjunto de diversas disciplinas que llegan, bajo una estructura dinámica de innovación y tecnología a puntos de coincidencia, que son la base del desarrollo positivo de las TIC's, a eso se le ha llamado convergencias tecnológicas.

Hilbert M, Kats J. (2003) las ha llamado: “la convergencia de las TIC's”, dicho concepto está integrado por 3 grandes bloques: informática, información y comunicaciones.³⁶

A partir del estudio de Katz y Hiberth se han demostrado las ventajas de dichas convergencias cuando son integrados a diversos factores productivos y de alta tecnología, siendo: las telecomunicaciones, la Internet y los sistemas de información, las tecnologías y factores productivos más evidentemente beneficiados.

Sin embargo, resultados teóricos y empíricos descritos por Aibar, E. (2001), Macau, R (2004) y más actualmente Lira A. (2005); revelan la posibilidad de la no existencia de dicha “convergencia” o “asociación” entre todos los componentes de las TIC's.³⁷, esto es, que la “convergencia” de las componentes de las TIC's puede o no existir, o tener características de crecimiento no homogéneo en todos los casos.

Lo anterior nos hace suponer que existen evidencias suficientes que podrían suponer elementos divergentes o de desfaseamientos tecnológicos entre las tecnologías integrantes de las TIC's

Complementando lo anterior, Lira A (2005) y Arango, J (2003) mencionan que las TIC's, al tener una alta dinámica inventiva en su conjunto, crea inestabilidades en algunos

³⁶ Vale la pena hacer notar, que coincidentemente los tres grandes bloques que describe Hilberth y Kats son tres de las “palabras claves” descritas en el apartado anterior

³⁷ Quiero hacer énfasis en un detalle, inicialmente el tema de tesis se centraba precisamente en determinar la no homogeneidad o no convergencia entre las TIC's y los SIeMD, en un fenómeno que en el último año se ha definido como la “divergencia tecnológica de las TIC's”, sin embargo algunas circunstancias generadas internamente en la RENASEC de la ANUIES me orillaron a cambiar el tema de tesis y hacer del tratamiento de este tema (divergencia tecnológica de las TIC's) sólo un subtema importante para la presente investigación de tesis.

de los factores relacionados con esta, dichas inestabilidades son manifestadas, entre algunas otras cosas, por problemas legales, estructurales, culturales, educacionales, regionales, etc., donde todos estos elementos no han conseguido seguir la dinámica tecnológica de las TIC's y, en consecuencia, se han hecho evidentes diversas dificultades en los últimos años..

Tanto las divergencias como convergencias tecnológicas deben constituir un aspecto fundamental en el entendimiento de los sistemas de gestión de seguridad en medios digitales, por lo que tendrán, en la investigación de la presente tesis, un apartado especial.

1.9. Los sistemas de gestión de seguridad de la información

Un sistema de gestión tecnológica de seguridad de la información (SGSI) se puede definir como un sistema de gestión usado para establecer y mantener un entorno seguro de amenazas y riesgos a la información³⁸.

Este SGSI debe tratar la puesta en práctica y el mantenimiento de procesos y de procedimientos para manejar la seguridad de la información³⁹, estas acciones incluyen la identificación de las necesidades de la seguridad de la información, así como la puesta en práctica de las estrategias para satisfacer estas necesidades, medir los resultados y mejorar las estrategias de protección.⁴⁰

Este entorno seguro debería considerar un conjunto de elementos que, de manera integrada, participarían en el sistema de gestión de seguridad de la información. Los estándares pueden incluir aspectos técnicos como seguridad de redes, firma digital, control de acceso, gestión de claves, etc. Los procedimientos fundamentales para poder garantizar una mínima seguridad incluyen elementos operacionales, técnicos, operativos y de gestión.

Sin embargo, hemos considerado en la presente tesis cuando menos 5 enfoques diferentes de cómo llevar a cabo una adecuada gestión tecnológica de seguridad de la información, los cuales son:

- Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation).
 - a. Para una mayor información de este sistema se puede consultar:

<http://www.cert.org/octave/>

³⁸ Definición acuñada en el 6º congreso internacional de seguridad de la información, UNAM 2005

³⁹ Octave, <http://www.cert.org/octave/>

⁴⁰ <http://www.cert.org/>

- NIST (National Institute of Standards and Technology)
 - a. Para una mayor información de este sistema se puede consultar:
<http://www.nist.gov/>
- AS/NZS (Australian/New Zealand Standard 4360:2004)
- La norma ISO 17799 y su equivalente británica
 - a. Para una mayor información de este sistema se puede consultar:
<http://www.iso-17799.com/>
- La norma ISO 27000 e ISO 27001
 - a. Para una mayor información de este sistema se puede consultar:
<http://www.iso27000.es/>

Además de éstos, existen cuando menos otros 10 esquemas de seguridad de la información que son operables a través del mundo en diferentes circunstancias y con diversas intensidades de acuerdo al tiempo y a las necesidades específicas.

Es sorprendente la cantidad de coincidencias entre ellos aunque tienen un enfoque específico, su principal desventaja es que ciertamente guardan en su naturaleza elementos genéricos y poco tangibles, lo que significa que en esencia dependen para su éxito de la capacidad de las personas que salvaguardan la información en las diferentes organizaciones, lo que hace que la herramienta se vuelva poco verificable..

Sin embargo, todas las normas mencionadas, pese a resaltar el elemento de conocimiento para su operación y sustentabilidad, no poseen elementos específicos enfocados a la gestión tecnológica desde la perspectiva de la innovación.

Este hecho es un nicho de oportunidad, ya que se puede partir de éste supuesto para poder determinar nuevas variables y hacer hallazgos importantes en la materia. Este es en si el objetivo principal de la presente investigación

1.10. Herramienta de medición de capacidades y gestión tecnológica.

En el presente capítulo se han descrito los elementos fundamentales de las capacidades tecnológicas y la gestión tecnológica, sin embargo, la herramienta más importante que se usó a lo largo de la presente tesis tiene como base una matriz cruzada donde se involucran a los elementos mencionados.

En ella se hizo una adecuación del modelo propuesto por Bell y Pavitt (1995) y del modelo propuesto por Lall. S (1996), contrastando el nivel de capacidades tecnológicas propuesto por Lall y el nivel de gestión tecnológica de SIeMD propuesto por Bell y Pavitt a través del tiempo.

Para poder cuantificar las capacidades tecnológicas, Lall. S (1996) y Bell y Pavitt (1995) las define como un conjunto de habilidades para realizar determinadas cosas. Así, el origen de las capacidades tecnológicas tiene como piedra fundamental el conocimiento que es creado a través de los procesos de aprendizaje.

De acuerdo a lo anterior, podemos adaptar el enfoque de capacidades de Lall y definir 3 elementos específicos:

Capacidades tecnológicas básicas: Como aquellas capacidades que permiten a alguna organización seguir operando, en otras palabras, son aquellas características mínimas necesarias para que se pueda dar seguimiento ya sea a una idea, un proceso productivo, un servicio, etc.

Capacidades tecnológicas intermedias: Son aquellas capacidades que van más allá de la operación, de hecho, involucran en esencia actividades complementarias que agregan valor al producto, servicio o proyecto resultante. Algunos de los ejemplos de estas capacidades van enfocados a elementos de calidad (sistemas de calidad), sistemas avanzados de control y organización productiva o de servicio (ERP's, CRM's, SAP, RPM, etc), elementos de adaptabilidad corporativa, transferencia tecnológica, alto grado de capacitación y aplicación de conocimiento, etc

Capacidades tecnológicas avanzadas: Son aquellas capacidades que, además de las características de las capacidades anteriores, generan conocimiento a partir de sus procesos de aprendizaje o bien de la aplicación directa de herramientas de trabajo, lo que supone una manera ordenada de generación e incluso de

generación/aplicación de conocimiento, hecho que les da una ventaja competitiva con respecto a las demás capacidades.⁴¹

Una forma de medir dichas capacidades es mediante la aplicación de un cuestionario/encuesta, que pueda evidenciar las características de cada una de dichas capacidades y los resultados de las mismas.

Asimismo, para cuantificar el aspecto de gestión tecnológica, Kanz y Lam (1996) enfocan el concepto de gestión tecnológica como una colección sistémica de procesos y metodologías que ayudan a la organización de procesos en la aplicación y creación de conocimientos, logrando una óptima, eficaz y eficiente producción de bienes y servicios, con una integración de elementos de “ingeniería, ciencias y disciplinas de gestión organizacional y económica” para planear, desarrollar e implementar estrategias en vías de alcanzar los objetivos de la organización.

Esto no lleva a que, a diferencia de los elementos de capacidad, para cuantificar los componentes de la gestión tecnológica se deben considerar elementos de interrelación, asociación y vinculación, en una idea de uso de redes de conocimiento; enfocados éstos tanto a la generación de conocimiento como a la administración del mismo, su aplicación y el control de sus resultados.

Como puede verse, son muchas las variables relacionadas y, asimismo, muchos los factores que intervienen para poder dar una cifra específica en términos de gestión.

De la misma forma que con las capacidades, se hace una adecuación del modelo propuesto por Bell y Pavitt (1995) y del modelo propuesto por Lall. S (1996) para así cuantificar:

La gestión de seguridad con capacidad de operación: Variables relacionadas con la administración y control de las actividades enfocadas a la operación; en otras palabras, son características mínimas necesarias para administrar, controlar y modificar elementos enfocados con la operación del aparato productivo, de servicio o estratégico.

⁴¹ Es de suponer que estas capacidades no se dan de manera espontánea, sino que surgen, crecen y evolucionan a partir de controles y planes de trabajo bien establecidos.

La gestión de seguridad con capacidad de administración: A diferencia de los elementos de gestión de seguridad con capacidad operativa, en la capacidad de administración se vislumbran elementos exógenos a la organización que se está estudiando, esto es, incorporando elementos del mercado, de los clientes y de la competencia, así como de proveedores.

La gestión de seguridad con capacidad de invención: Este es quizás el elemento de cuantificación más complicado, ya que, además de las características anteriores, se debe tener la capacidad de gestionar cambios tecnológicos que ayuden a la creación de innovaciones dentro de la organización; hecho que provoca tener cuidado con elementos evolutivos y de trayectoria en cada uno de los sistemas, ya que, como se ha mencionado anteriormente, este aspecto cambia con respecto al tiempo, tanto en características como en condiciones específicas.

1.11. Hallazgos y conclusión de capítulo

Éste primer capítulo de la tesis ha provisto los insumos conceptuales necesarios para conseguir los objetivos trazados tanto de la investigación como de la tesis misma.

En particular, los insumos conceptuales presentados que son base de la investigación son:

- La teoría de los medios digitales así como su influencia respecto a la información, los procesos de aprendizaje, el conocimiento y la seguridad de la información.
- La teoría de las capacidades, en particular eligiendo a las capacidades tecnológicas como las más importantes para nuestro estudio, así como su relación específica con la evolución de dichas capacidades y las trayectorias tecnológicas, específicamente en el rubro de seguridad de la información en medios digitales
- Teoría relacionada con las patentes, ya que se usó el estudio de patentes como una herramienta para determinar intensidad inventiva.
- Teoría relacionada con la gestión y la gestión tecnológica, específicamente la propuesta desarrollada por la fundación Cotec

- Teoría relacionada con la discusión entre las convergencias y las divergencias tecnológicas en materia de SIeMD
- Herramientas de medición e indicadores relacionados con las capacidades y la gestión tecnológica.

C

A

P

I

T

I

L

O

2

METODOLOGÍA

2. Metodología

2.1. Introducción

El objetivo del presente capítulo es el de mostrar la metodología de investigación usada en la presente tesis

La estructura básica del capítulo se compone de una entrada donde se discute la teoría que fundamenta a un caso de estudio, y tres partes o etapas de las cuales se conforma la metodología.

En la etapa preliminar se discute, básicamente los elementos que conforman una introducción a una investigación, esto es, desde determinar las fuentes de información, los tipos de información, discusión de teorías relacionadas, escenarios, etc. hasta llegar a dos elementos: un plan de trabajo y el protocolo de investigación, donde el resultado del mismo será precisamente lo relacionado con la problemática, la pregunta de investigación, la hipótesis, etc.

En la primera etapa se podrá encontrar la metodología para determinar lo relacionado con el capítulo 3, o sea, la evidencia empírica, para ello se detalla las herramientas usadas, en este caso: Análisis de tipos de tecnología de ataque, Análisis de Tecnologías de uso.

La presente etapa culmina con la metodología de uso de la herramienta llamada “estudio de patentes”.

En la segunda etapa se detalla la metodología de investigación que dará sustento al capítulo 4 y 5 de la presente tesis, y donde se empieza con la metodología de recogida de datos para los antecedentes y la organización en particular de la RENASEC de la ANUIES, asimismo se destaca la metodología usada tanto para las entrevistas personalizadas como de la encuesta nacional realizada en el 2006, finalizando con el análisis de los datos y la presentación de los mismos.

2.2. El Estudio de caso:

De acuerdo con Ghauri, P., Gronhaug, K. y Kristianslund, I. (1995), un “estudio de caso” es en realidad una investigación que sirve para analizar elementos fundamentales del objeto de estudio, por ejemplo: el contexto y los procesos implicados; por lo que puede considerarse como un estudio intensivo de ejemplos seleccionados, donde los hechos son dependientes del contexto. En este sentido, Yin (1994) expone que un estudio de caso enfocado a una investigación adopta, en general, una perspectiva que integra distintos elementos de acuerdo a cómo se vayan necesitando en la propia investigación de campo, textualmente Yin dice:

“... una investigación empírica (o estudio de caso) estudia un fenómeno contemporáneo dentro de su contexto de la vida real, especialmente cuando los límites entre el fenómeno y su contexto no son claramente evidentes. De hecho, una investigación de estudio de caso trata exitosamente con una situación técnicamente distintiva en la cuál hay muchas más variables de interés que datos que pudiesen ser observados; y, como resultado, se basa en múltiples fuentes de evidencia, con datos que deben converger para que los resultados de la investigación puedan tener sentido” Yin (1994).

. Yin (1994). hace algunas comparaciones de distintas estrategias de investigación para determinar distintos tipos de utilización de la metodología del caso, asimismo, describe las diferencias y utilidad de los siguientes estrategias:

- La encuesta
- La historia
- El análisis de archivos
- El estudio de encuestas.

Determinando con ello cuál de estas estrategias es adecuada para distintos casos específicos de investigación de campo, exponiendo para ello la siguiente gráfica:

Método:	Forma de la pregunta de investigación	¿Requiere control sobre los acontecimientos?	¿Se concentran en acontecimientos contemporáneos?
Experimento	¿Cómo? ¿Por qué?	SI	SI
Encuesta	¿Quién? ¿Qué? ¿Dónde? ¿Cuándo? ¿Cuántos?	No	SI
Análisis de archivos	¿Quién? ¿Qué? ¿Dónde? ¿Cuándo? ¿Cuántos?	No	SI/No
Historia	¿Cómo? ¿Por qué?	No	No
Estudio de casos	¿Cómo? ¿Por qué?	No	SI

Figura 2.1 Matriz para la elección de un método de investigación social según las características del objeto de estudio y el problema de interés. Fuente Yin (1994)

Como se puede observar, tanto el análisis de archivos (como lo puede ser un estudio de patentes), como en la encuesta, se debe tener cuidado de poder responder a las preguntas ¿Quién?, ¿Qué?, ¿Dónde?, ¿Cuándo? y ¿Cuántos?, lo que a la larga nos obliga a tener un método específico de análisis

Al respecto, se puede asegurar una evidente utilidad, en el estudio de caso, al contestar a las preguntas ¿Cómo? y ¿Por qué? ya que generalmente una investigación social tiene dos características específicas:

- Poco control sobre acontecimientos
- Tratar un tema de actualidad, en otras palabras, que se trabaje en un objeto de estudio de un tema contemporáneo¹.

La pregunta ¿Qué? Es, en forma general, exploratoria o descriptiva y se responde haciendo un análisis de encuestas o de bases de datos (como lo es, por ejemplo, el estudio de patentes que se realizó en la presente tesis)

Sin embargo lo que da sentido a buena parte de nuestra investigación son las preguntas: ¿Cómo? y ¿Por qué?, ya que son más explicativas y llevan de una manera natural a las estrategias de investigación del estudio de caso, de la historia y los experimentos.

¹ Podríamos decir al respecto que, en el objeto de estudio en particular (Las Tecnología de información y comunicaicones TIC's y los SIeMD) se tiene realmente muy poco control sobre los acontecimientos, así como la garantía de tratarse de un tema contemporáneo en su forma específica

Complementando lo anterior, y para ser precisos, la presente investigación puede ser descrita como un estudio de caso, donde los contenidos de la misma serán presentados en 3 etapas específicas:

- i) Una etapa preliminar: Cuyo objetivo específico se centra en presentar los elementos fundamentales de la investigación, mediante una revisión bibliográfica especializada en SIeMD, definir el protocolo de investigación, armar un plan de trabajo y revisar los antecedentes propios del objeto de estudio (Capítulo 1 y 2).
- ii) Una etapa de análisis de datos preliminares (Capítulo 3) donde el principal objetivo es el de exponer los resultados de las diversas revisiones de encuestas y del estudio de patentes.
- iii) La etapa empírica (Capítulo 4 y 5): donde el objetivo se centra en obtener, analizar, discutir y llegar a las conclusiones referentes a los datos obtenidos del estudio de campo, dando prioridad a los resultados del análisis del objeto de estudio, el análisis de las entrevistas personalizadas y el análisis de la encuesta nacional.

Así, se pueden observar en la figura 2.2 las acciones (rutinas) metodológicas que se usaron en la presente investigación.

Etapa Preliminar

- Revisión de bibliografía especializada en el tema de seguridad de la información en medios digitales
- Revisión de los antecedentes en materia del objeto de estudio
- Definición del protocolo de investigación (Pregunta, Hipótesis, Objetivo, etc.)
- Representación del plan de trabajo

Etapa 1 (Capítulo 3)

- Evidencia empírica sobre seguridad de la información en medios digitales
 - Revisión de encuestas (Mancera y Young 2002, 2003, 2004, 2005 y 2006)
 - Determinación de Tipos de Tecnología usada en los ataques a la seguridad de la información en medios digitales
 - Determinación de riesgo por tipo de tecnología
 - Determinación del número de incidentes totales
 - Revisión de encuestas (CSI/FBI)
 - Determinación de uso de las tecnologías de seguridad de la información en medios digitales
 - Análisis de pendientes
 - Estudio de Patentes.
 - Estudio de patentes “Palabras Clave”
 - Tendencia de la intensidad inventiva² “Por Palabras Clave”
 - Estudio de patentes “Clases de patentes”
 - Uso del Matheo Patent³
 - Tendencia de intensidad inventiva “Por Clases de Patentes”

Etapa 2 (Capítulo 4 y 5)

- Análisis de la RENASEC de la ANUIES.
 - Antecedentes y organización
 - Entrevistas personalizadas
 - Evolución de las capacidades tecnológicas
 - Entrevistas personalizadas y aplicación de encuesta nacional
 - La gestión tecnológica de la RENASEC/ANUIES
 - Análisis
 - Cuadro de comparación de evolución de capacidades tecnológicas y nivel de gestión de seguridad

Figura 2.2 Esquematización de las rutinas usada en la presente tesis, Realización propia.

2.3. Etapa Preliminar:

El objetivo de esta etapa es determinar cuál es el estado del arte y su relación con los elementos fundamentales para la investigación, esto, con base en la profundización de

² Spinak, E. (1996), define la intensidad inventiva, como el aumento o disminución del porcentaje de desarrollo de inventos (patentes) de un tema, área, sección, etc. con respecto al total.

³ Matheo Patent es una herramienta informática que facilita la tarea del análisis de patentes, su explicación mas detallada la podemos encontrar en los anexos.

los temas asociados con la seguridad de la información en medios digitales. Asimismo, brindar los elementos tecnológicos necesarios para la comprensión en un marco conceptual.

Con esta información y con el bagaje obtenido en la maestría, se tienen los argumentos necesarios para poder definir y realizar el protocolo de investigación y, con ello, la pregunta de investigación, la hipótesis, el objetivo, definir claramente cuál es la problemática, etc., elementos que fueron desglosados en la introducción de la presente tesis así como en el Capítulo 1.

2.3.1. Fuentes de Información:

Para llevar a cabo las rutinas propuesta en la figura 2.2, tanto en su etapa preliminar como en todo el estudio de caso, las principales fuentes de información son:

- 12 encuestas relacionadas con los SIeMD, cuyas fechas van de 1999 a 2005. y cuyo origen son Estados Unidos, Japón, América Latina, España, Argentina, Colombia y México (anexo A).
- Un cuestionario personalizado que se aplicará al menos a los responsables de los centros de cómputo y responsables administrativos de al menos las 25 IES más participativas en la RENASEC desde hace 7 años.
- Una encuesta elaborada por la ANUIES y aplicada a dos entes específicos: las universidades afiliadas a la ANUIES y las empresas productivas inscritas en el programa “Seguridad Informática” impulsado por la RENASEC, perteneciente a la ANUIES.
- La información derivada del Banco de Información Electrónica de la United State Patent and Trademark Office (USPTO) de Estados Unidos y la Oficina Europea de Patentes (OEP) por medio de la herramienta electrónica ESPANET
- Las memorias de algunos de los congresos en “Seguridad Informática” de entre los años 2004 y 2006.
- Además se usarán otras fuentes: material bibliográfico, información disponible en medios electrónicos, bases de datos y observaciones directas.

2.3.2. Encuestas y bibliografía especializada:

En una etapa preliminar, se dio prioridad a la obtención de información que pudiera ser útil para un planteamiento adecuado de tesis. La siguiente es una lista de encuestas y material relacionado usado para tal propósito, el cuál fue revisado y analizado para determinar su importancia y las aportaciones que pudiera tener para la realización de la tesis y en particular para el planteamiento del protocolo de investigación.

A pesar a que se uso principalmente 2 encuestas a lo largo del trabajo de investigación: CSI/FBI (2002, 2003, 2004, 2005 y 2006) y Mancera, Ernest y Young(2002, 2003, 2004, 2005 y 2006), a lo largo del mismo se mencionan algunos datos relacionados con la lectura, análisis y datos trascendentes de otros materiales, que por su naturaleza, nos ayudó a reafirmar evidencia de algún elemento específico.

Además de la bibliografía descrita anteriormente, se participó en diversos eventos relacionados con la seguridad de la información en medios digitales, entre los cuales, los más importantes fueron:

- “El congreso de seguridad en cómputo” en sus versiones 2003, 2004, 2005 y 2006 (Organizado por la UNAM)⁴.
- “Magno congreso internacional de computación CIC-IPN” en sus versiones 2004, 2005⁵
- “Encuentro iberoamericano de protección de datos personales IFAI” En sus versiones III y IV⁶

2.4. Etapa 1:

El objetivo principal de esta etapa ha sido evidenciar elementos fundamentales que son preliminares a un análisis de la gestión tecnológica en SIeMD.

Dicha evidencia está sustentada en 3 apartados (que son base del capítulo 3 de la presente tesis), y cuyos fundamentos metodológicos necesarios se pueden resumir como:

⁴ Mayor información en: www.congreso.seguridad.unam.mx/

⁵ Mayor información en www.magno-congreso.cic.ipn.mx/esp.html

⁶ Mayor información en http://www.ifai.org.mx/eventos/2005/enc_Ibero/programa.htm

1. Evidencia empírica recabada esencialmente en las encuestas globales sobre seguridad en cómputo Mancera, Ernest y Young(2002, 2003, 2004, 2005 y 2006), y cuyo objetivo particular fue evidenciar los tipos de tecnología usadas en los ataques de seguridad con una perspectiva evolutiva y de trayectoria tecnológica; midiendo asimismo el riesgo asociado de dicha evolución y mostrando los elementos incidentales de tales acciones, también en un entorno evolucionista (todo ello explicado a detalle más adelante), lo que en la figura 2.2 se marca como:

- i. **Tipos de Tecnología usada en los ataques a la seguridad de la información en medios digitales**

- ii. **Riesgo por tipo de tecnología**

- iii. **Número de incidentes totales**

2. Contraste de los resultados obtenidos en el primer apartado con la encuesta realizada por la CSI/FBI, donde el objetivo específico será el resaltar cuales son las tecnologías de SIeMD usadas para salvaguardar la información en un enfoque evolutivo y de trayectoria tecnológica en lo que denominamos “Análisis de pendientes”, lo que en la figura 2.2 se marca como:

- i. **Uso de las Tecnologías de seguridad de la información en medios digitales**

- ii. **Análisis de pendientes**

3. Un estudio exploratorio de patentes aplicando la técnica de “palabras clave” y de “clases de patente”, cuyo objetivo principal será el determinar y medir la existencia de elementos convergentes ó divergentes en la medición de “actividad inventiva” dentro de las patentes (resultado trascendente en materia de gestión tecnológica), lo que en la figura 2.2 se marca como:

- i. **Estudio de patentes “Palabras Clave”**

1. **Tendencia de intensidad inventiva “Por palabras Clave”**

- ii. **Estudio de patentes “Clases de patentes”**

1. **Uso del Matheo Patent**

2. Tendencia de intensidad inventiva “Por clases de patentes”

2.4.1. Evidencia empírica recabada esencialmente en las encuestas globales sobre seguridad en cómputo (Mancera y Young)

La evidencia empírica recabada principalmente en las encuestas de Mancera y Young nos dan una fuente de información que cubre con dos características fundamentales:

- Es de carácter global (involucra cuando menos datos de 42 países diferentes)
- Posee datos históricos, consistentes y adecuados para poder determinar “evoluciones” tecnológicas, esto es, a partir de estos datos se puede dar seguimiento específico de la evolución tecnológica de los sistemas de seguridad de la información en medios digitales.

2.4.1.1. Tipos de ataques a la seguridad de la información en medios digitales

El tratamiento de los datos se basan en graficar e interpretar, en forma porcentual, cuáles son los tipos de tecnología usadas en los ataques que reciben los centros de cómputo, para ello, la metodología usada por Mancera y Young, menciona que en la encuesta específica y se numeraron un total de 50 tipos distintos de ataque, de los cuales los encuestados (que varía de acuerdo con el año) han señalado el porcentaje de aparición del tipo específico de ataque siendo el 100% un tipo de ataque que siempre ha estado presente, y 0% un tipo de ataque que nunca estuvo presente durante el año (Como se muestra en la figura 2.3).

Los datos específicos que necesitamos son:

1. ¿Cuáles son los tipos de ataque más comunes?
2. ¿Cuál es su comportamiento evolutivo?, para así poder determinar elementos específicos de capacidades, como fue descrito en el primer capítulo.

La figura 2.3 será el modelo para la construcción de la gráfica denominada “tipos de ataque”, la cuál servirá para poder determinar los comportamientos y tendencias, a través del tiempo, de los tipos de ataque más frecuentes en los centros de cómputo.

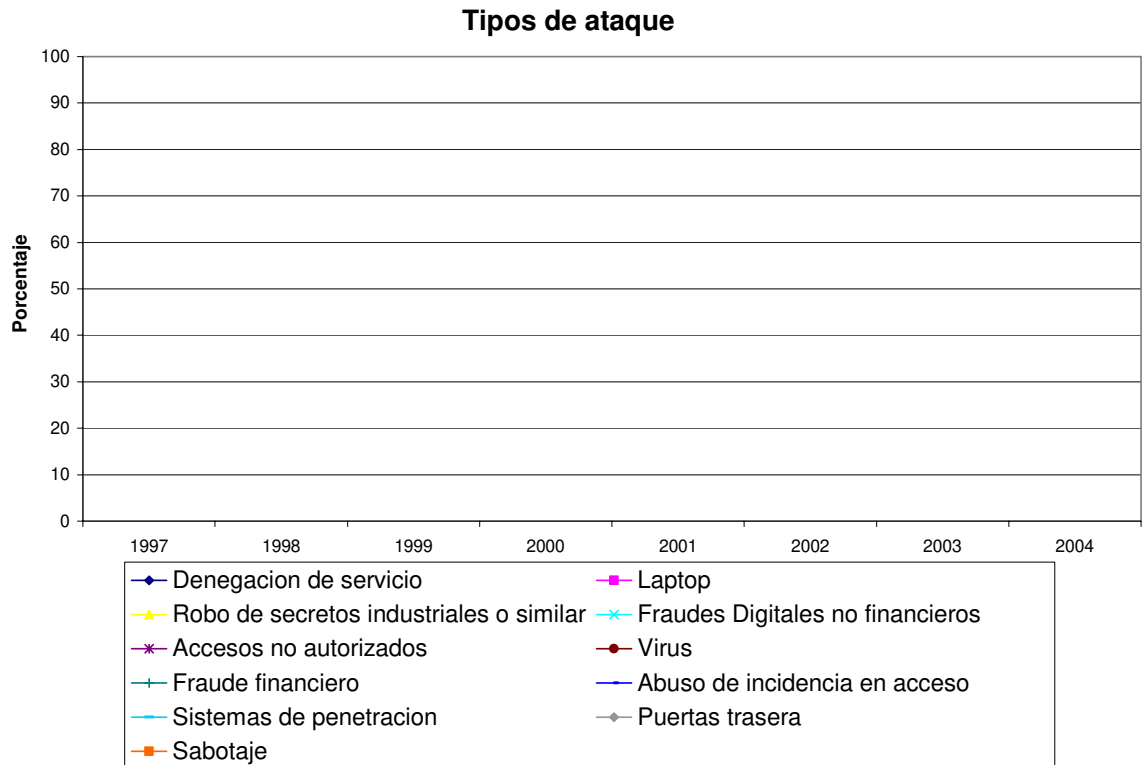


Figura 2.3 Gráfica propuesta para el tratamiento de datos de “Tipos de Tecnología usada en los ataques a la seguridad de la información en medios digitales”, Realización propia. Fuente de datos a interpretar: Mancera Ernest Young (1997 – 2004) “Encuesta Global de seguridad informática”

2.4.1.2. Riesgo por Tipos de Tecnología

Después de analizar los tipos de ataque más comunes y su evolución a través del tiempo (llenado de la figura 2.3 en el capítulo 3), el siguiente paso será examinar el riesgo que existe por tipo de tecnología.

Una tabla, como la mostrada en la tabla 3.1, donde se observa el riesgo por tipo de tecnología, fue usada en el 2002 en la CSI/FBI (Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”), y de manera consistente, en sus reportes de seguridad en los años subsecuentes hasta el 2005.

La razón por la cuál la CSI/FBI dejó de usar ésta herramienta fue por el desarrollo de instrumentos más complejos en sus metodologías, sin embargo, para los propósitos del trabajo de investigación, este esbozo es suficiente para poder observar cómo se comporta el riesgo informático de acuerdo al tipo de tecnología a través del tiempo.

Tipo de Tecnología	Riesgo tecnológico alto	Riesgo Económico alto	Riesgo Estructural alto	Pendiente a través del tiempo Positiva + Negativa -

Tabla 2.1 Interpretación de la Evolución de los tipos de ataque. Fuente: CSI/FBI (2002, 2003 y 2004) Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey.

2.4.1.3. Porcentaje de incidentes totales

La Figura 2.4 no es otra cosa más que un esquema para la clasificación del número de incidentes totales, en forma de frecuencia porcentual.

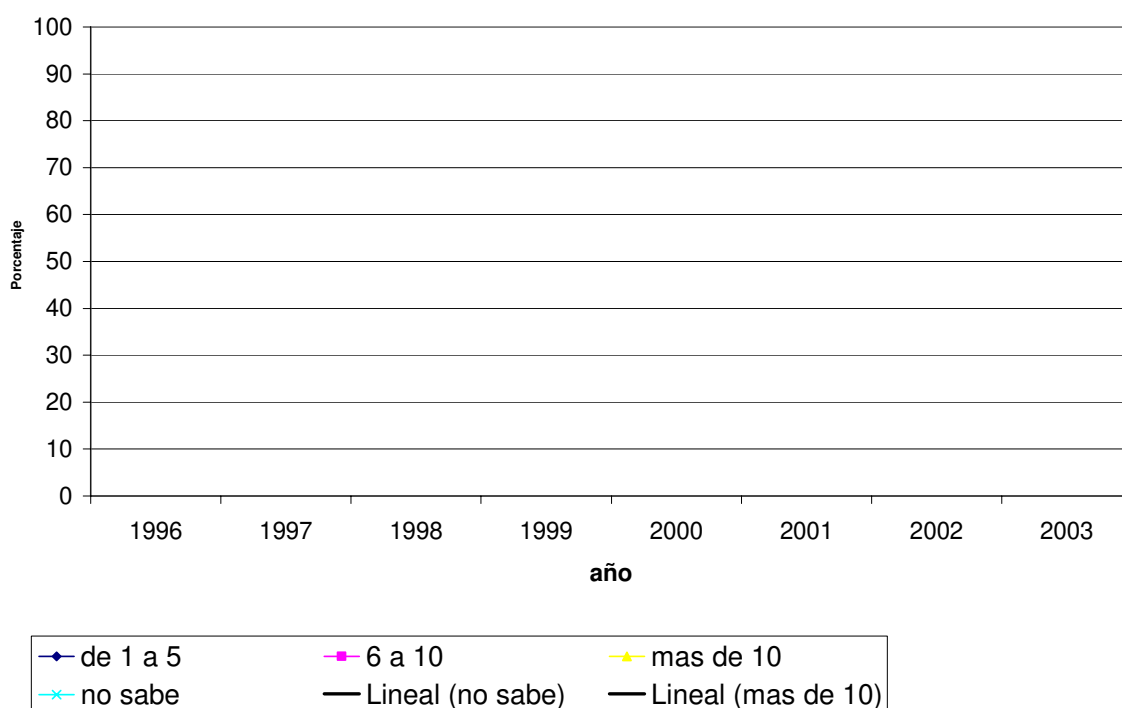


Figura 2.4 Gráfica propuesta para el tratamiento de datos de "Clasificación por número de incidentes totales", Realización propia.

Fuente de datos a interpretar: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática

Para obtener la información de la figura 2.4 se les preguntó a las IES: ¿Cuál es la cantidad de ataques en seguridad de la información promedio mensual recibida el presente año?, las opciones de respuesta eran:

1. de 1 a 5
2. de 6 a 10
3. más de 10
4. no sabe.

Con esta información se llena la figura 2.4, para ser usada en un análisis posterior.

2.4.1.4. Uso de las Tecnologías de seguridad de la información en medios digitales

En la figura 2.5 se observa el modelo de gráfica propuesto para describir la evolución en el uso de tecnologías en materia de SIeMD.

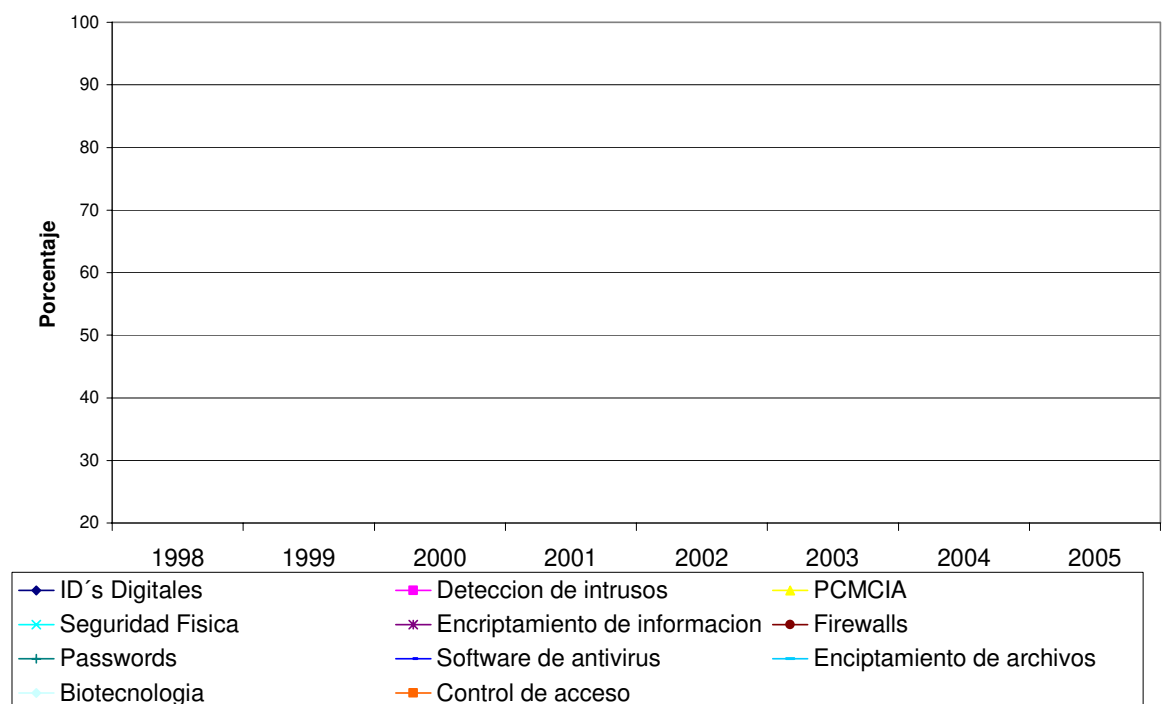


Figura 2.5 Modelo de Gráfica propuesta para medir la Evolución de las tecnologías usada en materia de seguridad por año, Realización propia.

Fuente: CSI/FBI (2002, 2003, 2004, 2005 y 2006), Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Para obtener la información de la figura 2.5, la pregunta concreta es: ¿En que porcentaje se usan las distintas tecnologías enfocadas a la seguridad de la información en medios digitales?. Las opciones de respuesta ascendieron a 50 diferentes opciones, de los cuales los mostrados en la figura 2.5 han sido las más representativos en el rango de tiempo de 1998 a 2005.

2.4.1.5. Análisis de pendientes

Posterior al llenado de la figura 2.5, se revisará la tendencia de las pendientes de cada una de las tecnologías, de las cuales hay esencialmente 2 posibilidades, que sea negativa (como ya se ha discutido, lo que significará la existencia de un menor uso de la tecnología específica), positiva (lo que significará la existencia de un mayor uso de la tecnología específica) a través del tiempo.

Esencialmente, lo que se busca con el ejercicio es determinar cómo se comportan los dos tipos de tecnologías (prevención y reacción) con respecto al tiempo, para así sacar conclusiones respecto a elementos de capacidad tecnológica

Tipo de Tecnología	Pendiente Positiva	Pendiente Negativa
Reacción		
Prevención		

Tabla 2.2 Tabla resultante para el análisis de pendientes, Realización Propia.

2.4.2. Estudio de Patentes

El objetivo de realizar un estudio de patentes será, a partir de las características descritas en el marco teórico, evidenciar la existencia de elementos convergentes ó divergentes entre las TIC's y los SIeMD.

La razón por la cuál este elemento tiene una importancia significativa para la tesis es porque el resultado puede cambiar la apreciación que se tiene en términos de la gestión tecnológica en seguridad de la información en medios digitales, esto es, de encontrarse

“divergencias” o “no convergencias”⁷ en el estudio de patentes propuesto, podemos entonces suponer que, en general, existe un desfase o no convergencia tecnológica de los elementos de seguridad en las TIC’s **que provoca inseguridad desde la misma concepción del invento enfocado a las TIC’s.**

Antes de seguir, se hace necesario definir claramente lo que se entiende por intensidad inventiva ya que este término será usado a lo largo de la tesis de manera continua. **Intensidad inventiva:** para las necesidades de la presente tesis, se define como la relación cuantitativa entre las patentes específicas de un subcampo tecnológico y las patentes del campo tecnológico al que pertenecen⁸.

Para conseguir el objetivo específico planteado, se hacen 2 estudios de patentes, un estudio de “palabras claves” y otro de “clases de patentes”

2.4.2.1. Estudio de patentes. “Palabras Claves”

Como ya se mencionó, el objetivo del presente estudio es el determinar la intensidad inventiva de las patentes de seguridad de la información dentro de las TIC’s, en este caso, en las patentes cuya característica común sea la asociación con una “palabra clave”

Las palabras claves que se usaran son: “system”, “software”, “hardware”, “computer”, “computing”, “Internet”, “information”.

Usando la herramienta Matheo Patent, se llena una gráfica como la mostrada en la figura 2.6

⁷ Lo que en otras palabras significa tener distintas intensidades inventiva a través del tiempo entre las TIC’s y los SIeMD

⁸ Dicha definición fue otorgada por el Dr. Manuel Soria en una de las asesorías de Tesis y fue acuñada a partir de dos conceptos: el primero de la misma definición de intensidad como el cociente de dos cantidades relacionadas y cuya característica es que una de ellas es subconjunto total de la otra, y la segunda de la definición de invento y su relación directa con las patentes.

Gráfica de Intensidad inventiva

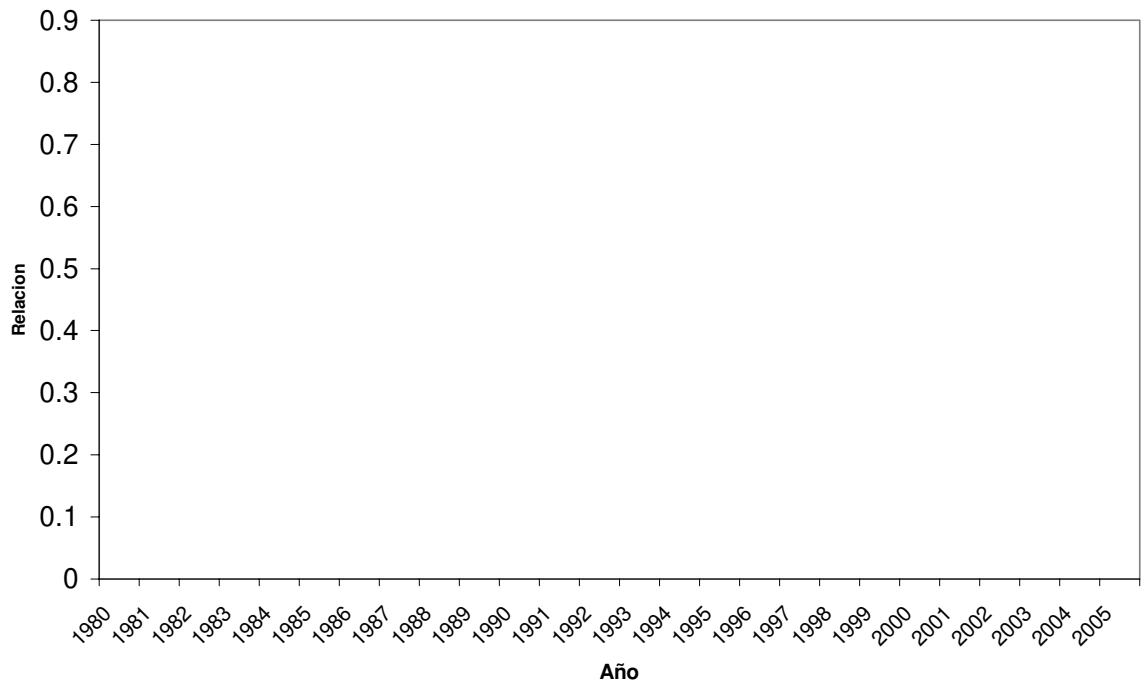


Figura 2.6 Modelo de Gráfica de “Intensidad Inventiva” a través del tiempo

Para determinar la “intensidad inventiva” a través del tiempo (Figura 2.6), en el eje de las abscisas se representa el tiempo y en el eje de las ordenadas se representa la relación cuantitativa entre las patentes específicas de un subcampo tecnológico (en nuestro caso la SIeMD y la palabra clave) y las patentes del campo tecnológico al que pertenecen (en nuestro caso las TIC’s)

Asimismo, para dar una mayor certidumbre de este resultado, y usando el beneficio del programa llamado Matheo Patent, se realizó el mismo ejercicio en las patentes otorgadas de dos bases de datos:

- La oficina de patentes de Estados Unidos (USPTO)
- La oficina de patentes de la Unión Europea (UEP),

El análisis preliminar realizado por el programa “Matheo Patent” puede ser consultado en el anexo B de la presente tesis.

2.4.2.2. Estudio de patentes. “Clases de patentes”

Para tener certidumbre en los resultados que se obtienen del apartado anterior (2.4.2.1), se realizó un segundo estudio de patentes con una metodología un poco distinta al anterior, esto, para poder validar los resultados e interpretaciones obtenidas en el estudio de patentes por “palabras claves” (ejercicio 2.4.2.1).

La diferencia entre ambas es el uso de “clases de patentes” en vez de usar “palabras clave”. Para ello se hace uso de las “clases de patentes” más comunes en elementos de seguridad de la información en medios digitales, éstas son:

- G06F: TRATAMIENTO DE DATOS DIGITALES ELÉCTRICOS
- H04: TÉCNICA DE LAS COMUNICACIONES ELÉCTRICAS
- G11: REGISTRO DE LA INFORMACIÓN
- H04K: COMUNICACIONES SECRETAS; PERTURBACIÓN DE LAS COMUNICACIONES

Al igual que en el estudio anterior, se requiere del uso de la herramienta informacional “Matheo Patent” para obtener los datos y elaborar una gráfica equivalente a la mostrada en la figura 2.6

De la misma manera, se debe determinar la “intensidad inventiva” a través del tiempo (Figura 2.6). En el eje de las abscisas se representa el tiempo y en el eje de las ordenadas se representa la relación cuantitativa entre las patentes específicas de un subcampo tecnológico (en nuestro caso la SIeMD y las clases tecnológicas) y las patentes del campo tecnológico al que pertenecen (en nuestro caso las TIC’s)

Cabe señalar que las dos oficinas de patentes en las que se centra nuestro interés son:

- La oficina de patentes de Estados Unidos (USPTO)
- La oficina de patentes de la Unión Europea (UEP),

2.5. Etapa 2:

El objetivo de esta etapa será la de evidenciar los elementos significativos en materia de Gestión Tecnológica y capacidades tecnológicas en un entorno de Trayectorias Tecnológicas y elementos Evolutivos de los dos objetos de estudio: La Red Nacional de Seguridad en Cómputo RENASEC perteneciente a la Asociación Nacional de Universidades e Instituciones de Educación Superior ANUIES y las Instituciones de Educación Superior IES adscritas a la ANUIES y que participan activamente en la RENASEC

En esta fase de la investigación se priorizan algunos elementos: la obtención de información para los antecedentes de la organización, las entrevistas personalizadas a las IES asociadas a la ANUIES, la aplicación de la Encuesta Nacional, y el Análisis de los datos obtenidos.

2.5.1. Antecedentes y Organización:

Para la obtención de información en este apartado, existen diversas fuentes de información:

- Los anuarios de la ANUIES desde 1998 al 2005
- Contacto directo con miembros activos tanto de la ANUIES como de la RENASEC
- Apuntes Técnicos en las diversas áreas de la ANUIES
- Los estatutos y la biblioteca de interna de la ANUIES

Con la información disponible, es relativamente sencillo obtener la información tanto de los mecanismos de acción de la ANUIES tanto como de la RENASEC, sus antecedentes históricos y muchos elementos evolutivos que son desglosados, analizados y concluidos en el capítulo 4

2.5.2. Entrevistas Personalizadas:

La aplicación del cuestionario/entrevista, dará elementos importantes de la gestión tecnológica que son tomados en cuenta en las IES entrevistadas

La realización y aplicación de una encuesta exploratoria es un esfuerzo, en esta segunda etapa, por homologar y reafirmar criterios descritos en las acciones anteriores, con ello se dará una certeza formal a los datos y encuestas.

2.5.2.1. Características del Cuestionario aplicado en las Entrevistas personalizadas:

Metodología del cuestionario:

El cuestionario fue diseñado por tres instituciones:

- La RENASEC de la ANUIES.
- El centro de inteligencia de la Universidad de Guadalajara.
- El centro de respuesta tecnológica de la Universidad Nacional Autónoma de México.

El objetivo principal del cuestionario es tener un esquema piloto de comportamiento organizacional y de aplicación de gestión tecnológica en las IES que más hayan participado con la RENASEC en los últimos 4 años, las razones principales para incluir a estas instituciones son:

- Su compromiso mostrado con los objetivos de la RENASEC
- Su rápida Respuesta
- Tienen al menos 2 años continuos de aplicación de programas de crecimientos y capacitación sugerida por la RENASEC desde hace 4 años

Los tópicos más importantes abordados en el cuestionario son:

- Seguridad: En referencia específicamente a la existencia o no de normas, programas específicos, capacitación, estructura organizacional, elementos técnicos/tecnológicos, recurso humanos y financieros, etc.
- Organización: Organización propia de las personas, las estructuras organizacionales de la IES específica, cómo se concentra la organización, cómo se transforma y evoluciona a través del tiempo y cuál es el comportamiento de la organización en las contingencias.

- Dirección:Cuál es el compromiso de la dirección con la seguridad de la información en medios digitales, cuáles son los apoyos, los recursos, los elementos de institucionalidad, los acuerdos y, sobre todo, la interacción de la dirección, tanto con el departamento informático y como con los elementos externos a la organización.
- Evolución de los sistemas de gestión de la seguridad informática.

2.5.3. Encuesta Nacional:

2.5.3.1.Características de la Encuesta Nacional (RENASEC 2006):

Metodología de encuesta:

La encuesta fue diseñada por:

- La RENASEC de la ANUIES.
- El centro de respuesta tecnológica de la Universidad Nacional Autónoma de México.

El objetivo de dicha encuesta es la elaboración de dos modelos (uno enfocado a elementos técnicos y otro enfocado a elementos de gestión) para levantar una encuesta nacional sobre seguridad en cómputo que fuera la base para éste y otros estudios relacionados.

Ésta versión de encuesta fue presentada durante “La Sexta Reunión Nacional de Seguridad en Cómputo” y fue aprobada por unanimidad en el marco del Día Internacional de Seguridad en Cómputo (25 de noviembre de 2005) por las IES asociadas a la ANUIES que estuvieron presentes en el acto.

La encuesta fue aplicada e impulsada por 121 universidades de todo el país al menos a dos figuras específicas:

- Una persona cuya función sea directiva y representativa ante la ANUIES
- Una persona encargada del centro informático, de comunicaciones y/o flujos de información dentro del IES

La estructura de la encuesta es la siguiente:

Preguntas abiertas y de Interés general: Parte de la encuesta cuyas preguntas serán del tipo dirigido y nos darán un acercamiento al panorama entre las TIC y los SIeMD

Preguntas específicas: Dichas preguntas serán la guía de comparación y homologación de criterios de la revisión de preguntas anteriores

Preguntas técnicas de Seguridad: Dichas preguntas resuelven dudas técnicas más específicas y su profundidad no es el principal interés del presente trabajo de investigación.

Dicha sección de la entrevista está compuesta por:

Preguntas Lógicas

Preguntas Físicas

Preguntas Estructurales

Preguntas Organizacionales

Preguntas estructuradas: Donde se enfatizará el carácter tecnológico específicamente en elementos evolutivos, de trayectorias tecnológicas y organizacionales estructurales.

Las preguntas más importantes para la investigación, no por ello las únicas, son:

En términos de seguridad:

1. ¿Su organización contempla algún modelo de gestión de seguridad de la información?
2. ¿Qué nivel de gestión de seguridad tiene?
3. ¿Cuáles herramientas usa para tener una eficiente seguridad y gestión informacional?
4. ¿Usa terceros (outsourcing) para la gestión de la seguridad de información en la empresa?
5. De usar outsourcing, ¿Cuál es el nivel de flujo de información que se tiene con dicho proveedor?
6. ¿El proveedor posee algún tipo de certificación?

7. ¿Sabe usted si su proveedor usa algún modelo de gestión de la información?
8. ¿En su organización tiene alguna forma de jerarquizar el acceso a los diferentes fuentes de información?
9. ¿Se posee las capacidades humanas suficientes para atender problemas de seguridad de la información?
10. ¿Existen redes de intercambio de información en elementos relacionados con la seguridad de la información?

En términos de la dirección de la organización:

11. ¿Conoce las actividades de gestión de seguridad de la información?
12. ¿Participa en las actividades de gestión de seguridad de la información?
13. ¿Apoya las acciones de seguridad de manera económica o de recursos?
14. ¿Esta involucrado y apoya en todos los niveles las acciones encaminadas a seguridad de la información?
15. ¿Cada cuanto se les reporta un incidente de seguridad?
16. ¿Esta conciente de los riesgos que involucran la inseguridad de la información?

En términos de la organización:

17. ¿Dispone de una persona (Directivo) a quien se asigne las responsabilidades de la gestión de la seguridad de la información?
18. ¿Dispone de recursos humanos, financieros, materiales enfocados al área de gestión tecnológica en seguridad de la información?
19. Enumere de más importante a menos importante el tipo de tecnología que usa la organización en materia de Seguridad de la Información
20. Esta contemplada la Seguridad de la Información en el organigrama estructural de la organización

2.5.4. Análisis de Datos (evidencia empírica):

Se debe de considerar que los aspectos esenciales: el cuestionario y la encuesta nacional que se va a formular y aplicar a las IES, serán fundamentalmente la base para el desarrollo de la investigación, los análisis posteriores y las conclusiones finales, a partir de este apunte, supondremos entonces que el diseño y desarrollo del cuestionario y de la encuesta nacional deben tener elementos que puedan explicar comportamientos enfocados hacia la gestión tecnológica, por un lado, y hacia la capacidad tecnológica, por el otro, para que la información obtenida sea útil.

Un apunte importante de los resultados en la presente investigación es que, a partir de sus características, presenta tendencias y comportamientos específicos en las IES analizadas, que si bien dichas tendencias y comportamientos no pueden ser tomados como contundentes y/o globalizados, si dan una suficiente aproximación con cierto grado de certeza y resuelven las preguntas de tesis planteadas desde el primer capítulo.

Con base en lo anterior y conciente de las limitaciones con la información obtenida en ésta metodología y con la adecuación al modelo propuesto por Bell y Pavitt (Explicados en el capítulo 1), se propone el uso de una Gráfica Cruzada Evolutiva de Capacidades Tecnológicas y Capacidades de Gestión Tecnológica a través del tiempo (Figura 2.7)

Donde, a partir de los elementos evolutivos, el análisis de las entrevistas realizadas en las universidades, los resultados de la encuesta nacional y los resultados de las entrevistas personales, se puede determinar los niveles de capacidad tecnológica y niveles de gestión de seguridad de la información a través del tiempo como ya se mencionó en el primer capítulo.

Asimismo, aunque los elementos que pudieran componer una gráfica de este estilo, son en su mayoría elementos de percepción más que elementos de cuantificación, la construcción de la presente es un esfuerzo de apreciación de tendencia evolutiva, que pudiera ayudar quizás, no a medir con exactitud un fenómeno (hay que recordar que la medición de la misma tecnología puede ser muy subjetiva), sí a apreciar comportamientos específicos que pudiesen llevar a la toma de decisiones adecuada.

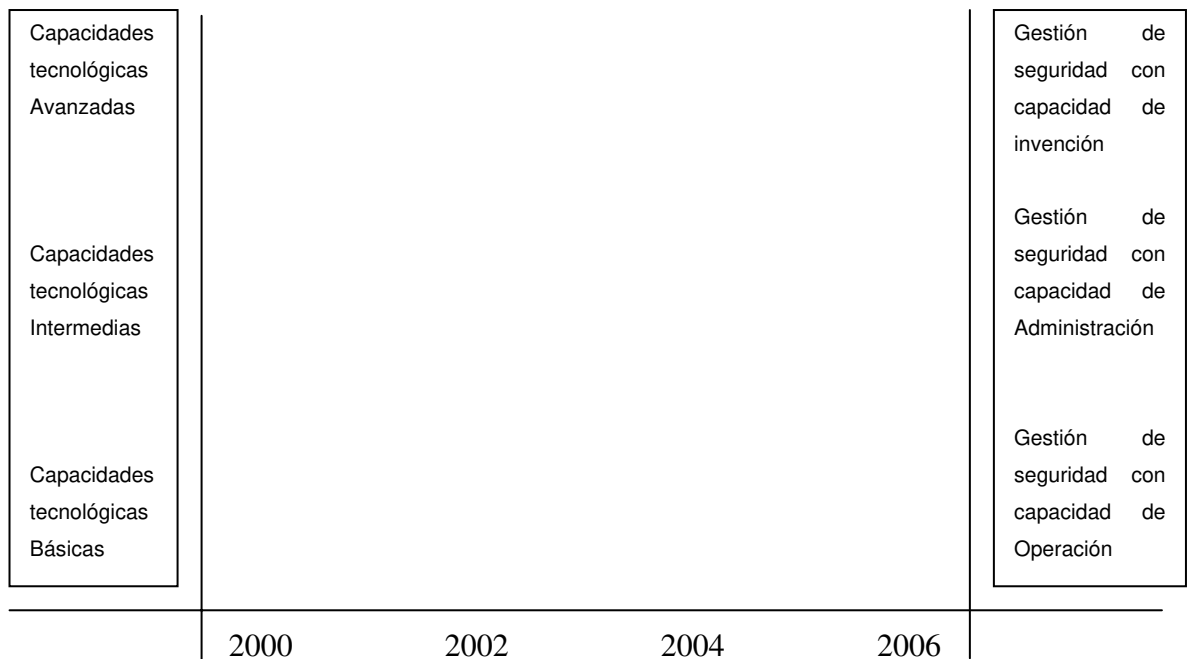


Figura 2.7 Gráfica Cruzada evolutiva de capacidades tecnológicas y capacidades de gestión tecnológica a través del tiempo. Adecuación de modelo propuesto por Bell y Pavitt (2006). Fuente: Realización Propia

El objetivo que se busca en la realización de la gráfica de la figura 2.7 es el poder determinar la evolución interna tanto de las capacidades tecnológicas de las IES como de la RENASEC, para así poder concluir si se tienen “homogeneidades” suficientes para poder interaccionar entre ambas

Los criterios para poder llenar de información la gráfica presentada en la figura 2.7 fueron descritos en el capítulo 1, y se basan en cuantificar las preguntas fundamentales de la encuesta nacional y en el resultado de las entrevistas personales con las IES

Lo que se espera es precisamente determinar cuál es el comportamiento evolutivo entre las capacidades tecnológicas en las IES y la RENASEC, así como su comportamiento evolutivo de gestión tecnológica.

Además, se espera poder contrastar la diferencia, si llegase a existir, entre lo que son la capacidad tecnológica y la gestión tecnológica en la RENASEC y en las IES asociadas.

2.5.5. Preguntas para la gestión tecnológica:

La gestión tecnológica debe poder sustentarse, de acuerdo con nuestro marco conceptual, en 5 puntos esenciales mínimos (más nunca suficientes).

- a) Vigilar y analizar
- b) Focalizar
- c) Capacitar
- d) Implantar
- e) Aprender

Además, de apoyarse con elementos reales para contrastar y analizar resultados. Dichos elementos reales pueden ser extraídos de las preguntas específicas realizadas en la presente investigación. Así, a cada uno de los 5 puntos esenciales, las preguntas asociadas quedarían de la siguiente manera:

a) Vigilar y analizar

- ¿Su organización contempla algún modelo de gestión de seguridad de la información?
- ¿Qué nivel de gestión de seguridad tiene?
- ¿Cuáles herramientas usa para tener una eficiente seguridad y gestión informacional?
- ¿El proveedor posee algún tipo de certificación?
- ¿Existen redes de intercambio de información en elementos relacionados con la seguridad de la información?
- ¿Conoce las actividades de gestión de seguridad de la información?
- ¿Cada cuanto se les reporta un incidente de seguridad?
- ¿Esta conciente de los riesgos que involucran la inseguridad de la información?
- ¿Dispone de una persona (directivo) a quien se asigne las responsabilidades de la gestión de la seguridad de la información?

b) Focalizar

- De usar outsourcing, ¿cuál es el nivel de flujo de información que se tiene con dicho proveedor?

c) Capacitar

- ¿Usa terceros (outsourcing) para la gestión de la seguridad de información en la empresa?
- ¿Participa en las actividades de gestión de seguridad de la información?
- ¿Apoya las acciones de seguridad de manera económica o de recursos?

d) Implantar

- ¿Sabe usted si su proveedor usa algún modelo de gestión de la información?
- ¿En su organización tiene alguna forma de jerarquizar el acceso a los diferentes fuentes de información?
- ¿Se poseen las capacidades humanas suficientes para atender problemas de seguridad de la información?
- ¿Existen redes de intercambio de información en elementos relacionados con la seguridad de la información?

e) Aprender

- ¿Existen redes de intercambio de información en elementos relacionados con la seguridad de la información?
- ¿Está involucrado y apoya en todos los niveles las acciones encaminadas a seguridad de la información?

2.6. Hallazgos y conclusiones del capítulo:

Los hallazgos más importantes en materia de metodología son precisamente los referentes a la elección de las herramientas y metodologías que se van a usar para el proceso de investigación de tesis, esto es:

- El presente es un estudio de caso que tiene como principales herramientas metodológicas: la aplicación de entrevistas dirigidas, una encuesta nacional así como investigación de análisis de encuestas internacionales.
- Se resaltan como fundamentales para el estudio de caso las siguientes rutinas metodológicas :
 - Elección de las fuentes de información
 - Recogida de datos de encuestas

- Análisis de datos de encuestas
- Conformación de encuesta
- Análisis de pendientes y tendencias.
- Estudio de patentes (Intensidad Inventiva)

C
A
P
Í
T
U
L
O

3

Análisis de Evidencia Empírica

3. Análisis de Evidencia Empírica

3.1. Introducción

El presente capítulo se divide en 3 partes, cada una de ellas da el resultado de análisis de evidencia empírica en 3 fuentes de información y cuyos objetivos particulares y características son las siguientes:

1. Un primer apartado que contiene el análisis de la evidencia empírica recabada esencialmente en las encuestas globales sobre seguridad en cómputo (Mancera Ernst y Young), y cuyo objetivo particular es evidenciar los tipos de tecnología usados en los ataques de seguridad en una perspectiva evolutiva y de trayectoria tecnológica, midiendo asimismo el riesgo asociado de dicha evolución.
2. Un segundo apartado, que contrasta los resultados obtenidos en el primer apartado con la encuesta realizada por la CSI/FBI, donde el objetivo específico es el resaltar cuales son las tendencias de las tecnologías de SIeMD usadas para salvaguardar la información, en un enfoque evolutivo y de trayectoria tecnológica en lo que denominamos “Análisis de pendientes”
3. Un tercer apartado, que es un estudio exploratorio de patentes aplicando la técnica de “palabras clave” y de “clases de patente”, cuyo objetivo principal será determinar y evidenciar la existencia de elementos convergentes, divergentes o mixtos en la medición de “actividad inventiva” dentro de las patentes (resultado muy importante en materia de gestión tecnológica argumentado en el primer capítulo de ésta tesis).

3.2. Revisión de encuestas internacionales, nacionales y globales (Encuestas)

La evidencia empírica, conjuntamente con el marco teórico, da un entorno real al objeto de estudio, esto es, el marco teórico evidentemente da los insumos conceptuales, sin embargo, dichos elementos resultarían limitados si no se pueden contrastar con un marco de referencia empírico que integre elementos reales, generales y globales a la investigación, esto se puede lograr haciendo análisis de encuestas globalizadas.

El objeto de este capítulo será dar un entorno real al objeto de estudio, desde una perspectiva empírica y global a partir de distintas fuentes de información. (entre las que se encuentran las patentes y las encuestas de seguridad de la información globales).

3.2.1. Tipos de Tecnología usada en los ataques a la seguridad de la información en medios digitales.

De acuerdo a lo discutido en el capítulo 1, los ataques son eventos, exitoso o no, que atentan sobre el buen funcionamiento del sistema; los hay de diferentes tipos y de distintos niveles de riesgo.

En nuestro caso particular, una introducción a los elementos empíricos se da al vislumbrar de manera general: cuáles son los ataques más comunes, sus tipos y el significado que estos datos tienen para nuestra investigación.

Siguiendo la metodología presentada en el capítulo 2, el análisis hecho a las encuestas de Mancera y Young (1997 -2004)¹ nos arrojan los siguientes resultados:

¹ Cabe recordar que la elección de las encuestas de Mancera Ernst y Young es debido a que dicha encuesta se aplica (de forma anual desde 1998) en los 50 países más importantes económicamente, convirtiendo a estas encuestas en las de mayor confianza en la materia.

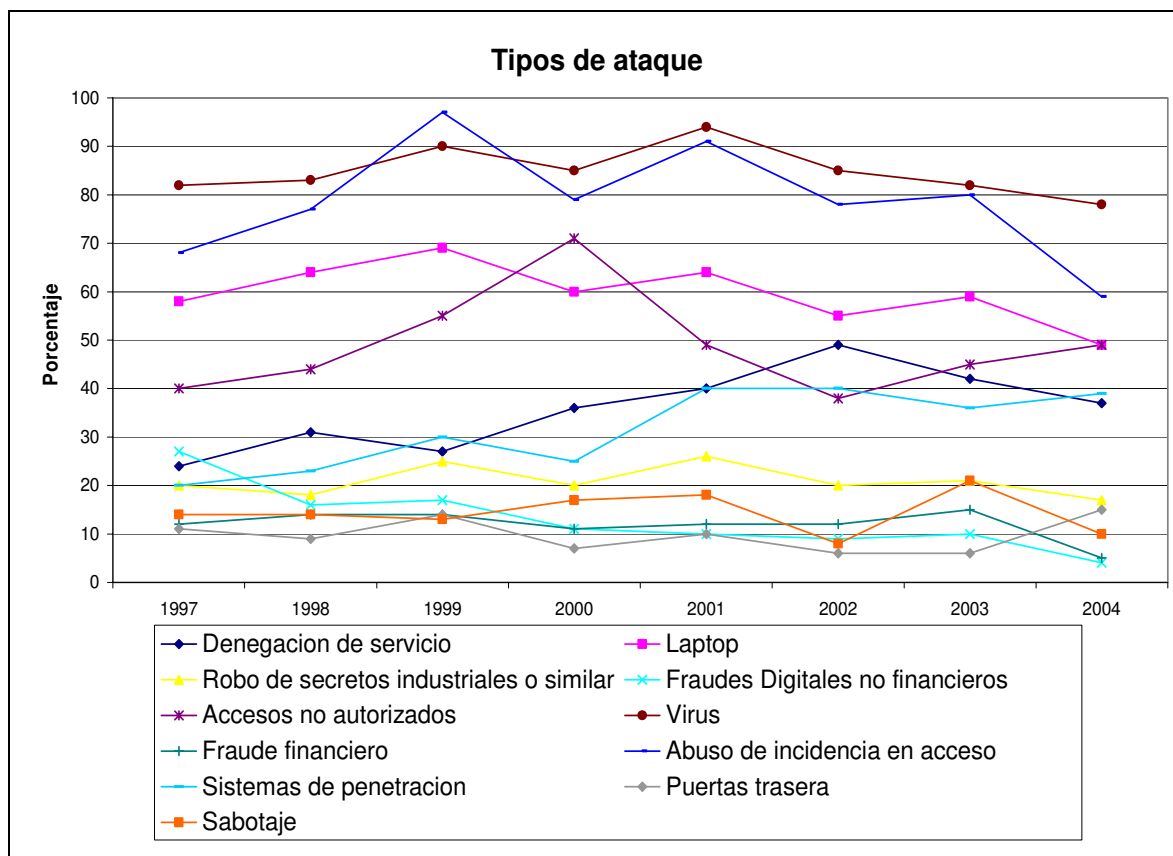


Figura 3.1 Evolución de los tipos de ataque

Realización propia, con base en: Mancera Ernst & Young (1997 – 2004) “Encuesta Global de seguridad informática”

A partir de los resultados mostrados en la figura 3.1, uno de los elementos que se pueden analizar son las tendencias evolutivas a través del tiempo de los tipos de ataque realizado a las tecnologías de información y comunicaciones, de acuerdo a Mancera Ernst y Young (1997 -2004).

Se destacan 4 tipos de ataque: El aumento a través de los años de los sistemas de penetración, el aumento a través de los años de la denegación de acceso, y sobre todo, la tendencia a través de los años de niveles altos de ataques por virus y el abuso en la incidencia de accesos.

Cabe hacer notar que los elementos antes mencionados, pese a ser resultados de una encuesta en particular, son consistentes con la mayoría de los análisis en encuestas sobre seguridad de la información en medios digitales en diversas partes del mundo CSI/FBI (2002, 2003, 2004, 2005 y 2006), CEPAL (2003).

Aunque no es el objetivo específico de la presente tesis, es significativo que, en las encuestas de la RENASEC hechas en el 2002, 2004 y 2006, existen coincidencias en forma general con los resultados de Mancera Ernst y Young (1997 -2004) descritos en la Figura 3.1.

La denegación de servicio y el ataque por virus son los dos tipos de ataque más frecuentes en los últimos 4 años. Este dato es fundamental para nuestra investigación, ya que con este primer hallazgo podemos apreciar una coincidencia en las tendencias del comportamiento de los ataques tanto en la RENASEC como en otras encuestas realizadas a través del mundo.

De acuerdo a la metodología descrita y a los resultados plasmados en la figura 3.1 se puede asegurar que el hallazgo más importante es la existencia de 3 tipos de tendencia en la gráfica:

- Una tendencia de pendiente negativa (decrecimiento constante) en algunos de los riesgos (Sobre todo en aquellos que tenían un mayor porcentaje inicial), lo que significaría una disminución del riesgo a través de los años.
- Una tendencia estacionaria, lo que significaría que no existe aumento ni disminución de ataques.
- Una tendencia de pendiente positiva (crecimiento constante) en algunos de los riesgos, sobre todo en aquellos que tenían un menor porcentaje inicial, lo que significaría un aumento del riesgo a través de los años.

Complementando esta información, las entrevistas realizadas a los encargados de la seguridad de la información en medios digitales de las IES, y otras encuestas revisadas, coinciden en 3 puntos:

1. Sí, existe una disminución en la frecuencia de los ataques (en los tipos de tecnología que inicialmente tenían valores altos) debido, entre otras cosas, a que las personas responsables de los centros de cómputo están cada vez más preparados para identificar y contrarrestar los ataques. Lo que en otras palabras muestra la existencia de un aumento en las capacidades tecnológicas dentro de los centros de cómputo e informática de las IES,

incluso la presencia de acumulación de capacidades tecnológicas a través del tiempo.

2. Al haber un aumento en las capacidades tecnológicas de las personas involucradas, y una evidente acumulación de capacidades en seguridad de la información, también podemos notar que los efectos negativos (económicos, tecnológicos, sociales, culturales, etc.) de los ataques son cada vez más fuertes, en otras palabras, aunque ciertamente hay una menor frecuencia de ataques a través del tiempo, dichos ataques son cada vez más contundentes y sus efectos negativos (Económicos, sociales, culturales, etc) suelen ser más indiscutibles y duraderos, haciendo que el número de personas afectadas vaya en aumento y la sensación de inseguridad de la información también crezca.
3. Si bien existen algunos tipos de ataque que permanecen constantes en su frecuencia a través del tiempo, e incluso van disminuyendo su frecuencia, es indudable que la sensación de inseguridad no ha podido ser disminuida; más al contrario, en todas las encuestas se coincide con la percepción de que día a día van aumentando los niveles de inseguridad relacionada con la información en todos los niveles (personal, escuelas, oficinas, industria, etc).

Este es un elemento que llama la atención ya que, si se analizan los tres puntos anteriores, podemos llegar a la conclusión de que: **el aumento en las capacidades tecnológicas y la acumulación de dichas capacidades en los centros de cómputo de las IES, está siendo opacado, por los elementos y factores que generan inseguridad en la información de los medios digitales.**

Asimismo, pareciera ser que en el rubro de la tecnología en SIeMD, las personas y organizaciones que generan inseguridad están siendo más eficientes y eficaces que las personas y organizaciones que generan la seguridad.

La conclusión más importante es que **de acuerdo a los resultados y al análisis, generar capacidades tecnológicas en el rubro de seguridad de la información en medios digitales no genera certidumbre suficiente para disminuir la sensación de inseguridad de la información en las IES.**

Una pregunta oportuna sería ¿Qué factores son los que inciden directamente con las capacidades tanto de la gente que genera seguridad como de la gente que genera inseguridad?, incluso si ¿existen algún otro agente, que no haya sido considerado, el cual influya en la sensación de seguridad de la información en medios digitales?

Se debe recordar que, en materia de seguridad de la información en todos los niveles, un parteaguas importante de inseguridad es el que se vivió en los Estados Unidos el 11 de septiembre de 2001, donde, debido a elementos de inseguridad de varios tipos, al menos 3 aviones fueron usados como misiles en contra de blancos específicos civiles, evidenciando con ello, entre otras muchas cosas, sistemas informacionales limitados, poco confiables y altamente violables.

Esta experiencia alertó al mundo entero, de lo vulnerable que son los sistemas de información, y cómo “alguien” podía usarlos en contra del mismo sistema² (como se menciono anteriormente, al menos un agente, llamado “terrorismo”, pudo generar las capacidades tecnológicas y concentrar conocimiento suficiente en la materia de seguridad de forma que los sistemas informáticos de aquel año (2001) fueron insuficientes para poder generar seguridad), desafortunadamente no es éste un elemento aislado ni único, ya que los ataques en Estados Unidos son solo una de las formas de manifestación de inseguridad informática; otras manifestaciones como fraudes electrónicos, accesos no autorizados, pérdida de información, etc, son cada vez más comunes en nuestros días

Siguiendo con el análisis de los datos de la figura 3.1, y de acuerdo con el apartado 2.4.1.2 se construye la tabla 3.1:

Tipo de Tecnología	Riesgo tecnológico alto	Riesgo Económico alto	Riesgo Estructural alto	Pendiente a través del tiempo Positiva + Negativa -
Denegación de servicio			X	+
Laptop			X	-
Robo de secretos	X	X	X	-

² En este caso el sistema de seguridad de toda una nación y con una influencia global a los sistemas de seguridad de todo el mundo.

industriales o similar				
Fraudes Digitales no financieros	X	X		-
Accesos no autorizados	X	X	X	-
Virus	X	X	X	-
Fraude financiero	X	X	X	-
Abuso de incidencia en acceso		X	X	-
Sistemas de penetración	X		X	+
Puertas trasera	X	X		+
Sabotaje	X	X	X	-

Tabla 3.1 Interpretación de la Evolución de los tipos de ataque.

Realización propia, Fuente: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática”

Al observar las pendientes en la tabla 3.1, puede notarse como dichas pendientes han disminuido en la gran mayoría de las tecnologías, lo que nos haría suponer que existe una mayor preocupación por los Sistemas de Seguridad de la Información, y por ende la implementación de una mayor cantidad de herramientas en seguridad; sin embargo, este dato es engañoso ya que si bien disminuye el porcentaje (frecuencia de los ataques), también se encuentra que ha aumentado la contundencia y efectos negativos de los mismos, en otras palabras, significa que el riesgo va disminuyendo en cantidad pero aumentando en complejidad y efectos negativos.

El efecto más evidente (aunque no el único) es el que se detecta en las consecuencias económicas que provocan los ataques y la inseguridad de la información en medios digitales, ya que se evidencia, en todas las encuestas revisadas en la presente investigación, que año con año, va aumentando la cantidad de dinero que se pierde por la inseguridad, lo que nos hace ver, como ya se mencionó, menor cantidad de incidencias pero con mayores grados de consecuencia (en este caso económica).

Efectos sociales, culturales, educativos, etc. siguen la misma lógica, aparentemente menor cantidad de incidencias pero un mayor efecto negativo de éstas.

Podríamos suponer, por sus efectos y características, que este efecto de inseguridad sólo se presenta en países en vías de desarrollo, sin embargo es consistente también en

economías tan controladas como la de Estados Unidos, Japón y la Unión Europea CSI/FBI (2002, 2003, 2004, 2005, 2006) como el observado a nivel mundial Mancera Ernst & Young (2002, 2003, 2004, 2005 y 2006)

Otro dato interesante, para los intereses de nuestra tesis, es precisamente el aumento en la cantidad de ataques especializados o puntuales, esto es, si bien han disminuido el número de ataques a grosso modo, llamados también ataques estándar (Mancera Ernst & Young 2002, 2003, 2004, 2005 y 2006), también es cierto que han aumentado los ataques tanto “especializados” como los “desconocidos”³, este tipo de ataque e inseguridad evidencia 2 elementos:

- Nuevamente, la existencia de capacidades tecnológicas muy grandes por parte de las personas que provocan la inseguridad
- La existencia de capacidades tecnológicas limitadas por parte de las personas que gestionan, operan, monitorean y aplican los sistemas de seguridad en las organizaciones

Lo dicho anteriormente se puede observar en la siguiente gráfica:

³ Un ataque “desconocido” es aquel en el cual se tiene un desconocimiento del origen del ataque, los efectos del ataque o incluso el desconocimiento mismo de la existencia del ataque.

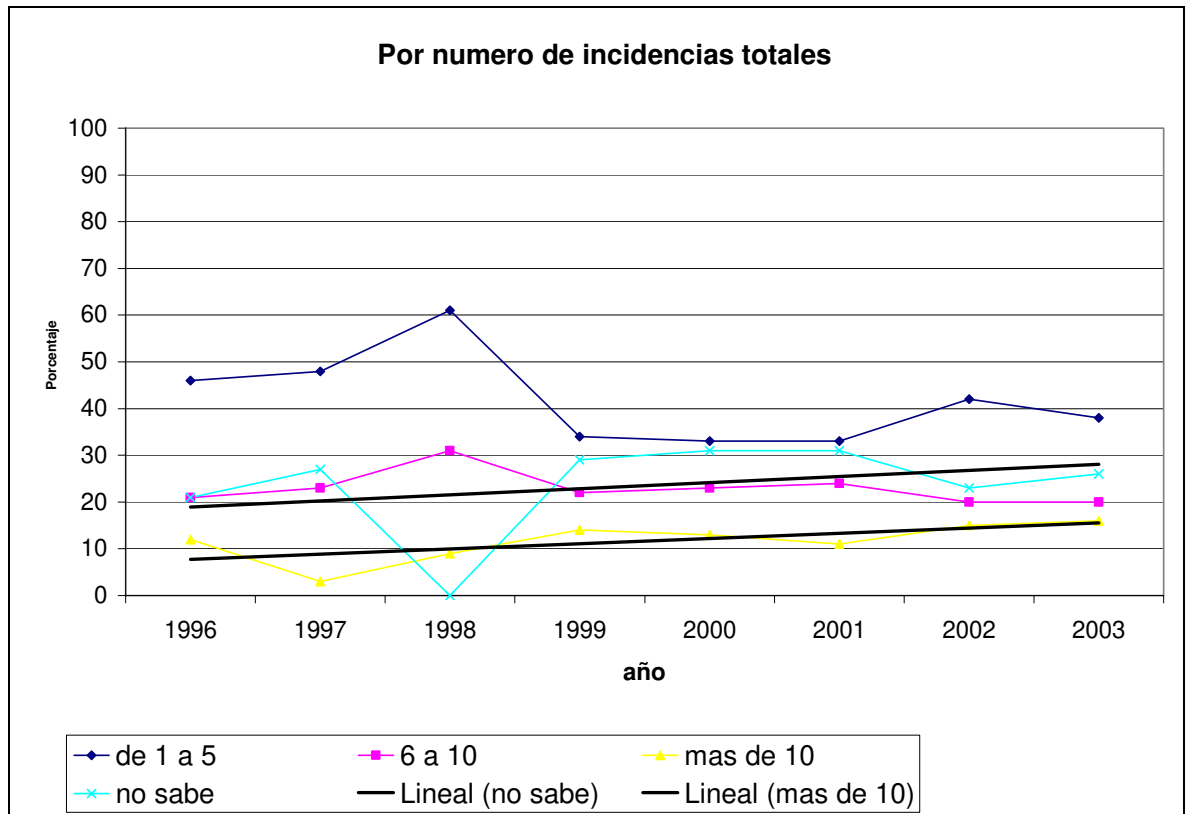


Figura 3.2 Evolución del # total de incidentes promedio por año.

Realización propia, Fuente: Mancera Ernst Young (1997 – 2004) “Encuesta Global de seguridad informática”

De acuerdo con los datos de la figura 3.2, podemos observar dos elementos fundamentales para el entendimiento de la investigación:

1. Existe una tendencia de crecimiento (pendiente positiva) a través de los años en el reporte de “10 o más incidencias de seguridad de la información totales durante el año”, en otras palabras, de manera general y de acuerdo con las encuestas del (CSI/FBI 2002, 2003, 2004, 2005 y 2006) “Reporte anual de delitos informáticos”, en el mundo va aumentando la cantidad de centros de computación que detectan más de 10 incidencias durante el año.
2. También existe una tendencia creciente, respecto al desconocimiento del número de incidencias (lo que manifiesta un desconocimiento del origen, tipo y forma del ataque), esto significa una disminución, a través de los años, de capacidades tecnológicas o bien de capacidades tecnológicas muy limitadas o nulas.

3.2.2. Uso de Tecnología de seguridad de la información en medios digitales.

Así como se han detectado los tipos de ataque, también es conveniente identificar los tipos de tecnología que se han desarrollado, y usado, para contrarrestar los ataques, ya que, para los intereses de la presente tesis, es de suma importancia tener una perspectiva de los tipos de tecnología de seguridad desarrollada, y con ello, poder concluir qué relación existe entre los ataques y las tecnologías desarrolladas.

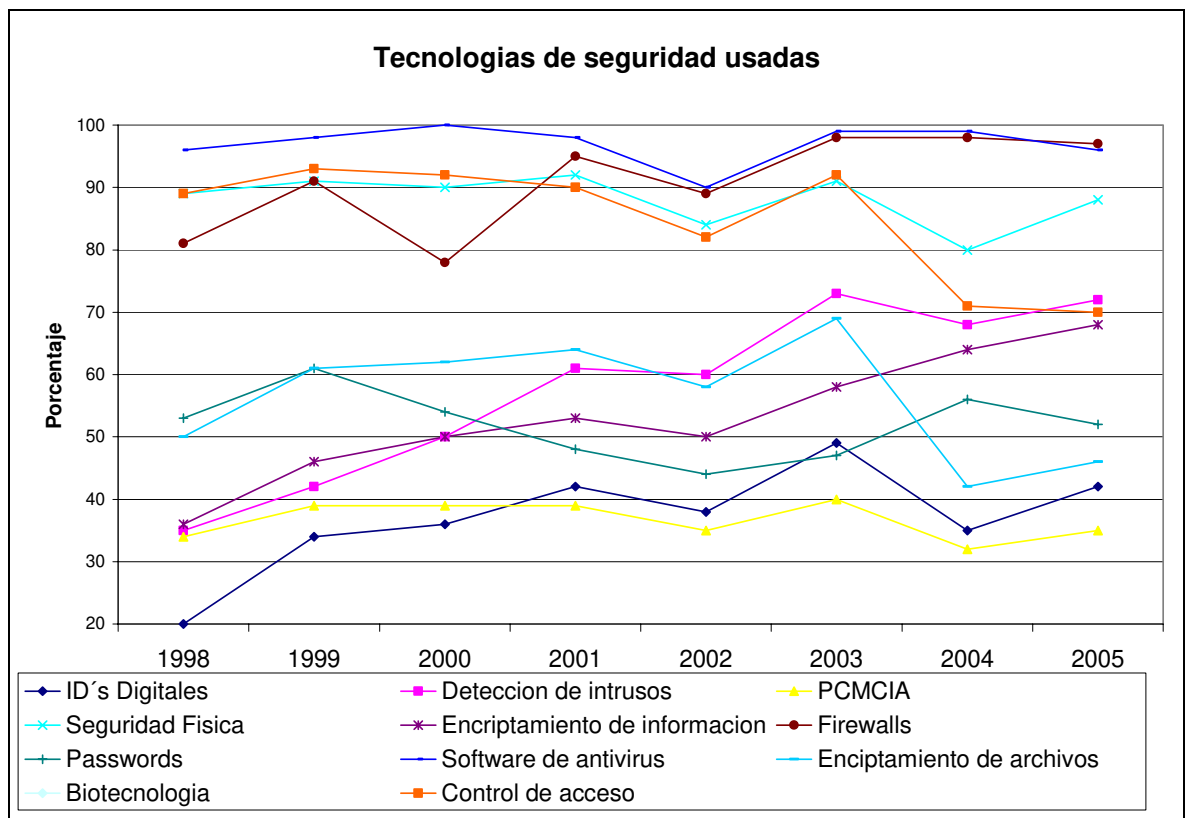


Figura 3.3 Evolución del tipo de tecnología usada en materia de seguridad por año.

Realización propia, Fuente: CSI/FBI (2002, 2003, 2004, 2005 y 2006), Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey"

Analizando 4 de ellos (en forma de muestra) a profundidades, se obtienen los siguientes resultados:

ID Digitales (Tecnología de Reacción): Este tipo de tecnología sirve para poder determinar la identidad de algún tipo de intruso en los sistemas de información.

Observando la figura 3.4, podemos decir que la pendiente nos indica un aumento en el uso de esta tecnología.

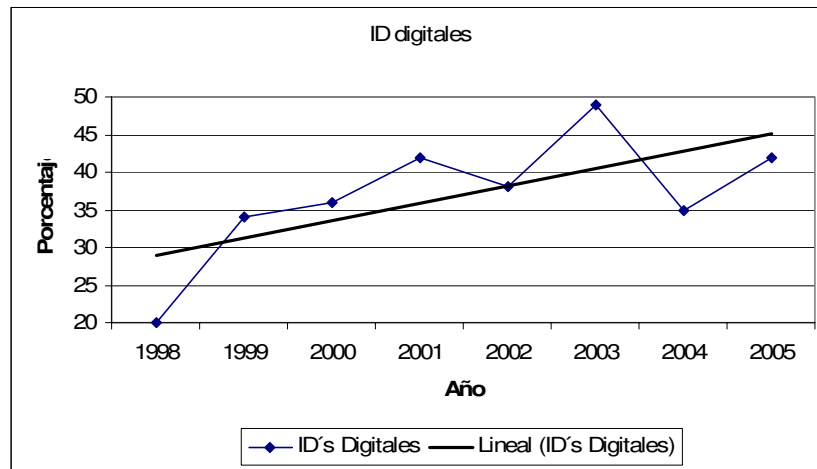


Figura 3.4 Evolución de las ID digitales usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Monitoreo y detección de Intrusos: (Tecnología de Reacción), Este tipo de tecnología sirve para poder detectar la presencia de intrusos en el sistema así como para generar registros de los movimientos de los intrusos.

De acuerdo con la figura 3.5, podemos determinar una pendiente positiva, lo que nos indica un aumento en el uso de esta tecnología.

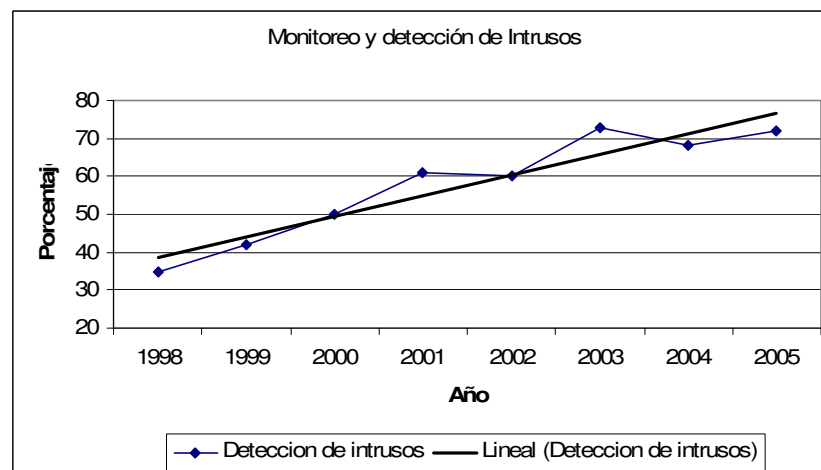


Figura 3.5 Evolución de “Monitoreo y detección de intrusos” usada en materia de seguridad por año. Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Desarrollo de tarjetas inteligentes: (Tecnología de Prevención), Este tipo de tecnología sirve para anticiparse a robos físicos o de información de los sistemas de información

De acuerdo con la figura 3.6, podemos determinar una pendiente que nos indica una disminución en el uso de esta tecnología.

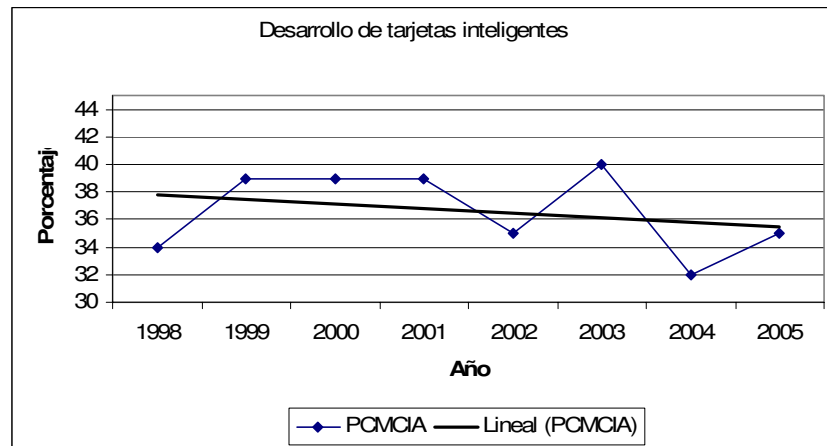


Figura 3.6 Evolución de “Desarrollo de tarjetas inteligentes” usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Seguridad Física: (Tecnología de Prevención) Este tipo de tecnología sirve para anticiparse a robos físicos o de información de los sistemas de información, así como de anticipación a ataques concretos por vías externas de los equipos de cómputo.

De acuerdo con la figura 3.7, podemos determinar una pendiente que nos indica una disminución en el uso de esta tecnología.

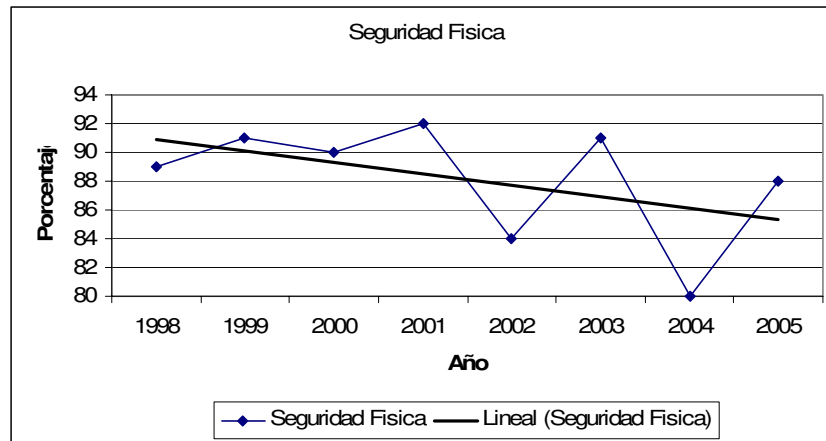


Figura 3.7 Evolución de “Seguridad Física” usada en materia de seguridad por año, Realización propia, Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Haciendo el análisis para el uso de cada uno de los elementos nos dio la tabla 3.2:

Tipo de Tecnología	Pendiente Positiva	Pendiente Negativa
Reacción		
ID Digitales	X	
Monitoreo y detección de Intrusos	X	
Firewalls	X	
Passwords	X	
Antivirus	X	
Prevención		
Desarrollo de tarjetas inteligentes		X
Seguridad Física		X
Encriptamiento de información	X	
Encriptameinto de Archivos		X
Biotecnología	X	
Control de acceso		X

Tabla 3.2 Interpretación de las “Tecnologías de Seguridad Usadas”, Realización propia, Fuente: Fuente: CSI/FBI (1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005) “Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”

Estos resultados son muy significativos por dos elementos específicos:

- 1) De acuerdo con lo observado en las gráficas 3.4 a 3.7, podemos asegurar que existe una tendencia a consumir y confiar más la seguridad de la información a tecnologías reactivas, esto es, evidentemente se está aumentando el uso y consumo de tecnologías reactivas, lo que concuerda con las entrevistas realizadas a los encargados de seguridad de la información de las IES asociadas a la ANUIES.

Las entrevistas con las IES de la ANUIES pertenecientes a la RENASEC evidenciaron, además 2 elementos adicionales:

- a. Presumiblemente esta tendencia (aumento de uso y consumo de tecnologías reactivas) se debe a las fallas constantes en la seguridad por parte de tecnologías preventivas, lo que ha orillado a confiar y usar más las tecnologías reactivas.
 - b. Otro aspecto importante es precisamente el precio, como ya se mencionó anteriormente, es en general mucho más económico el desarrollo, difusión e implementación de una tecnología reactiva que de una tecnología preventiva eficiente.
- 2) Siendo las tecnologías de reacción demandantes de menos capacidades tecnológicas para su uso, estamos entonces ante una manifestación de disminución de capacidades tecnológicas en el campo del desarrollo de tecnologías preventivas de seguridad de la información.

En términos de capacidades tecnológicas, estamos observando que la tendencia es la disminución del consumo de tecnologías que representen una alta concentración de capacidades tecnológicas.

Existe otra hipótesis distinta a la teoría de las capacidades:

A partir de los resultados, tanto de las encuestas de seguridad en la información realizada a las empresas, las personas, y en general, a los usuarios de tecnología de seguridad, como de las encuestas realizadas a los responsables de seguridad de la información de las IES, se encuentra que existe un aumento de la desconfianza en el uso en las tecnologías preventivas.

La razón de dicha desconfianza se basa en la suposición, de origen empírico, de que las tecnologías preventivas son de un nivel de obsolescencia alto, esto es, que en el corto plazo se vuelven obsoletas; lo que es lo mismo que decir que en el corto plazo existirá una contra tecnología⁴ que hará obsoleta y riesgosa la tecnología preventiva usada (consumida).

Cuando el fenómeno de obsolescencia tecnológica se presenta con cierta frecuencia, existe la sensación de estar “comprando” tecnologías poco eficientes y con ciclos de vida muy cortos, lo que a la larga provoca la disminución en el consumo de dichas tecnologías y un evidente desaliento y disminución del mercado, lo que a su vez provoca la disminución de la demanda y la disminución de la oferta.

Es un hallazgo importante darse cuenta que las tecnologías preventivas, con gran acumulación de capacidades tecnológicas van disminuyendo en su desarrollo, uso y aplicación a través del tiempo, en cambio las tecnologías reactivas que suponen una menor cantidad de acumulación y de capacidades tecnológicas van aumentando en su desarrollo, uso y aplicación.

Aunque no se puede sacar algún tipo de conclusión definitiva respecto a las causas de estas manifestaciones, si se puede usar estas tendencias para su uso posterior en la presente investigación al momento de analizar las causas por las cuales un sistema se SIeMD pasa de un estado inicial a uno final.

⁴ Una contra tecnología es conocida como una tecnología desarrollada para contrarrestar, mitigar o nulificar los efectos de otra tecnología conocida.

3.3. Evidencia empírica sobre inseguridad en medios digitales (Estudio de patentes)

Inseguridad debida al desfaseamiento y/o divergencia tecnológica

En el contexto de la presente investigación se ha discutido la existencia de elementos que pudiesen influir en los resultados de la misma, uno de los más importantes es el “desfaseamiento o divergencia tecnológica” entre las TIC`s y las Tecnologías de Seguridad de la Información en Medios digitales (TSIeMD).

Existe mucha evidencia respecto al comportamiento convergente o divergente en materia de TIC`s (CEPAL 2003, Castells, M. 1996-2000, Hilbert, M. & Katz J.2003); sin embargo, no existe hasta el momento de la realización de esta tesis, evidencia respecto a la divergencia tecnológica en el punto específico de seguridad de la información en medios digitales. Esta divergencia o desfaseamiento tecnológico puede ser detectado de varias formas, entre ellas, el estudio exploratorio de patentes.

3.3.1. Estudio de Patentes “Palabras Claves”

Después de realizar el estudio de patentes “palabras claves”, descrito en la metodología de la presente tesis, se tienen los siguientes resultados:

De acuerdo a lo que observamos en la tabla 3.3 (y con más detalle en la figura c.1, c.2, c.3, c.4 y c.5 del Anexo F) , se puede asegurar que existe una tendencia a la disminución de intensidad inventiva de patentes en seguridad de la información en medios digitales en las patentes de TIC`s y que corresponden a las palabras claves “system”, “software ó hardware”, “computer or computing” e “Internet”; lo cual, de acuerdo con nuestro marco conceptual, nos hace concluir la existencia de una divergencia tecnológica. Esto es, tanto en Estados Unidos como en el Mundo, en los rubros específicos antes mencionados, existe una disminución en la intensidad inventiva de sistemas de seguridad, lo que significa una divergencia tecnológica.

Este resultado es por de más importante, por las siguientes razones:

- Las palabras claves “software ó hardware” son especialmente significativas ya que en particular, de acuerdo con artículos publicados en la USPTO, éste rubro tiene la 3ª mayor tasa de crecimiento, por lo que adquiere gran importancia la divergencia encontrada

- Un resultado que llama poderosamente la atención es el mostrado en la figura c.3 del “Anexo F”, correspondiente a las palabras clave “computer or computing” y que, según la editorial de la pagina de USPTO de mayo del año en curso posee la 4ª mayor intensidad inventiva dentro de las “TIC’s”, y que como este resultado refleja también existe la evidencia de elementos divergentes.
- En la tabla 3.3, y con más detalle en la figura c.4 del anexo F, es quizá la gráfica más significativa del presente estudio exploratorio (ya que ningún otro rubro o palabra clave es tan representativo de las TIC’s como la palabra “Internet”, y la Internet es el símbolo de fortaleza de las TIC’s, su mejor representante y sin duda, pilar en el nuevo paradigma sociotecnológico de acuerdo a varios autores. Pérez, C 2000, Fremman, C. y Pérez, C., 1986) lo que hace destacar la existencia de una divergencia tecnológica en dicha palabra clave.
- Cabe destacar que la “figura c.5 del anexo F” tiene elementos característicos distintos a las demás gráficas analizadas:
 - Primero se caracteriza porque la primer patente solicitada con esta “palabra clave” es del año 1998 (2 años después de hacerse público la Internet)
 - Segundo, porque esta gráfica representa que la Internet es sin duda es el rubro con mayor dinámica inventiva dentro de las TIC’s.

	1980 – 1992 EUA	1993 – 2005 EUA	1980 – 1992 Mundo	1993 – 2005 Mundo
Promedio de la Intensidad Inventiva, Palabra Clave: “System”	0.3873	0.2738	0.2948	0.2597
Promedio de la Intensidad Inventiva, Palabra Clave: “Software or Hardware”	1.7307	0.5885	2.2930	0.8743
Promedio de la Intensidad Inventiva, Palabra Clave: “Computer or Computing”	1.6564	0.8510	0.9604	0.7985
Promedio de la Intensidad Inventiva, Palabra Clave: “Internet”	1.5960	1.2992	0.71386	0.65796
Promedio de la Intensidad Inventiva, Palabra Clave: “Information”	0.2209	0.2195	0.1621	0.3435

Tabla 3.3 Concentrado de resultados en la medición de la intensidad inventiva de patentes por palabra clave entre los años 1980 a 1992 y 1993 a 2005 en Estados Unidos (USITO) y el Mundo (ESPaNET).

Es de destacar entonces la existencia de una tendencia generalizada con pendientes negativas, lo que es reflejo de la existencia de una divergencia tecnológica, debida a que existe una disminución generalizada en las intensidades inventivas en el tiempo.

Como se puede observar, dentro del presente estudio exploratorio, la única figura que pudiese representar un aumento de la intensidad inventiva de la seguridad de la información en medios digitales es precisamente la de patentes del mundo con la palabra clave “information”.

3.3.2. Estudio de Patentes “Clases de Patentes”

Para realizar una verificación de la conclusión obtenida en el estudio exploratorio de patentes del apartado 3.2.1 de la presente tesis, se procedió a identificar cuáles eran las “clases de patentes”⁵ que fueran las más citadas en el ejercicio anterior, para así, validar los resultados obtenidos del ejercicio pero ahora no con “palabras claves”, sino con “Clases de Patentes Específicas”.

Para facilitar la tarea, se hizo uso de la herramienta informática llamada Matheo Patent, la cual nos da, por cada palabra clave, las clases de patentes más representativas de esta palabra clave en especial, incluso, de un conjunto de ellas.

The screenshot shows the Matheo Patent 7.1 software interface. The main window displays a list of patent classes (IPC Class) and their corresponding patent numbers, titles, and scores. The interface includes a menu bar (File, Edit, Show, Statistics, Reports, Exports, Tools, Scores, Window, ?) and a toolbar with icons for New, Open, Save, Add patents, Update, Patent Analysis, Patent Info, Patents filter, All read, Graphics, and Report. The main window is divided into several panes. The left pane shows a list of patent classes (IPC Class) and their corresponding patent numbers, titles, and scores. The right pane shows a detailed view of a specific patent, including its title, abstract, and bibliographic data. The bottom pane shows a list of patent classes (IPC Class) and their corresponding patent numbers, titles, and scores.

IPC Class	Family	Number	Title	PR.D	F...	Score
G06F	149	HK1020629	METHOD FOR STORING AND OPERATING SENSITIVE INFORMATION IN A SECURITY MODULE, AND ASSOCIATED SECURITY MODULE	13/03/1997	9	
H04L	110	EP1467366	SECURITY SYSTEM USING OPTICAL INFORMATION RE...	11/01/2002	7	
G06Q	32	HK1039507	SECURITY ROOM FOR INFORMATION TECHNOLOGY FA...	17/11/1998	6	
G06K	25	AU2005201002	METHOD AND SYSTEM FOR DISPLAYING AND MANAGI...	23/04/2004	6	
H04D	18	US2005289062	DATA STORAGE DEVICE CAPABLE OF STORING MULTI...	25/07/2002	5	
G09B	17	EP1548900	NETWORK ACCESSIBLE APPARATUS, SECURITY METH...	30/09/2002	5	
H04M	15	EP1497799	INTEGRATED VISUALIZATION OF SECURITY INFORMAT...	18/04/2002	5	
H04K	15	EP1418485	SECURITY AND AUTHENTICATION OF INFORMATION F...	06/11/2002	5	
H04N	14	CN1748405	COMMUNICATION SYSTEM FOR INFORMATION SECUR...	15/01/2003	5	
G09C	12	CN1468841	SMART CARD ENABLED MOBILE PERSONAL COMPUTI...	28/07/2000	5	
G11B	9	US6795553	METHOD AND APPARATUS FOR MODULAR INVERSION...	04/11/1997	4	
B42D	8	US2006074917	SCALABLE AND FLEXIBLE INFORMATION SECURITY FC...	30/09/2004	4	
G07C	7	US2006015943	METHOD AND DEVICE FOR ANALYZING AN INFORMAT...	10/11/2002	4	
H04B	4	US2005166259	INFORMATION SECURITY AWARENESS SYSTEM	10/01/2002	4	
G07F	4	US2004243496	FINANCIAL INFORMATION INPUT METHOD USING SYM...	25/04/2001	4	
B60R	4	IL128099	PERSONAL INFORMATION SECURITY AND EXCHANGE	22/07/1996	4	
E09B	3					
B44F	3					
B41M	3					
G08C	2					
G08B	2					

Figura 3.8 “Clases de patentes” más significativas en las TIC’s y los Sistemas de Seguridad de la Información en Medios Digitales obtenidas a partir de un estudio exploratorio de patentes denominada “Palabras Clave”.
Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

⁵ “Clases de patentes”, término usado en el apartado 2.2.2 de la presente tesis

Del ejercicio anterior, se decidió escoger las 4 “clases de patentes” que fueran más representativas tanto de las TIC’s como de los Sistemas de seguridad de la Información en Medios Digitales, las clases elegidas para hacer la validación del estudio de patentes en “palabras claves”, fueron:

- G06F TRATAMIENTO DE DATOS DIGITALES ELÉCTRICOS
- H04 TÉCNICA DE LAS COMUNICACIONES ELÉCTRICAS
- G11 REGISTRO DE LA INFORMACIÓN
- H04K COMUNICACIONES SECRETAS; PERTURBACIÓN DE LAS COMUNICACIONES⁶

La verificación nos arrojó los resultados mostrados en la figura 3.9.

⁶ Aunque no fue una de las más importantes la H04K fue incluida por la razón de que su contenido es, de acuerdo con Macau, R (2004). el más importante en términos de seguridad de la información en medios digitales.

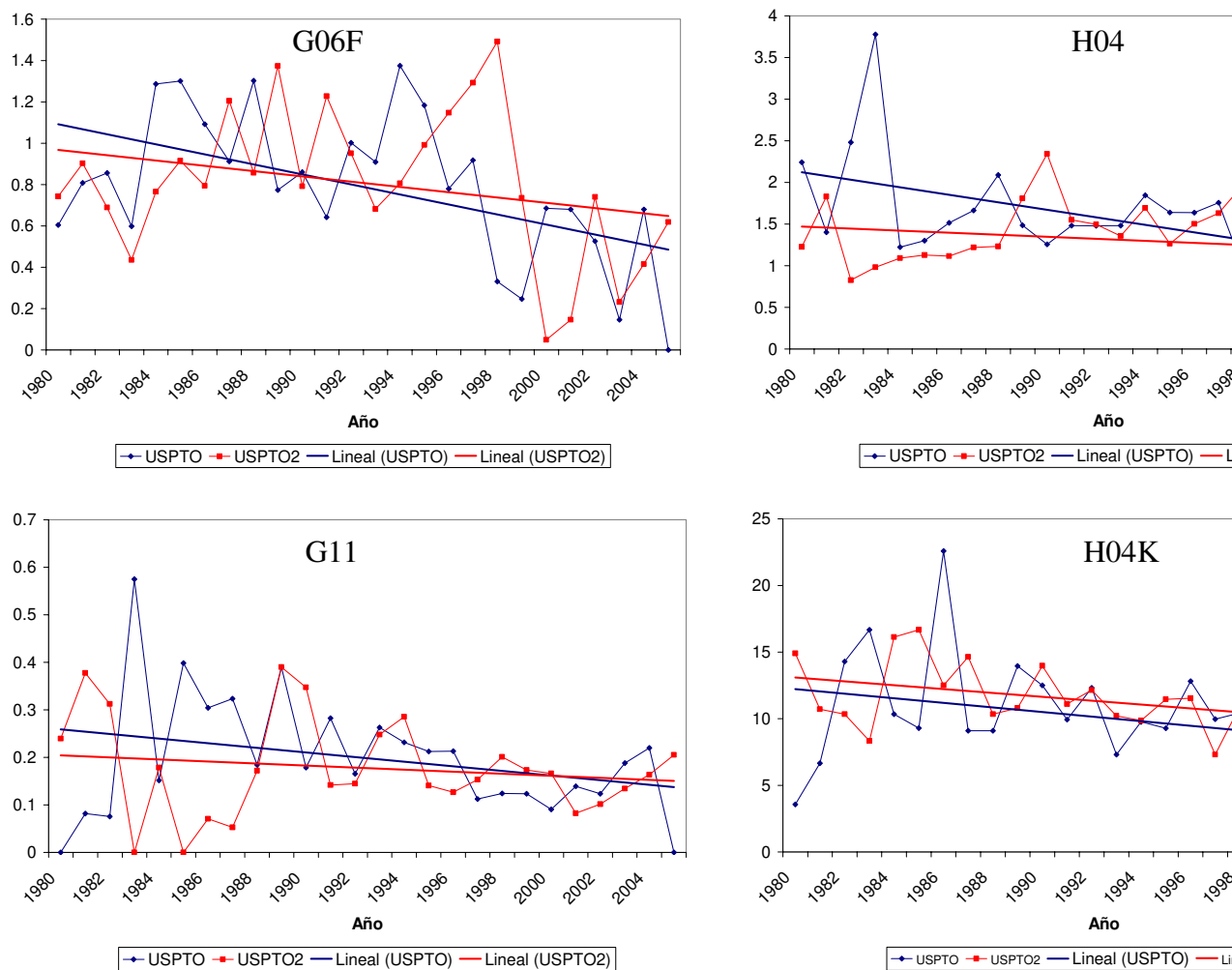


Figura 3.9 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que se relacionan con las clases de patentes G06F, H04, G11, H04K, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patentes y de datos de la USPTO y de ESPaNET

El principal hallazgo en este ejercicio de verificación es que se encontraron pendientes negativas, lo que nos indica definitivamente una tendencia a disminuir la intensidad inventiva realizadas en seguridad de la información en medios digitales con respecto al total de TIC's en distintas "clases de patentes representativas", lo que a su vez nos permite corroborar el resultado obtenido en el pasado apartado: existe un desfasamiento en la intensidad inventiva entre: las TIC's y la Seguridad de la Información en Medios Digitales

Este dato es sumamente importante ya que se está identificando que las nuevas tecnologías derivadas de las TIC's son, por su propia naturaleza, inseguras.

Nacen inseguras y se desarrollan inseguras. El análisis de los datos nos permite vislumbrar que, la intensidad inventiva de las TIC's ha creado, por sí mismo, un agente implícito de inseguridad que va arrastrando desde la creación misma de la TIC.

Esto es significativo puesto que ahora se tienen los elementos suficientes para poder asegurar que cualquier estudio de gestión tecnológica debe siempre considerar un grado de inseguridad implícito al uso de las TIC's ya que desde la propia invención de las mismas existe un defasamiento tecnológico, lo que evidentemente aumentará los niveles de inseguridad.

3.4. Hallazgos y conclusiones del capítulo

En términos generales los hallazgos de la investigación presentados en este capítulo son:

1. Los tipos de ataque que provocan inseguridad en la información de medios digitales son consistentes en casi todas las encuestas analizadas, siendo los ataques por virus y la denegación de acceso los más comunes
2. En los tipos de tecnología que inicialmente tenían valores altos, existe una disminución en la frecuencia de los ataques debido, entre otras cosas, a que las

personas responsables de los centros de cómputo están cada vez más preparados para identificar y contrarrestar los ataques, lo que, en otras palabras, muestra la existencia de un aumento en las capacidades tecnológicas dentro de los centros de cómputo e informática de las IES, incluso la presencia de acumulación de capacidades tecnológicas a través del tiempo

3. Los ataques a la información son cada vez más fuertes, en otras palabras, aunque ciertamente hay una menor frecuencia de ataques a través del tiempo, dichos ataques son cada vez más contundentes y sus efectos negativos (económicos, sociales, culturales, etc.) suelen ser más indiscutibles y duraderos, haciendo que el número de personas afectadas vaya en aumento y la sensación de inseguridad también crezca.
4. El aumento en las capacidades tecnológicas y la acumulación de dichas capacidades en los centros de cómputo de las IES, están siendo opacados, de alguna manera, por los elementos y factores que generan inseguridad en la información de los medios digitales.
5. **Generar capacidades tecnológicas en el rubro de seguridad de la información en medios digitales no genera certidumbre suficiente para disminuir la sensación de inseguridad de la información en las IES.**
6. La existencia de capacidades tecnológicas es limitada por parte de las personas que gestionan, operan, monitorean y aplican los sistemas de seguridad de la información en las organizaciones
7. En materia de inseguridad, van aumentando la cantidad de centros de computación que detectan:
 - a. Más de 10 incidencias negativas durante el año
 - b. No tienen idea del origen ni de las consecuencias de los ataques a la información en medios digitales en los centros de cómputo
8. De acuerdo con lo observado, se puede asegurar que existe una tendencia a consumir y confiar más la seguridad de la información a tecnologías reactivas, esto es, evidentemente se está aumentando el uso y consumo de tecnologías reactivas siendo dichas tecnologías de reacción demandantes de menos capacidades tecnológicas para su desarrollo, uso, y aplicación.

- 9. Un hallazgo sumamente importante es que: se puede asegurar que existe una disminución de intensidad inventiva en patentes desarrolladas en seguridad de la información en medios digitales respecto con la generación de TIC's en su conjunto, lo que nos habla de una divergencia tecnológica en este rubro específico.**
- 10. Se tienen elementos suficientes para poder asegurar que, cualquier estudio de gestión tecnológica, debe siempre considerar un grado de inseguridad implícito al uso de las TIC's ya que desde la propia invención de las mismas TIC's existe un grado de inseguridad, lo que evidentemente disminuye los niveles de seguridad en los sistemas de SIeMD.**

C

A

P

I

T

I

L

O

4

*EL CASO DE ESTUDIO DE LA RED NACIONAL DE
SEGURIDAD EN CÓMPUTO (RENASEC)
PERTENECIENTE A LA ASOCIACIÓN NACIONAL DE
UNIVERSIDADES E INSTITUCIONES DE
EDUCACIÓN SUPERIOR (ANUIES).*

4. El caso de estudio de la Red Nacional de Seguridad en Cómputo (RENASEC) perteneciente a La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES).

4.1. Introducción

El presente capítulo tiene como objetivo dar una visión general del objeto de estudio: la RENASEC de la ANUIES, para ello se ha estructurado de la siguiente manera:

Una descripción de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), dando los fundamentos más importantes de su composición y explicando el origen de la Red Nacional de Seguridad en Cómputo (RENASEC).

Otro aspecto importante que se presenta es en lo referente a los flujos de información de la RENASEC, los cuales explican la incursión de los Institutos de Educación Superior IES en la perspectiva de la RENASEC.

Finalmente, se desglosan los elementos reales de la evolución de las capacidades tecnológicas y de gestión tanto de la RENASEC como de las IES asociadas.

4.2. Descripción del objeto de estudio

La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) fue fundada en 1950. Es una asociación no gubernamental, de carácter plural y que agremia a las principales Instituciones de Educación Superior (IES) del país, tanto particulares como oficiales.

Hasta el día de hoy (junio 2006), la ANUIES está conformada por 203 IES, 29% de ellas de carácter público y 71% de carácter privado, lo que representa más del 93% de la matrícula total de alumnos que cursan estudios de licenciatura y de postgrado dentro de la república mexicana.

La ANUIES, además de agrupar a las principales IES del país, tiene como misión contribuir a la integración del Sistema de Educación Superior y al mejoramiento integral y permanente de las instituciones afiliadas en los ámbitos de la docencia, la investigación y la difusión de la cultura, desarrollándose así diferentes iniciativas tanto locales, regionales y nacionales.

Dada su importancia, presencia nacional e internacional y el gran flujo de información que maneja, representa los intereses académicos y administrativos de las IES afiliadas ante las instancias de los poderes ejecutivo, legislativo y judicial, en los ámbitos federal, estatal y municipal ante los organismos públicos y privados, nacionales y extranjeros, relacionados con la educación superior.

La visión/misión de la ANUIES es el punto de partida de nuestro análisis, ya que en ellas podemos identificar el origen de la iniciativa que es el campo de nuestra investigación: “la Red Nacional de Seguridad en Cómputo” RENASEC, cuyo origen esta inspirado en la visión/misión de la asociación y en los objetivos estratégicos institucionales.

En el punto 4, 7, 10 y 13 de la visión de la ANUIES¹ se resaltan los elementos esenciales que dan origen a la RENASEC, los cuales son::

La ANUIES:

- **Es una institución incubadora de proyectos estratégicos que generan cambios y propician el desarrollo sustentable de la educación superior.** En este punto se resalta el carácter incubador de proyectos con una visión estratégica en ayuda a la generación de cambios y desarrollo, lo que sin duda es elemento esencial de la RENASEC
- **Participa activamente en el establecimiento de los estándares de calidad y en los procesos de planeación, evaluación y acreditación de la educación superior.** Este elemento es sumamente importante por dos circunstancias, se habla de estandarización y un elemento de gestión visto desde una perspectiva estratégica (planear, evaluar y acreditar)
- **Ofrece beneficios muy importantes a sus afiliadas, lo que asegura su permanencia e incentiva la incorporación de nuevos miembros.** Iniciativas como la RENASEC ha motivado, a través del tiempo, la incorporación de nuevas afiliadas, las cuales perciben el carácter institucional de la ANUIES por medio de la RENASEC
- **Refleja la heterogeneidad del sistema al responder a los variados intereses o necesidades de las instituciones y de los subsistemas.** En este carácter

¹ La información de la visión y misión de la ANUIES puede ser encontrada en la pagina electrónica http://www.anuies.mx/la_anuies/que_es/vision.php

sistemático se refleja la inquietud de responder a necesidades, entre las cuales la inseguridad de la información en medios digitales en un común denominador entre las IES de todo el país

Asimismo, podemos encontrar dentro de los objetivos estratégicos de la ANUIES² cinco elementos que son fundamentales en la conformación de la RENASEC:

- **Realizar estudios estratégicos sobre la educación superior para prever los cambios, diseñar y concertar políticas, y sustentar la toma de decisiones.** En este caso, la RENASEC ha hecho diversos estudios dirigidos a vigilar y salvaguardar la información y los datos que las universidades hacen llegar a través de la ANUIES
- **Propiciar la complementariedad, la cooperación, la internacionalización y el intercambio académico de sus miembros.** Como se puede observar, uno de los objetivos de la RENASEC, siguiendo con el espíritu de los objetivos estratégicos de la ANUIES, es precisamente la complementariedad, vista desde el punto de vista de acuerdos e intercambios de experiencia, cooperación ínter universitaria e, incluso, la difusión e intercambio de experiencias de orden internacional
- **Aportar soluciones a los problemas de la educación superior y opciones para su desarrollo con calidad en los ámbitos nacional, regional y estatal.** Como se observará a través del estudio exploratorio, es precisamente la inseguridad de la información, uno de los problemas más importantes dentro de las IES.
- **Promover proyectos y actividades interinstitucionales que propicien la convergencia de intereses de las instituciones asociadas en los ámbitos nacional, regional y estatal.** Sin lugar a duda, este punto es el más importante en la concepción y justificación de la creación de la RENASEC
- **Fomentar el intercambio nacional, regional y estatal de información, servicios y personal académico y/o especializado entre las instituciones asociadas para una mejor comunicación y realización de tareas comunes.** Dada la importancia en la seguridad de la información y los elementos que la componen, se hace

² La información de los objetivos estratégicos de la ANUIES puede ser encontrada en la página electrónica http://www.anuies.mx/la_anuies/que_es/objetivos.php

imprescindible no solo el fomentar el intercambio de información, incluso de información crítica e importante, sino también la salvaguarda de la misma.

Como puede observarse, los elementos descritos de la misión, visión y objetivos estratégicos son un punto de partida adecuado para poder entender las iniciativas nacionales basadas en estrategias regionales, que dieron como resultado la formación de la RENASEC dentro de la ANUIES

4.2.1. La organización ANUIES

Para poder desenvolverse de manera eficiente y cubrir las necesidades a nivel nacional, la ANUIES ha desarrollado una estrategia de autonomía regional con un control estratégico centralizado, para ello, y de acuerdo a la normatividad interna, la ANUIES está compuesta por:

- La Asamblea General;
- El Consejo Nacional;
- Los Consejos Regionales;
- Los Consejos Especiales; y
- El Secretario General Ejecutivo

De acuerdo a la normatividad interna, la Asamblea General y el Consejo Nacional conforman la parte estratégica y los Consejos (Regionales y Especiales) así como el Secretario General ejecutivo son la parte de acción operativa a nivel sectorial, dividiendo a todo el país en 6 regiones estratégicas:

- **Región Noroeste compuesta por los estados de:** Baja California, Baja California Sur, Chihuahua, Sinaloa y Sonora;
- **Región Noreste compuesta por los estados de:** Coahuila, Durango, Nuevo León, San Luís Potosí, Tamaulipas y Zacatecas;
- **Región Centro-Occidente compuesta por los estados de:** Aguascalientes, Colima, Guanajuato, Jalisco, Michoacán y Nayarit;

- **Región Centro-Sur** compuesta por los estados de: Guerrero, Hidalgo, México, Morelos, Puebla, Querétaro y Tlaxcala;
- **Región Sur-Sureste** compuesta por los estados de: Campeche, Chiapas, Oaxaca, Quintana Roo, Tabasco, Veracruz y Yucatán;
- **Región Metropolitana de la Ciudad de México** compuesta por: D. F. y áreas conurbanas del Estado de México.

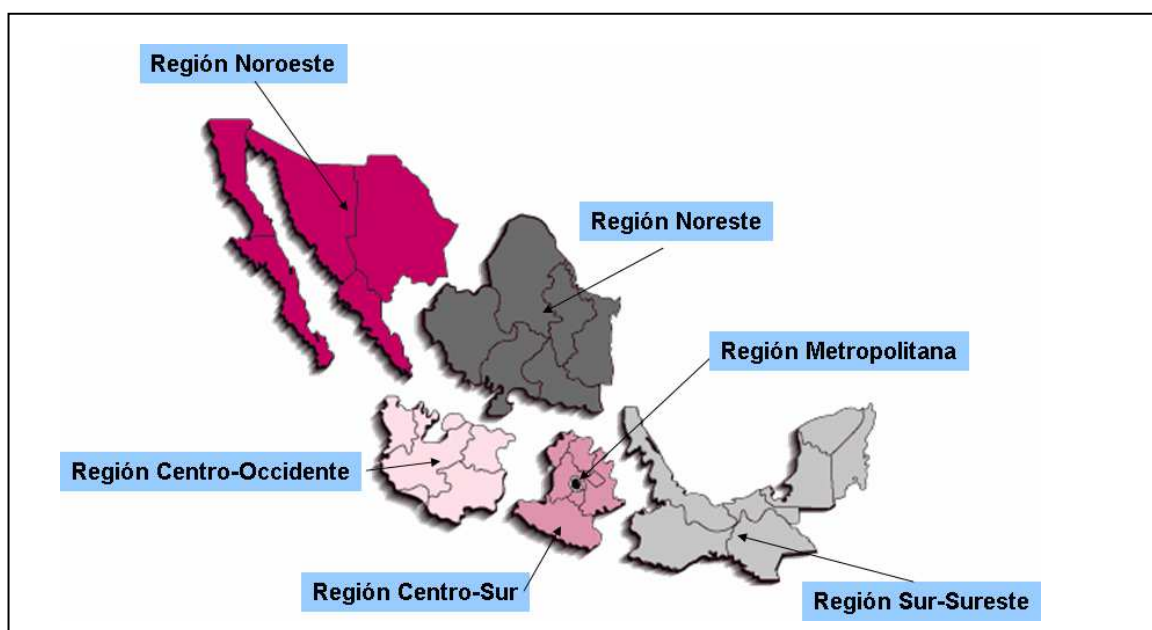


Figura 4.1 Conformación de las 6 regiones estratégicas de la ANUIES

Los proyectos de carácter nacional deben estar estructurados bajo un esquema de integración regional, coordinada por alguna IES asociada, de tal manera que todos los estados y regiones del país sean representados por coordinaciones regionales para que puedan participar de manera activa e inmediata.

4.2.2. El sistema informático de la ANUIES, la Red Nacional de Seguridad en Cómputo RENASEC

La ANUIES, aprovechando la configuración sectorial que posee, ha desarrollado una cantidad importante de iniciativas enfocadas a la promoción de proyectos y actividades interinstitucionales con el fin de propiciar la convergencia de intereses de las instituciones en ámbitos nacionales, regionales y estatales, éste es el caso concreto de la RENASEC

La RENASEC, siendo un proyecto institucional y de carácter nacional emanada de la ANUIES, respeta la misma configuración de regulación y acción regional teniendo puntos de control en cada una de las regiones; así, la conformación actual de la RENASEC tiene una coordinación centralizada en dos agentes: La ANUIES-RENSEC que se encarga de los elementos estratégicos y la UNAM-CERT que se encargan de los elementos técnicos y de avanzada.

Asimismo, se tiene un esquema de coordinación sectorial, cuya estructura está representada por dos o tres IES de la región que canalizan las acciones dictaminadas desde la parte central, brindando cierta autonomía a las coordinaciones. Actualmente (junio 2006) la composición de coordinación de la RENASEC está integrada como se muestra en el Anexo D.

4.3. La Red Nacional de Seguridad en Cómputo RENASEC

El objeto de esta red es el establecimiento de una comunidad académica de seguridad en cómputo que permita proteger y responder de manera adecuada a las emergencias relativas de las tecnologías de información en las instituciones de educación superior del país. En ella se integran las IES que voluntariamente así los solicitaron.

Asimismo, la RENASEC es el organismo de carácter nacional, representativo de la seguridad en cómputo que tiene por objeto normar la participación, coordinación, representación y estímulo de las IES afiliadas a la ANUIES. Dicha red está coordinada de manera conjunta por el UNAM-CERT de la Dirección General de Servicios de Cómputo Académico de la UNAM, y la RENASEC.

La RENASEC es la autoridad máxima en materia de seguridad en cómputo a nivel académico en la República Mexicana porque concentra a las 203 universidades e instituciones de educación superior (IES). Sus objetivos específicos, según su estatuto, son:

- Proteger y responder de manera adecuada a las emergencias relativas de las tecnologías de información en las instituciones de educación superior del país.
- Apoyar en los incidentes de seguridad en cómputo a cualquier miembro de la Red que lo solicite.
- Promover el desarrollo de las tecnologías de información en las IES, en cuanto a la materia de seguridad en cómputo, sistematizando y relacionando las diferentes iniciativas existentes en esta materia en el país.
- Fomentar, supervisar y coordinar el desarrollo de la seguridad en cómputo dentro de las IES del país.
- Autorizar, respetar y hacer cumplir los Estatutos y Reglamentos de las Redes Regionales, de conformidad con las normas establecidas por la propia Red, vigilando el estricto cumplimiento de las normas técnico-académicas correspondientes a las IES.
- Avalar la participación de miembros de la Red en congresos y/o conferencias nacionales o internacionales.
- Apoyar los eventos autorizados y organizados por las Redes Regionales, que hayan sido oportunamente incluidos en su programa de trabajo y aprobados por el Consejo Nacional de la RENASEC.

- Estudiar, adaptar y difundir los procedimientos de enseñanza técnica en materia de seguridad en cómputo.
- Extender los procedimientos de capacitación y enseñanza en todos los aspectos que se requieran a todos los miembros de la RENASEC que lo soliciten.
- Mantener actualizado el registro de sus miembros.
- Proporcionar oportunamente información técnica que contribuya a la mejor difusión, conocimiento y debida aplicación de la seguridad en cómputo.

4.3.1. El medio digital de la ANUIES objeto de estudio

La ANUIES, como cualquier otra organización, tiene internamente diversos flujos de información derivados de los procesos internos y procesos de carácter externo, que en su mayoría son intercambios de información y de relación con las IES asociadas. De todos los flujos de informativos, aquella información que es considerada crítica y estratégica para los objetivos de la ANUIES es la relacionada con las IES agremiadas.

Los flujos informativos se desplazan mediante complejas estructuras de Tecnologías de Información TI hacia la ANUIES, con lo que, desde un archivo, una base de datos, una imagen, un video, etc. puede ser recibida y gestionada desde cualquier IES hasta la ANUIES.

De toda la información que fluye entre las IES y la ANUIES, la que es considerada crítica por su propia naturaleza:

- Los datos e información de identificación de los institutos de educación superior (IES)
- Los datos e información interna de autoridades de cada instituto de educación superior (IES)
- Los datos e información relacionados con los profesores y su situación laboral y de información personal dentro de cada IES
- La información personal y académica de los alumnos de cada IES³.

³ De hecho, la ANUIES como institución debidamente acreditada, certifica la autenticidad de la figura profesional de todos los egresados profesionistas que tramitaron su terminación de estudios en los últimos 20 años

Mediante un proceso estandarizado y certificado, las universidades surten de información confidencial y crítica a la ANUIES, y ésta la gestiona y administra para fines institucionales diversos. En éste modelo, la RENASEC se encarga de la seguridad y salvaguarda del flujo de dicha información.

Este esquema de salvaguarda es obligatorio por norma⁴, ya que en ella se estipula que: tanto los flujos de información crítica interna como los flujos de información crítica de origen externos deben ser controlados y gestionados por un sistema de seguridad de información y gestión de la misma.

4.3.2. Los flujos de información y su seguridad

La manera en que fluye la información de las IES a la ANUIES es clasificada en 2 etapas:

- En la primer etapa, la IES entrega la información a un control administrado por el coordinador regional de la ANUIES
- En la segunda etapa, la información es “capturada o almacenada” y “enviada” al control central de la ANUIES

⁴ La norma a la que se hace referencia es la ISO17799 de seguridad de la información y la ISO9000:2000 de gestión de calidad aplicables a la estructura organizacional de la ANUIES

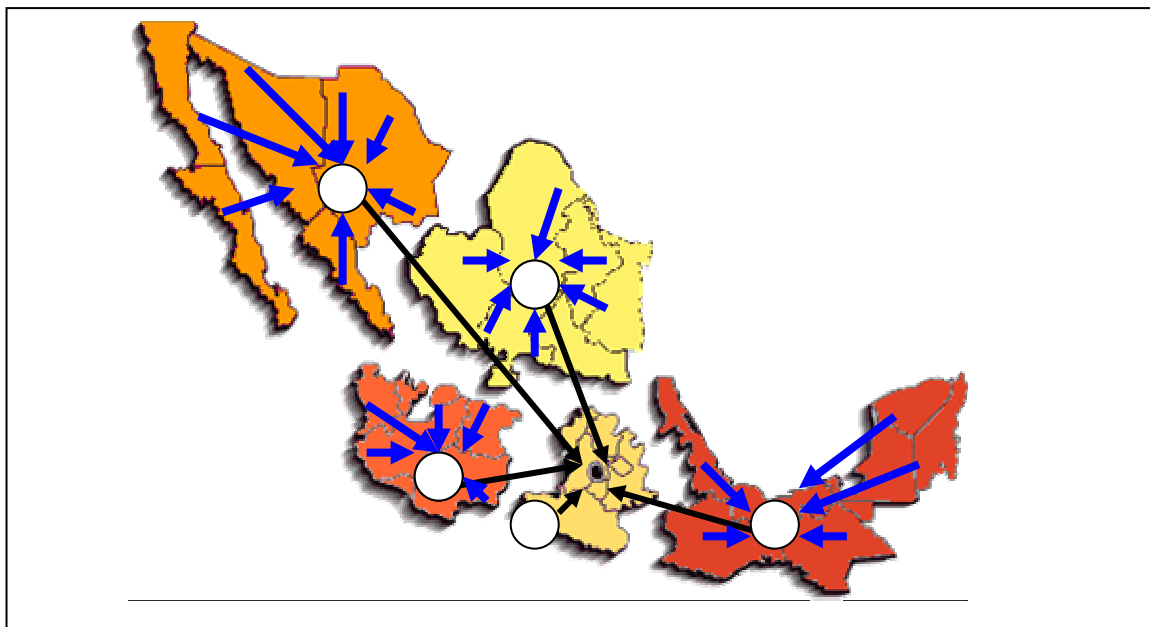


Figura 4.2 Flujos de información de las 6 regiones estratégicas de la RENASEC-ANUIES

De acuerdo a nuestro marco referencia, una adecuada gestión de seguridad debe considerar los puntos donde realmente existe indicio de inseguridad de la información, esto es, los puntos críticos de inseguridad desde que se genera la información en la IES hasta que es depositada en el centro de información de la ANUIES (Figura 4.2), lo que nos lleva a poner atención en tres puntos específicos de seguridad:

- La seguridad en la universidad
- La seguridad en el centro regional de la ANUIES
- La seguridad en el centro de concentración de la ANUIES (que es la RENASEC).

Ya que el centro regional y la RENASEC actúan bajo un mismo patrón de gestión tecnológica, el trabajo se centra en analizar las capacidades de gestión de seguridad de la información de las IES y de la RENASEC.

4.4. Evolución de las capacidades tecnologías de seguridad en las IES y la RENASEC 1999-2006

La mejor forma de disminuir el riesgo asociado con la inseguridad de la información, en medios digitales es aplicando un modelo de gestión tecnológica adecuado, ya que el debe de poder proveer, gestionar y salvaguardar la información, su traslado y su tratamiento.

Dicho modelo prevé la necesidad de contar con un elemento que **vigile y analice** comportamientos específicos fundamentales, que en nuestro caso se enfocan a las tendencias descritas por la evolución y trayectoria tecnológica específica así como las capacidades tecnológicas⁵ a través del tiempo, tanto de las IES como de la RENASEC.

De acuerdo a las entrevistas hechas a lo responsables de los centros de cómputo de las 25 universidades que más han apoyado a la RENASEC en los últimos años, y de las entrevistas hechas al personal de más antigüedad en la RENASEC, la trayectoria y evolución tecnológica puede ser descrita de la siguiente forma:

4.4.1. Una ANUIES insegura (1999 – 2000)

El primer antecedente que se tiene en materia seguridad de la información dentro de la ANUIES nos remonta a mediados de 1999, donde, debido a la alarma generalizada de la posible desconfiguración de los equipos de cómputo debido al cambio de siglo, se programa en la ANUIES una serie de acciones para hacer las adecuaciones, mediciones, análisis y estructuras para así poder estipular el riesgo que tienen las computadoras de la asociación y de la red interna.

La conclusión más importante, derivado del análisis de las instalaciones y del capital humano en la infraestructura organizacional del Departamento de Sistemas de la ANUIES es que dicho departamento no tenía la capacidad humana ni técnica suficiente para poder sobrellevar el posible riesgo derivado del cambio de siglo en la infraestructura computacional⁶.

⁵ Una gestión tecnológica supone capacidades específicas para poder llevarla a acabo de manera eficiente

⁶ En otras palabras, las capacidades tecnológicas y técnicas no son adecuadas para poder dar respuesta a las contingencias que pudiesen derivarse de los problemas en el cambio de siglo

A detalle, el reporte proyecta el siguiente resultado (ANUIES 1999):

- i) La infraestructura humana del departamento de sistemas de la ANUIES se limita a:
 - 1 maestro en sistemas computacionales (que funge como responsable del área),
 - 2 licenciados con una **formación distinta** a “sistemas o computación” que fueron asignadas a este departamento bajo el régimen de fortalecimiento sindical
 - 3 auxiliares que **no** cuentan con formación alguna en sistemas o computación
 - 1 auxiliar administrativo (secretaria)
- ii) La infraestructura técnica del departamento de sistemas:
 - 120 computadoras, de las cuales solo el 20% cuenta con software original y el 80% restante con software pirata
 - No existe un registro confiable de la infraestructura computacional de la ANUIES
 - La única información con la que se cuenta es derivada del departamento de compras el cual tiene un registro de las computadoras y componentes que ha adquirido la ANUIES para el Departamento de Sistemas.

Con base en lo anterior, podemos concluir que la capacidad técnica, tecnológica y humana de la ANUIES se limita a servicios de mantenimiento correctivo y preventivo básicos, lo que ubica a la ANUIES en este año en capacidades que son básicas y pueden ser definidas como de “capacidad operativa”.

En total, en el año 1999 (ANUIES 1999), y debido a limitaciones tanto humanas como técnicas, tecnológicas y de infraestructura, el 100% de las computadoras tuvo al menos 2 asistencias (servicios) por problemas derivados de elementos reactivos, siendo la infección por virus (90% de las computadora), problemas de cambio de siglo (75% de las computadoras) y problemas de configuración (60% de las computadoras) los problemas más frecuentes.

En el año 2000, y debido a la capacidad tecnológica básica medida en 1999, se dieron manifestaciones de inseguridad en la ANUIES, de los cuales los más importantes fueron (ANUIES 2000):

- 10 ataques importantes a los centros de información de la ANUIES (Entre los que destacan:
 - 2 ataques a la página Web
 - un ataque a los informes regionales de las IES de 1999 y a la base de datos general de la IES afiliadas a la ANUIES.
- En el 75% de las computadoras de la ANUIES se presentaron problemas derivados del efecto llamado: “el cambio de siglo”, lo que provocó severos atrasos y problemas en la infraestructura de información.
- En este año los virus provocaron pérdidas de información a los usuarios internos y externos de la ANUIES.

Como respuesta inmediata a estos hechos, la ANUIES toma la decisión de convertir al “Departamento de Sistemas” en la “Dirección de Sistemas Informáticos”, para darle mayor peso específico y que por ende tuviese mayores atribuciones en la toma de decisiones en materia de seguridad y manejo informático, cambiando con ello la infraestructura interna y dando prioridad a:

- La contratación de personas con un perfil técnico avanzado, con lo que la plantilla del departamento se nutre con 2 ingenieros con perfil computacional, 3 pasantes, 2 técnicos y un programa de becas (con lo que se pretendía aumentar las capacidades tecnológicas del área).
- La actualización de los insumos informáticos con lo que se actualizó el 80% de las computadoras. (como una manifestación de transferencia de tecnología e infraestructura del sistema de flujo de información)
- De 80% se redujo al 20% en el uso de software pirata
- La adquisición de servidores que ayudaran a la gestión tecnológica de la información generada internamente.

4.4.2. LA RENASEC (2001-2002)

El balance de enero y febrero del 2001, muestra datos alarmantes (ANUIES 2001); la información que la ANUIES recibe de la IES asociadas (principal activo y producto de la ANUIES) ha sido vulnerable a ataques de origen interno y externo, aumentando la frecuencia y los efectos económicos-institucionales negativos de las mismas⁷.

Existe una preocupación en la Dirección de Sistemas debida a la curva de aprendizaje tan lenta por parte de las personas encargadas de los sistemas de información y de la seguridad de la misma.

Análisis de la ANUIES posteriores (realizados en el mismo año 2001) detectaron que la Dirección de Sistemas y el personal operativo de esta dirección no tenían tiempo suficiente para actualizar o fortalecer sus capacidades técnicas internas en el área de seguridad, ya que el trabajo de dicho departamento era muy extenso.

Entre los mantenimientos correctivos (en promedio 12 al día), los mantenimientos preventivos (13 al día), el desarrollo y mantenimiento de la página Web y los proyectos institucionales, la seguridad de la información se convirtió en un elemento secundario

Dadas las condiciones anteriores, se decidió pedir ayuda a las universidades agremiadas analizándose distintas alternativas de gestión tecnológica en SIeMD.

La alternativa que se vota como mejor es la de incorporar un proyecto nacional de ayuda y gestión tecnológica global en elementos de seguridad informática y que éste sea impulsado por la ANUIES como un programa permanente e institucional, donde participen todas las IES a nivel nacional agremiadas a la ANUIES.

El 30 de Noviembre de 2001, coordinado a través de la ANUIES y el Equipo de de la UNAM-CERT, nace la Red Nacional de Seguridad en Cómputo RENASEC

Para consolidar este esfuerzo a nivel nacional, el 25 de Diciembre y con la participación del 75% de las IES agremiadas a la ANUIES, se da fe, aprobación y conocimiento de la existencia y puesta en marcha de la RENASEC, iniciando una estrategia de gestión/introducción compartida por dos instituciones, en este caso, la UNAM y la ANUIES de la siguiente manera:

⁷ En este periodo bimestral, se detectaron un total de 20 ataques externos exitosos y 12 ataques internos exitosos, lo que equivale a un promedio de 1 ataque cada 48 horas a los sistemas de información de la ANUIES, esto sin contar los ataques que no pudieron ser registrados.

- El elemento estratégico diseñado y gestionado por la RENASEC
- El elemento técnico/tecnológico diseñado y gestionado por la UNAM/CERT (Equipo de Respuesta a Incidentes de Seguridad en Cómputo)

En esta primer etapa, se acuerda como prioridad institucional elevar las capacidades estratégicas principalmente de conocimientos en seguridad y tecnológicas para poder enfrentar posibles problemas de SIeMD, para ello y como primer acción conjunta, se evalúa la necesidad de poseer un primer diagnóstico de las condiciones de seguridad de la información de las IES agremiadas a la ANUIES.

Como resultado, de Mayo del 2002 a Octubre del 2002, bajo un esquema de preguntas específicas a los responsables de los centros de cómputo de las diferentes IES, se programa la aplicación de la primer encuesta nacional para determinar el diagnóstico en SIeMD en las IES agremiadas a la ANUIES.

En las conclusiones de la Dirección de Sistemas de la ANUIES (ANUIES 2001) se pone de manifiesto un aumento en las capacidades tecnológicas internas específicas a la seguridad de la información debido a las interrelaciones y al intercambio de información entre la UNAM/CERT y la RENASEC, sin embargo, son éstas capacidades limitadas para poder reaccionar a las contingencias informáticas, con un bajo nivel de planeación estratégica y una casi nula gestión tecnológica de la información.

Entre los elementos mas destacados de la primer encuesta nacional se encuentra:

El diagnóstico fue contestado por 102 universidades agremiadas (75% del total), dando los siguientes resultados trascendentes:

- Solamente el 52% de las universidades tiene instalaciones y personal apropiado para poder hacer frente a alguna contingencia o problemática computacional, lo que de acuerdo al punto 1.2.2, indica que casi la mitad de las IES tiene potencialmente poca (o nula) capacidad tecnológica.
- Únicamente el 45% de las Universidades asegura tener personal capacitado, lo que nos indica que existe un 55% de las IES con un atraso significativo respecto a las capacidades técnicas y obviamente un mayor porcentaje en atraso de capacidades tecnológicas.

- Solamente el 10% de las IES tiene al día algún tipo de bitácora de problemas relacionados con la información digital.
- El 17% de las universidades reporta conocer y aplicar algún tipo de normatividad en seguridad de la información en medios digitales, sin embargo de éstas, solamente el 64% supo decir cual o que tipo de normatividad usaban.
 - Solamente 3 universidades tienen un certificado de seguridad de la información
 - Técnicamente el mayor problema es también reflejo de la falta de capacidades centrales (punto 1.2.1 de la presente tesis) específicas, ya que el 71% de las IES reporta malas configuraciones en sus sistemas de información
 - Los resultados totales pueden ser consultados en el anexo E

Las conclusiones de la Dirección de Sistemas y responsable de la RENASEC dan como conclusión general de la encuesta de seguridad informática 2002, la existencia de problemas derivados de faltas de capacidad e infraestructura dentro de las IES y que conllevan a inseguridad informática.

Como resultado de ello, para el año siguiente (2003) se planea una serie de conferencias, congresos y talleres enfocados a dos aspectos: aumentar el nivel de seguridad de la información en las IES y aumentar las capacidades técnicas/tecnológicas tanto de las IES agremiadas como de la RENASEC.

Para ello se sugiere aprovechar la infraestructura propia de la ANUIES como una institución no gubernamental, nacional y con un campo de acción sectorial para que pudiese otorgar facilidades en la ejecución, logística, recursos humanos y técnicos para conseguir los primeros objetivos de la RENASEC/ANUIES.

4.4.3. La gestión Tecnológica en la RENASEC (2003-2006)

A partir de enero del 2003, la RENASEC da prioridad a programas de capacitación y talleres enfocados a elevar las capacidades tecnológicas en materia de seguridad de la información a nivel sectorial.

Apoyados en programas de capacitación de 30 a 120 horas distribuidos de la siguiente manera:

- 2 programas nacionales de capacitación-taller continua que se gestionaban en las sedes de las universidades regionales coordinadoras de la RENASEC.
- 1 programa de talleres en seguridad impartido por la ANUIES con carácter nacional.
- Asignación de recursos al “V Congreso de Seguridad” organizado por la UNAM, donde los miembros agremiados de la ANUIES contaron con descuentos tanto en el congreso como en los talleres impartidos.

En la búsqueda de tener un registro del aumento en las capacidades internas en las IES y de la ANUIES, se implementó un monitoreo de los resultados derivados de las acciones descritas anteriormente, el resultado mas importante fue que, a mediados del 2003 disminuyó a casi el 50% los problemas de SIeMD dentro de la ANUIES, y el impacto económico de ellos se redujo 75%.

Sin embargo, en las IES y los talleres de capacitación de la RENASEC se presentaron diversos problemas que limitaron el maximo aprovechamiento de los programas.

Dado lo anterior, en las conclusiones de la RENASEC de ese año (ANUIES 2003) resalta los siguientes hechos:

- La RENASEC ha tenido problemas de coordinación y gestión con respecto a las regiones, entre los principales problemas se tienen:
 - Poca difusión entre las IES de los talleres y los programas de capacitación, lo que dio como resultado una pobre asistencia a los talleres regionales (menos del 25% de las IES agremiadas a la ANUIES en promedio siendo la región norte la más pobre en asistencia con el 12% y la región sur-sureste la más activa con el 40%)

- Por la poca participación se cancelaron los 2 programas nacionales de capacitación-taller continua que se gestionaban en las sedes de las universidades regionales
- El programa de talleres en seguridad impartido por la ANUIES, con carácter nacional, fue la de mayor éxito con 75 participantes
- El congreso de seguridad organizado por la UNAM fue el de mayor impacto (170 personas relacionadas con la RENASEC, entre ponentes, investigaciones y participaciones)

Es en este momento cuando se analizó cuáles habían sido los factores de éxito y de fracaso en las acciones y los objetivos de la RENASEC, dando como conclusión la no incorporación de planes enfocados a una **gestión tecnológica** adecuada, se decide así planear la creación de un grupo que trabaje sobre la gestión de seguridad de la información y que fuese manejado desde la RENASEC. Se da así pie a la creación del Grupo de Gestión de Seguridad de la Información de la RENASEC.

Una decisión tomada por este grupo fue la de no permitir la participación de las empresas privadas en las acciones internas de la RENASEC para no contaminar la infraestructura de las acciones entre la ANUIES y la UNAM-CERT, ésta decisión fue muy cuestionada, ya que las IES argumentaban no tener recursos internos suficientes para poder participar en las acciones que la RENASEC organizaba, y que la única fuente de recursos externos eran las Empresas Privadas.

Es entonces que las distintas regiones de la RENASEC se fragmentan, lo que a la larga provoca el nacimiento de otras organizaciones que aceptan el apoyo de la iniciativa privada⁸, lo que debilita la posición y liderazgo de la RENASEC a nivel nacional.

La conclusión en el reporte de diciembre de este año (ANUIES 2003) es una mejora en la capacidad técnica/tecnológica interna de la ANUIES en casi un 60%, y un aumento en las capacidades internas centrales y capacidades técnicas/tecnológicas de las IES en casi un 12%, datos que son tomados de manera muestral, lo que obliga a planear un nuevo diagnóstico de seguridad en las IES

⁸ Entre las organizaciones más representativas se encuentran: CUDI Corporación Universitaria para el desarrollo de Internet por parte de secciones metropolitanas, End to End de la Universidad de Guadalajara, NOCUDI Centro de operación de la red CUDI (Tijuana, Monterrey, Cancún, D.F, Guadalajara

**4.4.3.1.Periodo de Gestión Tecnológica en seguridad de la Información
UNAM-RENASEC**

Gracias al apoyo de la UNAM-CERT, y del 60% de las IES agremiadas a la ANUIES, se da seguimiento a las acciones planeadas para el 2003.

La RENASEC decide replantear los objetivos principales dando prioridad al logro de una adecuada gestión tecnológica en las IES agremiadas.

Para ello y como primera acción, se planeó la realización de un nuevo diagnóstico, teniendo como prioridad los indicadores en materia de administración de la seguridad de la información, gestión tecnológica, gasto en infraestructura y capacitación, así como la realización y aplicación de normatividades internas.

Este segundo diagnóstico de seguridad aplicado a las IES dio los siguientes resultados:

- El diagnóstico fue aplicado por el 71% de las universidades agremiadas (125 en total)
- Los resultados más importantes son los siguientes:
 - Aumentó el porcentaje de universidades con infraestructura adecuada para poder resolver contingencias, pasando del 52% en el 2002 al 65% en el 2004, lo que indica un fortalecimiento en las capacidades tecnológicas de las IES asociadas a la ANUIES, sin embargo, todavía el porcentaje es muy pequeño.
 - También existe un aumento en el porcentaje de personal capacitado para la seguridad de la información en medios digitales, pasando del 45% al 53%, lo que indica un aumento en las capacidades tecnológicas, aunque todavía el porcentaje es muy bajo
 - El inciso en donde se manifestó un aumento significativo es en el porcentaje de IES que hace un reporte de los problemas de inseguridad que se van presentando, pasando de 10% en el 2002 al 59% en el 2004, aumento razonable y que nos indica una mayor conciencia en los problemas de inseguridad y sus efectos negativos. Sin embargo, la distribución de este porcentaje, indica que solamente el 15% del total de

las IES hace un reporte semanal o inmediato al detectar problemas de inseguridad, dejando el 10 % a reportes mensuales y el resto a reportes anuales o no reportes. Este dato es sumamente interesante porque un reporte anual o un no reporte también es un indicador de falta de capacidad en la respuesta a problemas de seguridad de la información.

- El 33% de las universidades dice conocer y aplicar algún tipo de normatividad en seguridad de la información en medios digitales, lo que significa un aumento al 17% detectado en el 2002, de este 33%, el 90% supo decir qué tipo de normatividad usó
- En el 2004, solamente doce IES tienen un certificado de seguridad de la información
- En este nuevo diagnóstico, ha sido trascendente la preocupación por saber si existe alguna persona dedicada exclusivamente a la gestión tecnológica en seguridad de la información en medios digitales, el resultado obtenido es que solamente 5 IES tienen esa figura específica; Es interesante éste dato por 2 cosas, primeramente porque del 80% reportado solamente el 50% (40% del total) tiene una formación en seguridad de la información, o sea que el resto son personas con perfiles limitados en seguridad de la información, por otro lado, se evidencia una falta de visión específica en la concepción de gestores tecnológicos específicos

De acuerdo al anuario de ANUIES (2004) las conclusiones de la RENASEC resaltaron varias cosas importantes:

Evidentemente existe una mayor capacidad técnica/tecnológica relacionada con la seguridad de la información en medios digitales en las IES, resultado de acciones implementadas por la ANUIES/RENASEC y por esfuerzos internos de las IES, sin embargo, aunque existe una mejoría, de ninguna manera se puede hablar de un problema resuelto, por lo que para el 2005 se deben seguir dando facilidades a las IES agremiadas para el fortalecimiento tanto de las capacidades Técnicas/Tecnológicas internas, como de las capacidades gerenciales y de gestión tecnológica que, como se observó en el diagnóstico del 2004, son prácticamente inexistentes.

Es en este punto donde se resalta la preocupación por entender los elementos más significativos en materia de gestión tecnológica por parte de la RENASEC, lo que lleva a fortalecer la infraestructura interna de la ANUIES.

4.4.3.2. La exigencia de seguridad de calidad en la ANUIES y la RENASEC

A principios de enero del 2004 sucede un evento fundamental en la trayectoria tecnológica en seguridad de la ANUIES. Dado el fortalecimiento de la Federación de Instituciones Mexicanas Particulares de Educación Superior (FINPES) como órgano regulador de la calidad de la educación en escuelas tanto particulares como oficiales, se da la iniciativa en la Secretaría de Educación Pública (Diario Oficial de la Federación enero 2004) de que, dada la infraestructura organizacional de la ANUIES, de su importancia y liderazgo a nivel nacional, en acciones por la seguridad de la información digital a nivel nacional y con la experiencia en el manejo de datos:

- *Se otorgue a la ANUIES la responsabilidad de gestionar y manejar, de manera institucional y a nivel nacional, la información crítica de las IES, esto es, la información académica de todos los alumnos y exalumnos de las IES agremiadas a la ANUIES, esto con el fin de que la ANUIES funja como responsable institucional nacional de este tipo de información.*

La ANUIES acepta y para poder cumplir con las exigencias particulares en materia de seguridad, planea e implementa 2 acciones enfocadas a la SIeMD tanto en la ANUIES como las IES asociadas:

- El fortalecimiento de las tecnologías de información internas de la ANUIES (nuevamente con adquisición de infraestructura computacional, adquisición de una red inalámbrica general, transferencias y aplicaciones tecnológicas de punta, inclusión de la Dirección de Sistemas de la ANUIES a los esfuerzos de normatividad ISO9001:2000, etc)
- El fortalecimiento de tecnologías relacionadas con la comunicación y flujos de datos de las IES agremiadas con la ANUIES, sin la necesidad de pasar por filtros regionales.

Dichas acciones suponen el fortalecimiento de las capacidades internas (tecnológicas, centrales, de gestión, etc) tanto de la ANUIES, como de las universidades agremiadas (IES). Para ello, se plantea una estrategia enfocada a determinar cuales son las acciones de fortalecimiento en las capacidades tecnológicas de las IES que se requieren para garantizar el transporte (flujo) de la información y conocimiento de las IES a la ANUIES. Dicho análisis dio como resultado, la implantación de programas por parte de la gestión tecnológica de la RENASEC, los cuales son, a detalle:

- Un programa de continua capacitación en el uso de tecnologías de información
- Programas de capacitación enfocados a la creación de capacidades organizacionales internas hacia las IES
- Programas de capacitación y formación de Gestores Tecnológicos para las Universidades
- Fortalecimiento de la RENASEC como el órgano institucional más importante en materia de seguridad de la información en medios digitales
- Estructuración de planes estratégicos específicos que determinen las fortalezas y debilidades de las IES asociadas a la ANUIES en materia de seguridad de la información en medios digitales con base a experiencias previas
- Revisión de tendencias en tecnología (trayectoria de las tecnologías informáticas) a nivel local y a nivel mundial (Capítulo 3 de esta tesis)
- Análisis de la factibilidad del proyecto
- Proyección de los costos y beneficios a corto mediano y largo plazo
- Programación del 3er diagnóstico de seguridad en las IES, con un enfoque específico a gestión tecnológica.

Otra preocupación es precisamente la de determinar las trayectorias tecnológicas, con lo que se pudiera garantizar la seguridad en el flujo de información crítica y conocimiento entre las IES y la ANUIES, por ello se programó para principios del 2006 acciones concretas para el óptimo diagnóstico de la seguridad de la información en medios digitales, tomando como puntos de referencia las encuestas realizadas en el 2002 y 2004.

Sin embargo, el cambio de autoridades realizada en el 2005 retrasó mucho algunas de las acciones programadas para este año. No obstante, las nuevas autoridades dieron luz verde a los proyectos programados y presionaron para la implementación de nuevos proyectos que complementaron el fortalecimiento de las tecnologías de información tanto internas como externas.

Para el año 2005, en la RENASEC se fijaron objetivos específicos para determinar la trayectoria, evolución y capacidades tecnológicas de las IES asociadas y de la RENASEC, con lo que se dio prioridad al tercer diagnóstico de seguridad computacional en las IES.

Para lograr de manera mas óptima los resultados esperados, el diagnóstico se programó en 3 etapas:

- 1er etapa (5 diciembre 2005 al 15 mayo de 2006): aplicación de un cuestionario exploratorio al menos a 30 IES representativas de nuestro país en materia de seguridad de la información en medios digitales, el resultado del cuestionario servirá como base a la encuesta que se aplicará a nivel nacional. (El cuestionario se describe en el Anexo E):
 - Dicho cuestionario será almacenado en formato digital para referencias y dudas posteriores
 - El cuestionario será aplicado a dos figuras: el responsable técnico de seguridad o del departamento de cómputo y/o sistemas de la IES y al responsable institucional de la IES ante la ANUIES
- 2ª etapa (15 de mayo al 15 de junio de 2006): aplicación del cuestionario a las IES agremiadas a la ANUIES
 - Interpretación de los resultados
 - Examen DOFA
- 3ª Etapa (por determinar): Estructuración de un plan de gestión tecnológica que garantice la seguridad y salvaguarda de la información que se transfiera de la IES a la ANUIES, y asimismo

garantice y salvaguarde el uso de dicha información en la ANUIES por medio de la RENASEC.

Es importante hacer esta distinción ya que este diagnóstico será estructurado y aplicado para determinar, además de elementos puramente técnicos a la SIeMD, también elementos específicos de la gestión tecnológica de la seguridad de la información dentro de las IES agremiadas a la RENASEC

4.5. Hallazgos y conclusiones del capítulo

Los hallazgos y conclusiones más importantes del capítulo se pueden resumir en los siguientes puntos:

1. El origen de la RENASEC está inspirado en los estatutos, misión y visión de la propia ANUIES, por lo que su conformación tiene fuerza e ingerencia nacional e institucional
2. Para su óptima aplicación, la RENASEC trabaja bajo el esquema estratégico de la ANUIES, con una configuración regional
3. Se pueden distinguir en etapas progresivas a la RENASEC, lo cual ayuda a poder identificar la evolución histórica y específica de la misma:
 - a. El origen de la RENASEC
 - b. Primeras acciones
 - c. La RENASEC y las IES
 - d. La gestión tecnológica de la seguridad en la RENASEC
 - e. La gestión tecnológica de la seguridad en la RENASEC y las IES
4. Derivado de la evolución histórica y de las acciones realizadas:
 - a. Existe continuamente redefiniciones en los objetivos generales y la misión de la RENASEC
 - b. Evidentemente existe un aumento en la capacidades tecnológicas tanto en la ANUIES como en las IES, sin embargo, en las IES se pueden encontrar contrastes muy marcados en este aspecto

- i. IES muy por encima de los estándares de seguridad de la información
 - ii. IES muy por debajo de los estándares de seguridad de la información
 - iii. Más del 60% de IES por debajo de los estándares en seguridad de la información
- c. Existe un aumento en las capacidades de gestión tecnológica tanto en las IES como en la RENASEC, al respecto.
 - i. También se encuentran marcadas muchas diferencias en este particular, principalmente por las características y los intereses tan diversos entre las IES
 - ii. La mayoría de las IES se ha preocupado principalmente en aumentar sus capacidades tecnológicas, pero no el aumentar sus capacidades de gestión tecnológica, aunque evidentemente existe aumento, no es tan fuerte como en las capacidades tecnológicas

C

A

P

I

T

I

L

O

5

*GESTIÓN TECNOLÓGICA DE SEGURIDAD DE
INFORMACIÓN EN MEDIOS DIGITALES.
EL CASO DE LA RENASEC PERTENECIENTE A LA
ANUIES*

5. Gestión tecnológica de seguridad de información en medios digitales. El caso de la RENASEC perteneciente a la ANUIES.

5.1. Introducción

El objetivo del presente capítulo es el mostrar los elementos fundamentales del proceso de Gestión Tecnológica que inciden en la RENASEC de la ANUIES y en las IES asociadas, analizando los resultados obtenidos en las gráficas cruzadas de capacidades tecnológicas y capacidades de gestión tecnológica tanto en la RENASEC como en las IES asociadas.

El presente capítulo es el más importante de toda la tesis, esto por que resume, analiza y concluye las evidencias más importantes de la investigación y estudio de campo.

5.2. Gestión tecnológica

Como ya se ha mencionado, la gestión tecnológica debe sustentarse en 5 puntos esenciales, mínimos más nunca suficientes:

- a) Vigilar y analizar
- b) Focalizar
- c) Capacitar
- d) Implantar
- e) Aprender

Además, de apoyarse con elementos reales para contrastar y analizar resultados, dichos elementos reales pueden ser extraídos de las preguntas específicas realizadas en las encuestas nacionales aso como en las entrevistas personalizadas de la presente investigación.

5.2.1. Vigilar y analizar el elemento tecnológico (trayectorias y capacidades tecnológicas)

El proceso de vigilar y analizar el elemento tecnológico debe contemplar los elementos tecnológicos de ambas organizaciones (las IES y la RENASEC), ya que esto es significativo para poder concebir una gestión tecnológica adecuada.

Para ello, nos debemos concentrar específicamente en 2 puntos:

- a) Los elementos empíricos específicos referentes a las encuestas realizadas en las universidades en los años 2002, 2004 y 2006, y cuyo resultado se puede ver en la tabla 5.1, que dan sustento empírico a esta tesis.
- b) Las trayectorias tecnológicas y su evolución en las IES y la RENASEC.

5.2.1.1.Elementos empíricos de las encuestas realizadas en los años 2002, 2004 y 2006

Analizando las encuestas de los años 2002, 2004 y 2006, se hace evidente en su evolución que existe una mejoría en el elemento de vigilancia y análisis de problemas dentro de las IES con elementos de seguridad de la información en medios digitales.

Los hallazgos más importantes que se encontraron en las encuestas de seguridad nos indican que, a través del tiempo, ha aumentado la preocupación por la seguridad de la información de las IES agremiadas a la ANUIES, lo que ha llevado a un incremento en la aplicación de modelos de gestión de seguridad de la información pasando de 40% de las IES con un modelo de gestión de seguridad de la información en el 2002 al 75% en el 2006.

Este dato no significa necesariamente que por el hecho de que existe la aplicación de un modelo de gestión de la seguridad éste sea eficiente, ni que se garantice propiamente la seguridad de la información, sin embargo, sí habla al menos de un aumento de recursos destinados a la seguridad de la información.

Cabe aclarar que el mayor volumen de gasto (inversión) de las universidades en el rubro de sistemas (computación, informática, etc) evidentemente está destinado a la compra de computadoras e insumos informáticos, dejando a la seguridad como cuarta y hasta quinta prioridad en el rubro de “gastos del departamento de sistemas”, este dato es importante de considerar puesto que, siendo la información elemento fundamental en una Universidad, llama la atención que el gasto en seguridad y salvaguarda de la información y los datos no sea uno de los rubros más importantes.

Respecto a la percepción en las IES del nivel de gestión de seguridad de información en medios digitales que poseen internamente, existe también una mejoría; pasando de ser predominantemente bajo (70% de las IES con nivel bajo en el 2002) a ser

predominantemente medio (45% de las IES con nivel bajo en el 2006), lo que concuerda con lo observado en la revisión de la evolución.

Ya se ha apuntado que, de manera perenne, existen IES que pueden considerarse por encima de la norma de seguridad de la información e IES que se pueden considerarse por debajo de la norma de seguridad de la información de manera incluso homogénea y consistente a través de las distintas regiones de la ANUIES.

5.2.1.2. Trayectorias tecnológicas (seguridad de la información) y su evolución

La evolución en la trayectoria tecnológica (de seguridad de la información) mostrada por las IES y la RENASEC, muestra una tendencia hacia la homogenización tecnológica¹, hecho que, de acuerdo a la teoría de la convergencia es un elemento no solo generalizado en las TIC's sino que normal en este tipo de tecnología específica.

Sin embargo, y pese a la existencia de una homogenización tecnológica, la evidencia muestra también diferencias marcadas en la evolución de las capacidades tecnológicas entre IES². Esto nos lleva a encontrar IES que sobrepasan los niveles mínimos de seguridad informática recomendados (Como el Tec de Monterrey en cualquiera de sus campus, la UNAM, la U de G, la UA de G y el IPN), como IES que están muy por debajo de los niveles de seguridad mínimos recomendados (U. de Colima, la U. del Istmo de Tehuantepec, la U. de Chiapas, la U. Insurgentes, etc).

Asimismo, y analizando la misma información, se pueden encontrar elementos específicos interesantes para el entendimiento de orden tecnológico. Un ejemplo de ello son las características empíricas resultantes a nivel sectorial (encontradas en la Encuesta Nacional de Seguridad Informática de la RENASEC, 2006) los cuales no muestran, como

¹ Debemos recordar que hablar de homogenización tecnológica en seguridad de la información (y en ocasiones en las TIC's en general) implica que las características, los métodos, incluso los resultados derivados de las acciones de seguridad, concurren a un punto de estabilidad, que si bien no podemos manejar como óptimo, podemos considerar como representativo del conjunto de tecnológicos que se está tratando

² Diferencias que son constantes a través de los años y que pueden ser explicadas por diversos factores, entre los cuales podemos encontrar, recursos económicos, prioridades institucionales, infraestructura interna, capacidades específicas no desarrolladas; entre muchas otras que fueron evidenciadas en las entrevistas hechas a lo largo de la investigación

podríamos suponer, alguna marcada tendencia de inseguridad en alguna región en específico³, ya que todas las regiones muestran, de manera por demás consistente, IES muy por arriba de los niveles mínimos de seguridad informática recomendados e IES muy por debajo de los niveles mínimos de seguridad informática recomendados, incluso de manera proporcional (Los resultados nos muestran que en promedio a nivel sectorial el 30% del total de IES está muy por debajo de la norma, 15% del total de IES está muy por arriba de la norma y el 55% del total de las IES está cercana a la norma).

Resultados muy parecidos pueden observarse no solamente en las capacidades técnicas/tecnológicas, sino al nivel de seguridad de la información que poseen las IES en el país.

Sin embargo, quizá el hallazgo más importante encontrado en las entrevistas personales hechas en las universidades evidencian que, derivado de las propias características de la tecnología de la información y de la observación de la evolución en la trayectoria tecnologías de los riesgos y amenazas informáticas vistas en los capítulos anteriores, podemos asegurar que existe una evidente reducción del ciclo de vida de los productos relacionados con la seguridad de la información en medios digitales; esto es, el diseño de estos producto se convierten en obsoletos cada vez con más rapidez con la que su funcionalidad, aplicabilidad y uso es superado por dos elementos:

1. La introducción de nuevos productos en el mercado.
2. La existencia de esquemas de inseguridad que hacen inoperable o poco seguro el producto usado y que por ende tiene que ser reemplazado o actualizado⁴

En estas circunstancias, tenemos dos efectos inmediatos:

1. Las organizaciones (por ejemplo las IES) deben tener esquemas eficientes de vigilancia tecnológica, pero sobre todo flexibles a los cambios en materia de seguridad de la información, cosa que se encuentra de manera “pobre” en las IES entrevistadas.

³ Podríamos suponer que en regiones sin gran avance industrial o sin gran infraestructura educacional como universidades o centros tecnológicos (Como en el hemisferio sur de México) presentarían retrasos en las capacidades tecnológicas específicas. Rozga, L (2004)

⁴ Esta característica es muy común en productos conocidos comúnmente en el mercado, los dos ejemplo más evidentes son los antivirus (como Mcfee, Norton y Panda) y los programas computaciones y los sistemas Operativos (Como Windows)

2. Los proveedores que quieran mantenerse competitivos debe ser más eficiente que antes y aprovechar mejor sus recursos tecnológicos, ya que de no hacerlo seguramente aparecerá en el mercado un nuevo proveedor (competencia) que pueda garantizar la seguridad de la información dentro de las IES.

5.2.2. Focalización

Está claro que, teniendo un objetivo bien definido se puede lograr tener éxito en la gestión tecnológica encomendada, esto auxiliado con una estrategia que tenga un enfoque tecnológico adecuado (focalización), con esta base, el objetivo de la gestión tecnológica debe estar seguido del apoyo de las personas que puedan llevar a cabo dichos objetivos y que, además, gestionen y planeen las actividades adecuadas para llevar a cabo la estrategia.

Es evidente que la RENASEC y las IES, de acuerdo a la revisión de sus trayectorias, han cambiado sus objetivos continuamente. En el año 2002, por ejemplo, la prioridad en los objetivos era tener elementos relacionados con programas de capacitación, para el 2004 el objetivo principal cambió radicalmente al priorizar los elementos técnicos/tecnológicos para tener un aparato de intercomunicación y de flujos de información entre las universidades; de la misma manera, en el 2006 el objetivo era el de fortalecer a la RENASEC como una institución líder y afianzarse en esta posición.

Analizando estos elementos, se hace evidente la existencia de agentes (internos y externos) que provocan cambios continuos en el planteamiento de los objetivos generales tanto en la RENASEC como en las IES, debilitando con esto una posible estrategia a largo plazo.

Asimismo, de acuerdo a las entrevistas personales de los miembros de la RENASEC, otro aspecto importante es que si bien las características internas y externas de la ANUIES van dictando año con año las prioridades tanto de la Dirección de Computo como de la misma RENASEC, elementos como las condiciones políticas propias de la ANUIES, los recursos humanos, el financiamiento económico, otras tareas de la dirección de sistemas de la ANUIES, las implementaciones computacionales prioritarias, los cambios de configuración en la red interna, la falta de recursos, las capacidades mismas del personal

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

y los proyectos institucionales, son algunos elementos que pueden cambiar los objetivos y prioridades específicas de la RENASEC.

De acuerdo a las entrevistas con las universidades, en la investigación se encontraron aspectos, semejantes a los observados en la ANUIES, que influyen en la modificación o concepción de objetivos en materia de seguridad, siendo los aspectos económicos y de capacidades los más comunes.

En una gestión tecnológica adecuada, las recomendaciones teóricas descritas nos indica que preferentemente se deben de tener objetivos enfocados al largo plazo; asimismo, los objetivos a corto plazo deben ser mucho más flexibles y dependientes de las características propias del medio ambiente. Sin embargo, y pese a lo anterior, no se debe perder de vista que el objetivo principal (al corto mediano y largo plazo) de la RENASEC debe ser la seguridad y salvaguarda de la información, para poder hacer factible su manejo, consulta, modificación autorizada, etc; cualquier estrategia de gestión tecnológica en SIeMD debe de partir bajo este supuesto.

Otra particularidad es que dicha estrategia debe ser compartida con los demás IES, esto es, los objetivos y los planteamientos estratégicos deben ser compartidos por las personas y las instituciones involucradas. Este punto es sumamente importante, ya que esto significa que tanto la RENASEC como las IES asociadas deben estar concientes de que el elemento fundamental en la estrategia de gestión tecnológica debe estar orientada a homogenizar no solamente las capacidades tecnológicas y el nivel de gestión tecnológica, sino los objetivos comunes y sobre todo el objetivo general⁵.

Analizando este asunto de la estrategia, en particular, la evidencia empírica resultado de esta investigación puede ubicar cuando menos 2 aspectos fundamentales: Los objetivos y La dirección

⁵ En otras palabras, homogenizar es hacer coincidir los objetivos de gestión tecnológica entre las IES y la RENASEC para poder disminuir la incertidumbre y aumentar el nivel de seguridad entre ellas

5.2.2.1.Los objetivos

Como ya se mencionó, los objetivos relacionados con la seguridad de la información, tanto de la RENASEC como de las IES, han cambiado constantemente; al menos se tienen 3 registros de ello: en 2002, 2004 y 2006.

Asimismo se detectaron cambios en los objetivos internos de las IES respecto a la seguridad de la información; en ello: las prioridades, los métodos y herramientas usadas, la autonomía de las universidades en su campo de acción y otros aspectos determinantes varían de IES a IES.

La evidencia empírica nos revela que si bien es cierto que en el 2006 más del 70% de las universidades tienen objetivos relacionados con seguridad informática, más de tres cuartas partes de las universidades están convencidas que las acciones realizadas no son suficientes para garantizar dicha seguridad

Existe una preocupación creciente del tema de seguridad en las IES (del 19% en el 2002 al 60% en el 2006, de acuerdo con la Tabla 5.1) sin embargo, no se registra la misma intensidad de cambio en la formulación de objetivos dinámicos ni en las estrategias de seguridad internas a las IES⁶

Evidentemente, este elemento es una limitante en la focalización estratégica de la gestión tecnológica de la RENASEC respecto a las condiciones internas de las IES

5.2.2.2.La dirección

Toda estrategia corporativa, institucional, educacional, etc debe de involucrar directamente a la parte directiva para poder obtener los efectos positivos deseados, ya que en ausencia de este elemento cualquier estrategia podría carecer de apoyo estructural adecuado.

⁶ En la investigación se evidenció que, como ya se ha mencionado en la tesis, existen un porcentaje cercano al 30% de universidades cuyas características internas no podrían garantizar siquiera un esquema básico de seguridad de la información, y más de la mitad de las IES necesitarían de asesoría especializada para poder conformar adecuadamente estrategias que fuesen acordes con la estrategia de gestión tecnológica de la RENASEC.

De acuerdo a la evidencia empírica, existe un conocimiento de la dirección de las actividades de gestión de seguridad de la información, pasando del 12% al 35% en el periodo del 2002 al 2006 (Tabla 5.1); sin embargo, analizando estos datos y considerando la importancia de la información en las IES y de los efectos nocivos que se pueden derivar de su inseguridad, 35% es un número muy pequeño

Es verdad que las entrevistas personales nos revelaron que, aunque la dirección no estuviese enterada de las actividades de la gestión, eso no significaba necesariamente que hubiese rechazo de la problemática por parte de la misma dirección, o que no hubiese apoyo (de hecho la misma encuesta revela que existe apoyo); sin embargo, experiencias en otros ámbitos nos demuestran que cuando la dirección no tiene conocimiento de las acciones de gestión, dichas acciones van deteriorándose poco a poco hasta el grado de ser jerárquicamente poco importantes para la institución⁷.

Aquí existen dos datos contradictorios respecto a la dirección y la estrategia de gestión de seguridad de la información: por una parte, la encuesta (Tabla 5.1) evidencia que la dirección participa en las actividades, apoya con recursos y apoya las acciones en alrededor del 60 - 70% de las IES, por el otro, las entrevistas a las IES revelan que la prioridad de estas acciones están, en promedio, entre el lugar 30 y 35 de los objetivos institucionales, lo que nos indica que, sí, existe un compromiso por parte de la dirección pero dicho compromiso tiene una prioridad limitada en la mayoría de los casos.

5.2.3. Capacitación

Una vez que la RENASEC y los IES involucradas se pongan de acuerdo en la estrategia y en los objetivos propios de las IES, la siguiente tarea va enfocada al desarrollo de capacidades tanto personales como de gestión en las propias instituciones, esto es, dotarse de las capacidades organizativas, conocimientos, habilidades, recursos monetarios, bienes de equipo y herramientas necesarias para conseguir los objetivos planteados.

La experiencia acumulativa (acumulación de conocimiento incremental), tanto de la RENASEC como de las IES asociadas, ha resultado insuficiente para poder garantizar el

⁷ Estudios de gestión de calidad y certificación son muestra de este hecho, por ejemplo, el intento de certificación ISO9000 por parte de la ANUIES en el 2005 que, por falta de apoyo directivo, fue abortado.

éxito de la gestión de la seguridad de la información que exige no solo la competencia y capacitación misma de las partes involucradas, sino también un grado de actualización (Capacitación) continua y mantenimiento (de los tres tipos de mantenimiento: preventivo, predictivo y reactivo) para poder conservarse competitiva.

Esto nos obliga a plantear la necesidad continua de adquirir, usar y generar nuevo conocimiento que, una vez combinado con el ya existente, resuelva más eficientemente los problemas de inseguridad que se van presentando.

Dicha adquisición, uso y generación de nuevo conocimiento puede realizarse básicamente de tres formas:

1. Internamente mediante la realización de investigación y desarrollo.
2. Por transferencia en un esquema comercial
3. Por transferencia en un esquema de acuerdo y cooperación.

De acuerdo a la encuesta realizada a las universidades (Tabla 5.1), los tres puntos tienen implicaciones favorables y desfavorables, como se explica a continuación.

5.2.3.1. Generación interna de conocimiento mediante la realización de investigación y desarrollo

El dato más relevante al respecto es que solamente el 30% de las IES tienen la capacidad de generar conocimiento aplicado en materia de SIeMD derivado de investigación y desarrollo interno a la universidad. Concretamente, solamente 12 IES han puesto a disposición de la RENASEC herramientas desarrolladas de SIeMD de autogeneración de conocimiento, de las cuales solamente 6 de ellas⁸ han mostrado capacidad de generar dichas herramientas con un alto grado de capacidades tecnológicas.

⁸ Las universidades que han puesto a disposición de la RENASEC herramientas de seguridad con un alto espectro de protección informática son: La Universidad Nacional Autónoma de México, El Instituto Politécnico Nacional, La Universidad de Chiapas, La Universidad de Guadalajara, El Tecnológico de Monterrey y La Universidad Autónoma Metropolitana.

5.2.3.2. Transferencia de capacidades en un esquema comercial

Cotec, la ONU y la RENASEC han evidenciado un riesgo moral derivado de la adquisición de conocimiento vía proveedores.

De acuerdo a la exploración realizada en las universidades, se pudo observar que las tecnologías ofrecidas por los proveedores tienen un crecimiento extraordinario (en número pero también en costo), y una dinámica continua de cambio y evolución, sin embargo, dicha dinámica pareciera ser insuficiente para cubrir las necesidades de seguridad, esto es, pareciera ser que mientras mayor sea la dinámica de cambio en las tecnologías de seguridad de la información, y exista un incremento en la variedad de éstas tecnologías, mayor aún es la incertidumbre de invertir recursos económicos en ellas y a su vez, mayor es la presión en las instituciones por el uso de tecnologías más baratas, incluso tecnologías libres⁹.

Cabe recordar en este punto que la evidencia empírica mostrada puso de manifiesto problemas serios para la generación de tecnologías y desarrollos predictivos de seguridad de la información, asimismo, y como ya se ha discutido, la tendencia es a desarrollar tecnologías reactivas, esto es, las capacidades se han concentrado en generar herramientas tecnológicas reactivas, lo que no resuelven en realidad el problema, solamente lo alivian¹⁰.

Si se analizan ambos elementos, por un lado tenemos un gran cúmulo de proveedores con soluciones diferentes, pero cuya solución al problema de seguridad de la información está tomando una tendencia de carácter reactivo y no preventivo, con herramientas costosas y cuyo ciclo de vida es cada vez más corto. Esta circunstancia obliga, sin duda, a discutir el elemento de adquisición de capacidades por la vía comercial, esto es, la vía de los proveedores.

Asimismo, podemos asegurar que hasta el momento son pocas las tecnologías que realmente significan una transferencia de conocimiento “fundamental” de proveedor a

⁹ El término “libre” se refiere al permiso expreso del autor respecto al uso de la tecnología condicionando en todo momento a que el usuario reconozca al autor como el creador de la tecnología usada.

¹⁰ Haciendo una analogía con la medicina, un paciente puede decir que tiene dolor de cabeza, la tecnología no ha sido capaz de eliminar la causa del dolor, pero se ha vuelto experta en generar “aspirinas” que quitan y alivian el dolor y que son cada vez más efectivas, lo que ciertamente alivia el problema, pero no lo resuelve.

usuario; que de acuerdo con la investigación, este efecto es catalizado principalmente por las siguientes causas:

1. La tecnología de seguridad “de punta” tiene su origen en el extranjero, por lo que el conocimiento de la tecnología tiene que pasar por muchas personas desde el origen del conocimiento hasta el usuario final, lo que provoca un especie de “efecto de teléfono descompuesto”
2. No existe la posibilidad de explorar, mucho menos influir, en la tecnología de seguridad comercial, ya que “los códigos”, “las configuraciones”, “las tecnologías particulares”, etc son consideradas como “secretos industriales”, lo que limita a las universidades a su uso y no a su adecuación, mucho menos a su configuración tecnológica específica, lo que en términos de capacidades, significa que existe un crecimiento en la capacidades de uso, pero un decremento en las capacidades de innovación, incluso de desarrollo tecnológico en materia

5.2.3.3. Transferencia en un esquema de acuerdo y cooperación

Uno de los objetivos principales y claros que busca la RENASEC es la generación de conocimiento vía redes de comunicación entre las IES, tema que además de ser muy interesante es sumamente importante y trascendente sin embargo, por el momento queda abierto a estudio ya que la presente tesis no tiene contemplado dicho análisis.

La razón principal está concentrada en las respuestas dadas a una de las entrevistas personales, donde se evidencia que solamente el 4% de las universidades usan redes de intercambio de información y conocimiento interuniversidades en materia de SIeMD.

Además de la RENASEC, no existe en materia de seguridad, ninguna otra red de cooperación interuniversitaria a nivel nacional, de hecho, es más fácil el uso de otras redes de conocimiento en SIeMD ajenas a la RENASEC, cuyo control y gestión está lejos de poder ser útil a las necesidades planteadas.

5.2.4. Implantación

No se debe de perder de vista un elemento vital, la implantación debe ser un aspecto fundamenta para cumplir con los objetivos de una gestión tecnológica, y que dichos objetivos, según el estatuto de la RENASEC, son:

- Proteger y responder de manera adecuada a las emergencias relativas a las tecnologías de información en las IES del país.
- Apoyar en los incidentes de seguridad en cómputo a cualquier miembro de la Red que lo solicite.
- Promover el desarrollo de las tecnologías de información en las IES, en cuanto a la materia de seguridad en cómputo, sistematizando y relacionando las diferentes iniciativas existentes en esta materia en el país.
- Fomentar, supervisar y coordinar el desarrollo de la seguridad en cómputo dentro de las IES del país.
- Autorizar, respetar y hacer cumplir los Estatutos y Reglamentos de las Redes Regionales de conformidad con las normas establecidas por la propia Red, vigilando el estricto cumplimiento de las normas técnico-académicas correspondientes a las IES.
- Avalar la participación de miembros de la Red en congresos y/o conferencias nacionales e internacionales.
- Apoyar los eventos autorizados y organizados por las Redes Regionales, que hayan sido oportunamente incluidos en su programa de trabajo, aprobado por el Consejo Nacional de la RENASEC.
- Estudiar, adaptar y difundir los procedimientos de enseñanza técnica en materia de seguridad en cómputo.
- Extender los procedimientos de capacitación y enseñanza en todos los aspectos que se requieran a todos los miembros de la RENASEC que lo soliciten.
- Mantener actualizado el registro de sus miembros.
- Proporcionar oportunamente información técnica que contribuya a la mejor difusión, conocimiento y debida aplicación de la seguridad en cómputo.

Esto nos obliga a plantear lo siguiente: la capacitación y el aumento de las capacidades, la estrategia, los objetivos comunes y la vigilancia (puntos tratados anteriormente en la presente tesis), tanto de la RENASEC como de las IES, ha llevado al fortalecimiento y aumento de su base de conocimientos (hecho que puede ser demostrado con los cuestionarios y las entrevistas realizadas en esta investigación); sin embargo, tener una base de conocimientos fortalecida y aumentada no necesariamente significa que tanto la RENASEC como las IES sean más competitivas y seguras.

La complejidad de la gestión nos obliga a plantear la siguiente pregunta: ¿cómo convertir el conocimiento, capacidad y estrategia adquirida en una eficiente gestión tecnológica enfocada a la seguridad de la información en medios digitales entre las IES y la RENASEC?

La implantación de la gestión tecnológica es la única forma de poder observar, administrar y verificar algún tipo de resultado, que se demostrará, en nuestro caso, en esquemas de seguridad útiles, prácticos y resolutivos.

Implementar una gestión tecnológica significa asegurarse que los distintos componentes generales, particulares, comunes, etc. sean llevados a cabo de una manera eficiente, tomando en cuenta que los modelos, estructuras o estrategias resultantes deben contener insertados conocimientos específicos que den contenido y sustento a las distintas argumentaciones, así, encontramos por ejemplo varios esquemas de gestión de seguridad en información (la norma ISO 17799 que ahora es conocida como la norma ISO 27800, Octave y la metodología de gestión de la red de seguridad IRIS)

La evidencia empírica nos da indicaciones puntuales importantes a éste respecto: Primero que nada revisando los anteriores puntos específicos de gestión (vigilar, focalizar, capacitar), encontramos que evidentemente existen rezagos en cada uno de ellos tanto en las IES como en la RENASEC.

Además, al revisar la evidencia empírica (Tabla 5.1) y las entrevistas personales en las 26 universidades seleccionadas, evidentemente encontramos mejoras en estructura, capacidad, incluso en gestión tecnológica del 2002 a la fecha, pero que de ninguna manera son suficientes.

A nivel personal, de capacidad, directiva, organizacional, de conocimiento, de relación proveedor-usuario, etc; existen elementos, por demás evidentes de que las acciones implementadas no han dado los resultados esperados.

5.2.5. Aprendizaje

En este apartado, hablar de aprendizaje es hablar de generación de conocimiento, de procesos de aprendizaje tanto en lo individual como colectivo. En una perspectiva de gestión tecnológica, se deben tener claros los canales por medio de los cuales se facilita dicho proceso de aprendizaje y, en consecuencia, se aumentan las capacidades en sus diferentes perspectivas.

Como podemos observar durante el desarrollo de la presente tesis, es evidente la existencia a través del tiempo (desde 2001 hasta 2006) de la creación y aplicación de programas cuyo objetivo es elevar las capacidades tanto de la RENASEC como de las IES asociadas; sin embargo, al revisar la evolución histórica de la aplicación de dichos programas, nos encontramos con severas dificultades que a la larga se manifiestan como síntomas de ineficiencia en la aplicación de la gestión tecnológica.

Se debe buscar que los programas de gestión tecnológica ayuden a homogeneizar y hacer converger los factores implícitos a la gestión tecnológica y de los asuntos relacionados con ella, sin embargo, y pese a homogeneidades en las características regionales, al revisar los programas regionales nos encontramos con diferencias significativas que provocan que no exista realmente una tendencia hacia la convergencia, sino más bien hacia la especialización de grupos concretos, lo que da como consecuencia diferencias significativas entre las IES, esto es, se encuentran IES altamente capacitadas con formación de capacidades tecnológicas avanzadas, e IES que realmente no han podido ni siquiera conseguir capacidades operativas respecto a la propia seguridad de la información

Lo anterior nos obliga a suponer que, si bien en la región Centro Sur y en la Región Metropolitana, se han creado las condiciones para aumentar en los últimos 5 años las capacidades tecnológicas enfocadas a la seguridad de la información, existen elementos en

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

las demás regiones que no permiten la creación de capacidades; en otras palabras, no existe generación de conocimiento.

Solo 15% de las IES tiene las capacidades tecnológicas suficientes para la generación de conocimiento específico en seguridad de la información en medios digitales, sin embargo, solamente doce IES lo hacen.

Asimismo la evidencia empírica nos da información importante relacionada con los procesos de aprendizaje al día de hoy:

- Sólo el 35% de las universidades tienen jerarquizada su información, en otras palabras es jerárquicamente equivalente la información de calificaciones y de los egresados de la misma universidad que el precio de las donas de la cooperativa de la esquina.
- Sólo el 40% de las universidades tienen la capacidad humana suficiente para atender y resolver problemas de seguridad de la información de manera interna a la universidad
- Sólo el 35% de los directivos conocen las actividades de gestión de seguridad de la información
- El 60% de las universidades poseen redes de información, con iniciativa privada, ORG, etc, pero solamente 17% de ellas las usan con fines de seguridad de la información y el 3% de ellas las usan las redes interuniversitarias.
- El 70% de los reportes de problemas en seguridad catalogadas como graves o importantes, son reportados mensualmente, anualmente o nunca; esto es, 70% de los reportes no influyen de forma inmediata en la solución de los problemas.
- El 50% de las universidades que usan algún tipo de proveedor no saben si el mismo proveedor usa algún tipo de modelo de gestión de la información

Lo anterior nos señala alguna de las más importantes limitantes para un óptimo proceso de aprendizaje: Analizando los puntos anteriores, no podemos esperar un óptimo proceso de aprendizaje puesto que no se tiene una jerarquía de la información.

Menos de la mitad de las IES tienen capacidades internas suficientes para identificar, analizar y resolver algún tipo de problema y contingencia.

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

La parte directiva juega un papel fundamental en el proceso de aprendizaje de cualquier institución, porque funciona como catalizador del proceso de gestión de seguridad. En este asunto particular, es evidente el desconocimiento de la importancia de las acciones de seguridad informática por parte los directores institucionales ya que solamente el 30% de ellos tiene conocimiento de ellas.

En otras palabras, podríamos suponer que solamente en el 30% de las IES existen las condiciones directivas suficientes para esperar un eficiente proceso de aprendizaje.

Uno de los mecanismos más importantes en el proceso de aprendizaje es el uso de las redes que son proveedoras de información, aquí se presenta un problema al encontrar que solamente el 17% de las universidades usa estos canales para sus procesos de aprendizaje.

Una máxima ingenieril dice que “lo que no es medible no es controlable”, así, si el 70% de las universidades no contemplan “la medición” de la seguridad de la información vía reportes, esto genera un estado de “confort” que sin duda puede derivar en elementos negativos que no ayuden a los procesos de aprendizaje.

5.3. Análisis de los resultados

Al día de hoy, podemos identificar que la evolución de trayectoria tanto de las capacidades tecnológicas como de la gestión en seguridad en la RENASEC y en las IES es la siguiente:

Respecto a la ANUIES-RENASEC

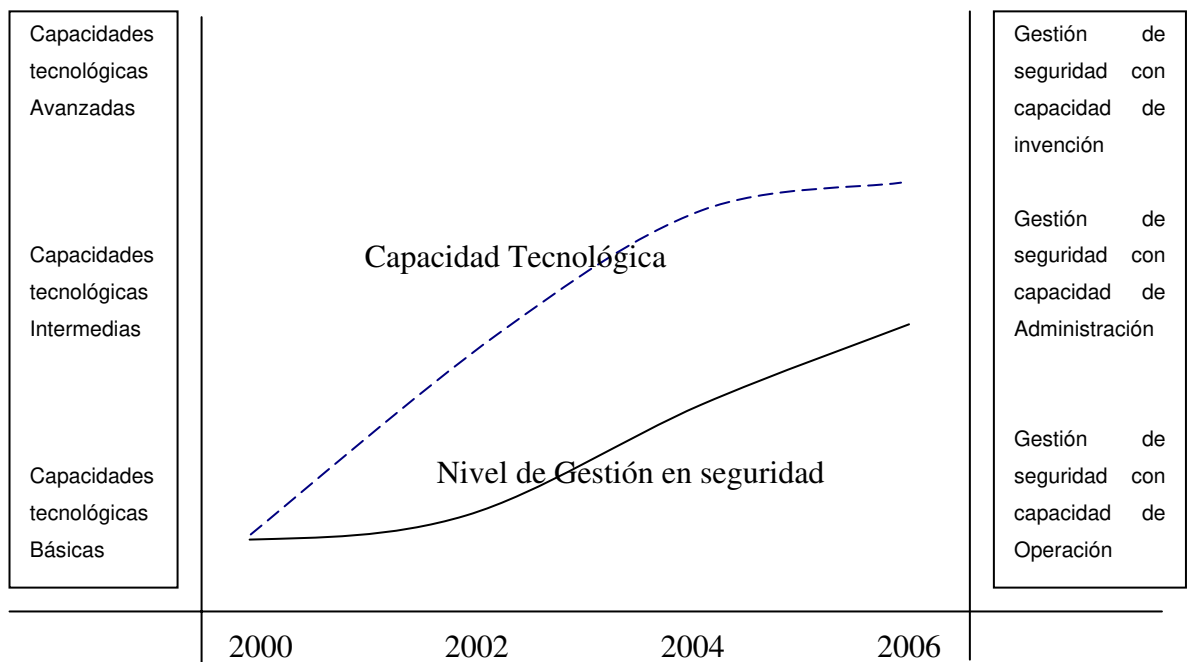


Figura 5.1 Comparación de la evolución de las capacidades tecnológicas y del nivel de gestión de seguridad en la ANUIES (Realización propia)

De las evidencias empíricas, las encuestas en la RENASEC y la ANUIES, y del análisis de la evolución de su trayectoria, podemos asegurar que existe un aumento tanto de las capacidades internas tecnológicas como del nivel de gestión de seguridad, lo que ha sido provocado por el fortalecimiento de los elementos fundamentales intrínsecos de la gestión: focalización, aprendizaje, vigilancia, capacitación e implementación. En ellos se destacan algunos elementos como:

- Desde el 2000 compromiso de la dirección de la ANUIES
- La Autonomía propia de los apartados de seguridad a partir del 2002

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

- Uso de las redes regionales de la ANUIES para la RENASEC a partir del 2001
- La adecuación de los programas y objetivos a la misma RENASEC (2000, 2002, 2005 y 2006)
- Flujos de información y conocimiento en los diversos congresos organizados por la UNAM-RENASEC, etc.

Profundizando un poco en la figura 5.1, es evidentemente que la RENASEC tiene limitantes en sus capacidades tecnológicas internas, sin embargo, el principal problema no es el tema de capacidad, sino el tema de gestión tecnológica. Éste hallazgo es uno de los principales y más importantes de la investigación: La principal limitante de la RENASEC y de las IES, en relacion con la SIeMD, es relacionada principalmente por aspectos de gestión tecnológica y no por la capacidad tecnológica.

Respecto a las IES

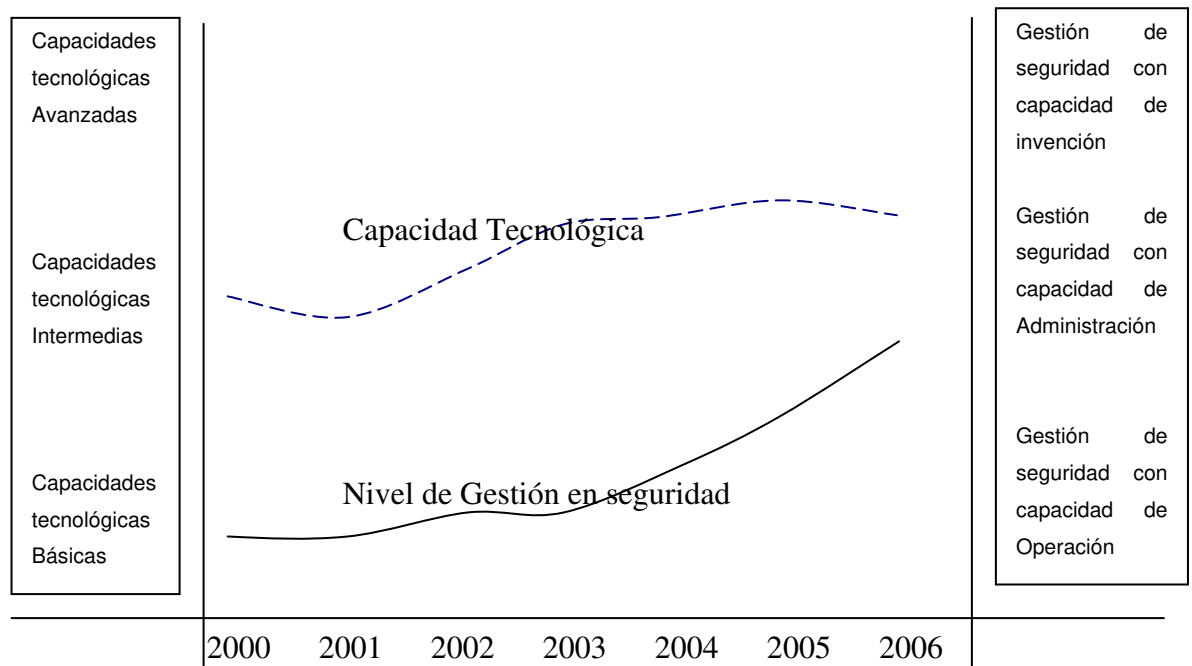


Figura 5.2 Comparación de la evolución de las capacidades tecnológicas y del nivel de gestión de seguridad en las IES (Realización propia)

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

La evidencia empírica en la investigación es clara, las IES presentan tres grandes bloques que son concurrentes, homogéneos y consistentes a través de las diferentes regiones de la RENASEC:

1. IES con grandes recursos económicos, estratégicos, de gestión, infraestructura, etc, las cuales suelen estar por arriba de las normas de seguridad internacionales conocidas, poseen alta capacidad tecnológica y niveles de gestión de la seguridad apreciables.
2. IES promedio que poseen ciertamente una cantidad limitada de capacidades tecnológicas, y, generalmente, poco nivel de gestión en seguridad de la información.
3. IES que no poseen niveles significativos ni de capacidades tecnológicas, ni de gestión en seguridad de la información.

Cabe destacar que la gráfica anterior se basó principalmente en elementos empíricos, de evolución histórica y en un trabajo de campo de más de dos años, con entrevistas semidirigidas personalizadas a los encargados de las universidades, encuestas y observación directa.

Dada esta diferencia entre las IES, era de esperarse niveles bajos de SIeMD, sin embargo, lo que la gráfica de la figura 5.4 muestra es la existencia de otros elementos que explican los niveles bajos de seguridad, entre los que encontramos:

- El cambio continuo de los objetivos de la RENASEC respecto a las acciones aplicadas a las IES año con año, esto es, no se puede trazar un plan de desarrollo cuyo origen sea el institucional (la RENASEC al momento presentar cambios continuos de sus prioridades no ha podido fijar un liderazgo de gestión tecnológica que logre convencer a las IES la adaptación de medidas de crecimiento y homogenización).
- Las condiciones internas de las IES, donde los elementos directivos, los elementos organizacionales, los elementos sociales, los elementos económicos, entre muchos otros varios, debilitan los procesos de aprendizaje, lo que hace disminuir las capacidades tecnológicas y más aun la gestión tecnológica de las IES.

Sin embargo, el análisis más importante en este sentido, es cuando podemos contrastar las características de la RENASEC contra las características de las IES para

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

poder ver si, a partir de sus capacidades y de su nivel de gestión tecnológica se pudiera pensar en la posibilidad de una buena gestión tecnológica de seguridad entre ellas, lo que nos muestra contrastes interesantes:

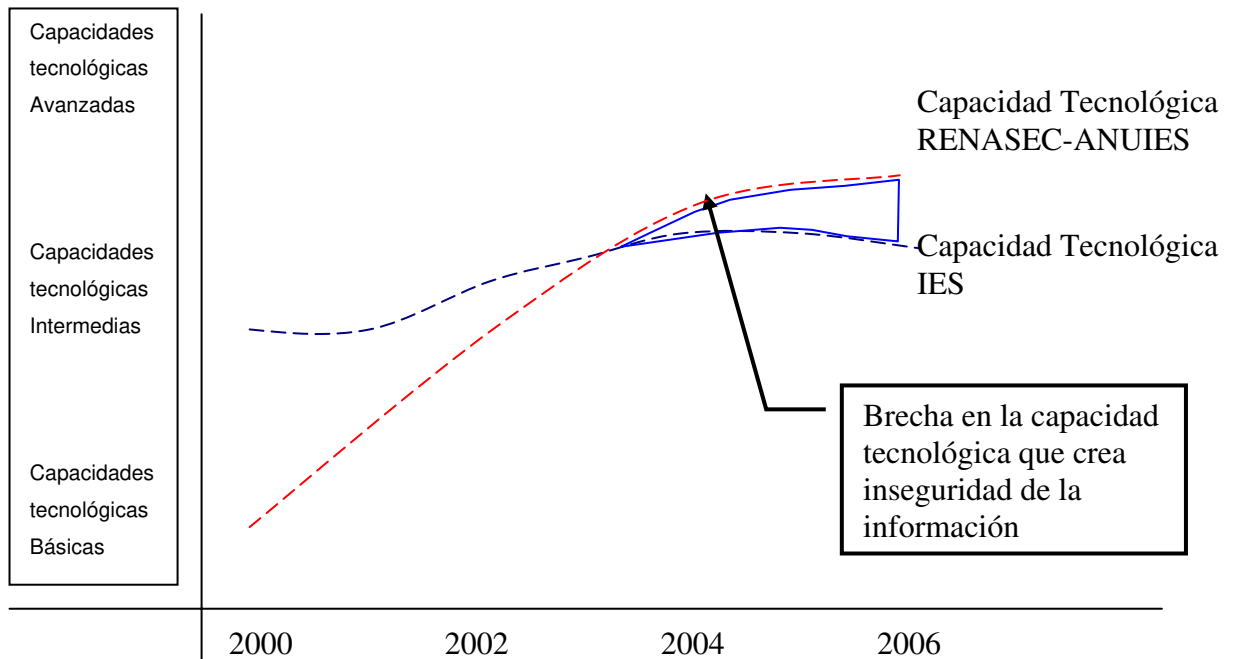


Figura 5.3 Comparación de la evolución de las capacidades tecnológicas en las IES y en la RENASEC (Realización propia)

En la Figura 5.3 es muy interesante notar que, en promedio, las capacidades tecnológicas de la RENASEC son superiores en este momento a las de las IES; sin embargo, esto no fue siempre, sino que ha sido un proceso continuo en el cual es evidente que los programas de capacitación, los objetivos de la RENASEC, el apoyo institucional, entre otros tantos factores, ha permitido fortalecer las capacidades tecnológicas de básicas llevándolas a un punto medio entre las capacidades intermedia y las avanzadas.

Es también de llamar la atención que el crecimiento de las capacidades en las universidades ha sido muchísimo menor, por lo que la conclusión más importante en este sentido es que, de acuerdo con las entrevistas y la investigación realizada, podemos asegurar que el cambio dinámico del entorno en materia de seguridad informática ha sido mucho más rápido que la capacidad de las IES para entenderlo, analizarlo y reaccionar a partir de él.

Capítulo cinco: Gestión Tecnológica en Seguridad de la Información en Medios Digitales, El caso de la RENASEC perteneciente a la ANUIES

El problema no es en sí el estancamiento, sino la brecha de capacidad tecnológica entre las IES y la RENASEC.

Otro factor que incide en la seguridad de la información es otra brecha tecnológica detectada en las entrevistas personalizadas y la encuesta nacional: la que podemos ver que existe entre las IES, esto es, la existencia de IES que están por arriba de la norma y las IES que están por debajo de la norma.

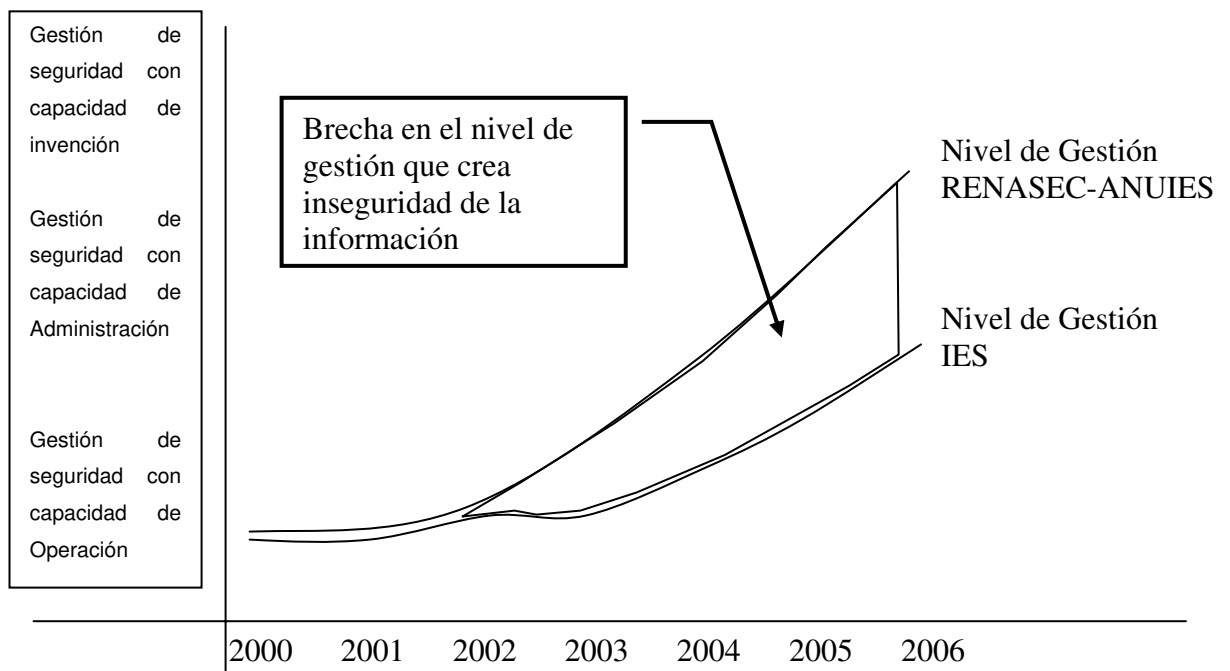


Figura 5.4 Comparación de la evolución del Nivel de Gestión Tecnológica entre las IES y en la RENASEC (Realización propia)

Observando la figura 5.4, es evidente también que la brecha tecnológica en gestión tecnológica es mucho más grande que la que representa las capacidades tecnológicas (figura 5.3).

Esto no es un resultado extraño, ya que como se pudo apreciar a lo largo de la investigación, existe una mayor posibilidad de contar con gente con un perfil de capacidades tecnológicas promedio dentro de las IES y en la RENASEC, que con personas de alto nivel técnico, esto principalmente porque antes de ser la seguridad de la información un elemento de estrategia dentro de las IES, es un elemento de satisfacción de necesidad.

Sin embargo y pese a que no es extraño el apunte anterior, no deja de ser preocupante, ya que, la brecha que se aprecia en la figura 5.4, respecto a la gestión tecnológica, no podría garantizar la SIeMD debido a diferencias significativas en la gestión tecnológica de la RENASEC y de los IES..

Se debe recordar que la gráfica representa el promedio de las IES, y que, indudablemente existen IES que incluso superan el nivel de gestión tecnológica que la RENASEC, pero también existen IES que ni siquiera tienen contemplada la gestión tecnológica en su esquema organizacional.

5.4. Hallazgos y conclusiones del capítulo

Los hallazgos y conclusiones presentados en este capítulo son:

Evidentemente ha aumentado la preocupación por la seguridad de la información de las universidades agremiadas a la ANUIES a través del tiempo, lo que ha llevado a un incremento en la aplicación de modelos de gestión de seguridad de la información.

Existe una evidente reducción del ciclo de vida de los productos relacionados con la seguridad de la información en medios digitales

La RENASEC y las IES tienen limitantes en sus capacidades tecnológicas internas, sin embargo, el principal problema no es el tema de capacidad sino el tema de gestión tecnológica.

Existe un aumento tanto de las capacidades internas tecnológicas como del nivel de gestión de seguridad; este aumento es provocado por el fortalecimiento de los elementos fundamentales intrínsecos de la gestión (focalización, aprendizaje, vigilancia, capacitación e implementación), destacando algunos elementos como compromiso de la dirección de la ANUIES (desde el 2000), el uso de las redes regionales de la ANUIES para la RENASEC a partir del 2001, la adecuación de los programas y objetivos a la misma RENASEC (2000, 2002, 2005 y 2006), los flujos de información y conocimiento en los diversos congresos organizados por la UNAM-RENASEC

En promedio, las capacidades tecnológicas de la RENASEC son superiores que las de las IES, sin embargo, esto no fue siempre. Ha sido un proceso continuo, en el cual, es evidente que los programas de capacitación, los objetivos de la RENASEC, el apoyo institucional entre otros tantos factores; han permitido fortalecer las capacidades

tecnológicas, transformándolas de básicas a un punto medio entre las capacidades intermedias y avanzadas.

El crecimiento de las capacidades en las IES ha sido muchísimo menor que en la RENASEC, por lo que, la conclusión más importante en este sentido es que el cambio dinámico del entorno en materia de seguridad informática ha sido mucho más rápido que la capacidad de las IES para entenderlo, analizarlo y reaccionar a partir de él.

Una conclusión importante es que el problema no es en sí el estancamiento, sino la brecha de capacidades tecnológicas y de gestión tecnológica entre las IES y la RENASEC.

También existe implícitamente una brecha tecnológica entre las IES debido a sus características internas propias.

La brecha evidenciada en gestión tecnológica es más grande que la brecha que representa las capacidades tecnológicas entre las IES y la RENASEC.

A partir de los datos y los resultados generados en la presente tesis: En éste momento la RENASEC no tiene los elementos suficientes para garantizar seguridad de la información en medios digitales.

C
O
N
C
L
V
S
I
O
N
E
S

En la presente investigación se plantearon tres preguntas e hipótesis de tesis:

¿Cuáles son los factores, desde una perspectiva tecnológica, que provocan la inseguridad de la información en medios digitales?

La hipótesis es que los factores que provocan la inseguridad de la información en medios digitales van relacionados con elementos de tipo “gestión tecnológica” y no solamente de “capacidades tecnológicas”

La conclusión en este particular es la siguiente:

Efectivamente, los factores que provocan elementos de inseguridad de la información en medios digitales tienen 3 orígenes:

1. Elementos de capacidad tecnológica

- a. Generar capacidades tecnológicas en el rubro de SIeMD no genera certidumbre suficiente para disminuir la sensación de inseguridad de la información en las IES
- b. Existen capacidades tecnológicas limitadas por parte de las personas que gestionan, operan, monitorizan y aplican los sistemas de seguridad de la información en las organizaciones
- c. Existe un aumento de los efectos negativos económicos, técnicos, sociales, etc; de los ataques a la SIeMD, aumentado asimismo el numero de ataques por tecnología específica y el desconocimiento del origen y cantidad de los ataques. Esto podría significar una evidencia de retrasos tecnológicos, capacidades tecnológicas limitadas y, sin duda, capacidades tecnológicas superiores de las personas que generan la inseguridad de la información en medios digitales.
- d. Se puede asegurar la existencia de una tendencia a consumir y confiar más la SIeMD a tecnologías reactivas, esto es, evidentemente se está aumentando el desarrollo, uso y consumo de tecnologías reactivas, siendo dichas

tecnologías de reacción demandantes de menos capacidades tecnológicas para su desarrollo, uso, y aplicación

2. Elementos de gestión tecnológica

- a. Como ya se mencionó, no basta tener un aumento en las capacidades tecnológicas ya que este rubro no es suficiente para disminuir la inseguridad de los SIeMD, como se mostró en la presente investigación, es fundamental el elemento de gestión tecnológica
- b. En ausencia de elementos de gestión tecnológica, no es posible asegurar la existencia de SIeMD
- c. Existe evidencia en la cual la gestión tecnológica no solo es un elemento importante para la garantía de seguridad de la información, sino que es un elemento vital para ello

3. Elementos de inseguridad intrínsecos al proceso de invención de las TIC's

- a. Se tienen los elementos suficientes para poder asegurar que, cualquier aplicación de gestión tecnológica en SIeMD debe siempre considerar un grado de inseguridad implícito al uso de las TIC's, cuyo origen se presenta desde la propia invención de la misma TIC's, lo que evidentemente aumentará los niveles de inseguridad (Capítulo 3)

¿Son dichos factores fundamentales en el proceso de gestión tecnológica en seguridad de la información en medios digitales dentro de la ANUIES-RENASEC?

La Hipótesis a esta pregunta es: la inseguridad de la información en medios digitales se debe principalmente a 3 elementos:

- 1. Divergencia Tecnológica**
- 2. Elementos deficientes en la gestión tecnológica dentro de las organizaciones que utilizan medios digitales, particularmente en la gestión tecnológica de la relación entre las IES y la RENASEC.**
- 3. Capacidades tecnológicas limitadas**

La conclusión en este asunto particular es la siguiente:

Efectivamente, existe un retraso dinámico entre las TIC's y la SIeMD, dicho retraso dinámico se evidencia en el capítulo 3 de la siguiente manera:

Se puede asegurar la existencia de una disminución de intensidad inventiva en patentes desarrolladas en seguridad de la información en medios digitales respecto con la generación de TIC's en su conjunto, lo que nos habla de una divergencia tecnológica en este rubro específico.

Se tienen los argumentos suficientes para poder asegurar que, cualquier estudio de gestión tecnológica debe siempre considerar un grado de inseguridad implícito al uso de las TIC's desde la propia invención de las mismas, lo que evidentemente aumentará los niveles de inseguridad (divergencia tecnológica).

Respecto a los elementos deficientes de la gestión y capacidad tecnológica entre la RENASEC y las IES, podemos asegurar que es la gestión tecnológica, y no las capacidades tecnológicas, el elemento que mas ha contribuido a la inseguridad de la información entre estos dos actores.

La evidencia presentada marca claramente que tanto en las IES como en la RENASEC se han dado las condiciones para la generación de capital humano con capacidades tecnológicas en materia de seguridad que son competitivas para las necesidades de la propia RENASEC y de las IES asociadas; sin embargo, también es evidente que dicha generación de capacidades no ha sido suficiente para la disminución de la inseguridad de la información.

De esta manera, la misma evidencia ha mostrado limitantes en las capacidades tecnológicas de las personas que gestionan la seguridad en las IES asociadas a la ANUIES, ya que también se ha encontrado un aumento en la capacidades, por lo que la visión debe

ser dinámica y pensar que la velocidad de generación de capacidades ha sido mas lenta y limitada que la capacidad de generar seguridad en los medios informáticos.

¿Es la RENASEC capaz de aplicar un modelo exitoso de gestión tecnológica de acuerdo a la evaluación de sus capacidades tecnológicas y los niveles de gestión tecnológica?

La hipótesis es: sí, la RENASEC es capaz de aplicar un modelo de “Gestión Tecnológica” exitoso.

La conclusión al respecto es: NO, con las condiciones actuales la RENASEC no es capaz de garantizar la SIeMD mediante la aplicación de modelo de “gestión tecnológica”, por las siguientes razones:

Continuamente existe redefiniciones en los objetivos generales y la misión de la RENASEC

Podemos encontrar IES muy por encima de los estándares de seguridad de la información, IES muy por debajo de los estándares de seguridad de la información (mas del 60%)

La RENASEC tiene limitantes en sus capacidades tecnológicas internas, sin embargo, el principal problema no es el tema de capacidad, sino el tema de gestión tecnológica.

En promedio, las capacidades tecnológicas de la RENASEC son superiores en este momento que las de las IES.

El cambio dinámico del entorno en materia de seguridad informática ha sido mucho mas rápido que la capacidad de las IES para entenderlo, analizarlo y reaccionar a partir de él.

Conclusiones

Uno de los problemas no es en si el estancamiento, sino, la brecha de capacidad tecnológica entre las IES y la RENASEC

La brecha evidenciada en gestión tecnológica es más grande que la brecha que representa las capacidades tecnológicas entre las IES y la RENASEC, por lo que una conclusión importante seria que realmente la RENASEC no tiene los elementos suficientes para garantizar seguridad de la información en medios digitales.

ibliografía

- Aboites, J. y Soria M. (1999), Innovación, propiedad intelectual y estrategias tecnológicas: La experiencia de la economía mexicana, UAM Xochimilco y Miguel Angel Porrúa, México.
- Aibar, E. (2001) "Fatalismo y Tecnología: ¿Es autónomo el desarrollo tecnológico", Revista Sociedad y Tecnología de la UOC No 1, España.
- Ariffin, N. and P. Figueiredo (2003), Internacionalização de competências tecnológicas, Río de Janeiro, Editora FGV.
- Anuies (1999), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 1999", Anuies
- Anuies (2000), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2000", Anuies
- Anuies (2001), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2001", Anuies
- Anuies (2002), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2002", Anuies
- Anuies (2003), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2003", Anuies
- Anuies (2004), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2004", Anuies
- Anuies (2005), "Reporte anual de la Asociación Nacional de Universidades e Instituciones de Educación Superior 2005", Anuies
- Archibugi y Pianta (1996), "Innovation surveys and patents as technological indicators: the state of the art" en Innovation, Patents and Technological Strategies, OECD.
- Arango, M. (2003). Foros virtuales como estrategia de aprendizaje. Revista Debates Latinoamericanos, N° 2, Abril 2004. Recuperado
- Barney, J. (1991), "Firm resources and sustained competitive advantage", en Journal of Management, vol.17, No.1.
- Bell, M. (1984), "'Learning' and the Accumulation of Industrial Technological Capacity in Developing Countries", in K. King and M. Fransman (eds), Technological Capacity in the

Third World; London, Macmillan

Bell, M. and K. Pavitt (1995), "The Development of Technological Capabilities", in I.u. Haque (ed.), Trade, Technology and International Competitiveness; pp. 69-101, Washington, The World Bank.

Castells, M (1999 2a Ed) La sociedad red, La era de la información vol. I, vol II y Vol III Madrid. Alianza Editorial

Castells, M. (1996-2000): La Era de la Información: Economía, Sociedad y Cultura. Alianza. Madrid.

CEPAL (2003), Los caminos hacia una Sociedad de la Información en América Latina y el Caribe.

Cimoli, M. y Della Giusta, M. (2003). The Nature of Technological Change and its Main Implications on National Systems of Innovation, en Aboites, J y Dutrénit, G. 2003. Innovación, aprendizaje y creación de capacidades tecnológicas. Coedición UAM- Ed. Miguel Angel Porrua.

COTEC (1999) "Pautas metodológicas en gestión de la tecnología y de la innovación para empresas", Tomo 2 "Herramientas de gestión de la tecnología", España

COTEC (2001) "Innovación Tecnológica, Ideas Básicas", España

COTEC (2005 a) "Capacidades empresariales para la innovación. Su gestión", Cotec, España,

COTEC (2005 b) "Technology transfer, Issues common to national innovation system in Italy, Portugal and Spain", España.

Clegg, S., M. Kornberger, y T. Pitsis (2004), Managing and Organizations: An Introduction to Theory and Practice, Sage, 584.

CSI/FBI (2002) Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey"

CSI/FBI (2003) Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey"

CSI/FBI (2004) Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey"

CSI/FBI (2005) Reporte anual de delitos informáticos y encuesta de seguridad "Computer Crime And Security Survey"

- CSI/FBI (2006) Reporte anual de delitos informáticos y encuesta de seguridad “Computer Crime And Security Survey”
- Davenport, T (1996): “Some principles of knowledge management”, en el sitio web: www.incombs.utexas.edu/kman/pubs.htm
- Davenport, T.; Prusak, L. (1998), “Working Knowledge: How Organizations Manage What They Know”, Harvard Business School Press.
- Dixon, N. (2000). Common knowledge: How companies thrive by sharing what they know. Harvard Business School Press. EE.UU.
- Dosi, G.; Freeman, C.; Nelson, R.R.; Silverberg, G.; Soete, L.(1988), Technical Change and Economic Theory, Pinter Publishers, Londres, 1988.
- Dosi, J (1982), 'Technological paradigms and technological trajectories: the determinants and directions of technical change and the transformation of the economy', Research Policy, 11, pp. 147-62.
- Faga, R (2000), “Como profundizar en el análisis de sus costos para tomar mejores decisiones empresariales”, Buenos Aires: Granica
- Fransman, M. (1994); “Information, knowledge, vision and theories of the firm”, Industrial and Corporate Change, vol.3, n°3, 1994.
- Fremman, C. y Perez, C., (1986) "The diffusion of technical innovations and changes in techno-economic pa
- Grant, R (1995) “Ventaja Competitiva en Sectores Intensivos en Tecnología y la Gestion el Conocimiento, en: Direccion Estratégica. Ed Civitas
- Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scout, P., y M. Trow (1994), La nueva producción de conocimiento; La dinámica de la ciencia y la investigación en las sociedades contemporáneas, Ediciones Pomares-Corredor, Barcelona.
- Griliches, Z.(1990).Patent Statistics as Economic Indicators: A Survey, Journal of Economic Literature, vol. XXVIII (diciembre 1990) pp. 1661-1707.
- Ghuri, P., Gronhaug, K. y Kristianslund, I. (1995). Research methods in business studies: a practical guide. Nueva York, Prentice Hall.
- Hamlin, CH. (1992), “Reflexivity in technology Studies: Toward a technology of technology (and Science)”, Social Studies of Science, Vol.22, SAGE, London, Newbury and New Delhi, 511-544

- Hilbert, M. & Katz J.(2003) “Building an Information Society: A Latin American and Caribbean Perspective”, CEPAL LC/L.1845.
- Hitt, M., Ireland, D. y Hoskisson, R. (1999), Administración estratégica, competitividad y conceptos de globalización, México, Thomson Editores.
- Hitt, M., Ireland, D. y Hoskisson, R. (1999), Administración estratégica, competitividad y conceptos de globalización, México, Thomson Editores.
- Jaramillo, L. (1978-2000). “Difusión de Tecnología en el Japón- 2a Revision”. Ciencia, Tecnología y Desarrollo. Bogotá.
- Johannisson, B. y Nowicki, K. (1993) “Using networks to organize support for entrepreneurs” Växjö University and Lund University, Suecia.
- Kanz, J., Lam, D. (1996) "Technology, Strategy, and Competitiveness: An Institutional Managerial Perspective". Gaynor, G. (de.). "Handbook of Technology Management C. McGraw-Hill. New York.
- Hilbert M, Kats J. (2003): “Los caminos hacia una sociedad de la información en América Latina y el Caribe ”, CEPAL
- Khalil, T.M. (1998) "Future Directions and Needs for the New Century". Report of the Workshop on Management of Technology and the Paradigm Shift in Education in Response to the Technology Revolution, NSF, Arlington. Virginia. U.S.A.
- Lall, S (1996). Las capacidades Tecnológicas, In F. Sagasti & C. Sachs (Eds.) Una Búsqueda incierta: ciencia, tecnología y desarrollo. México: Fondo de Cultura Económica.
- Lall S. (2000). The technological structure and performance of developing countries manufactured exports, 1985-1998. Oxford: Queen Elizabeth House, Working Papers. Oxford University.
- Leonard-Barton, D. (1992), "Core Capabilities and Core Rigidities: a Paradox in Managing New Product Development", Strategic Management Journal.
- Leonard-Barton, D. (1992): “Core capabilities and core rigidities: a paradox in managing new product development”, Strategic Management Journal, vol. 13, Summer Special Issue, vol. 13,
- Lira A. (2005) “La tecnología de la información y la comunicación: Estudio Económico”, Revista Problemas de Desarrollo, Vol 36, Num 143.

- Macau, R (2004). "TIC: ¿para qué? (Funciones de las tecnologías de la información y la comunicación en las organizaciones)". Revista de Universidad y Sociedad del Conocimiento (RUSC). Vol. 1, nº 1.
- Malhotra, Y (1997), "La dirección del conocimiento en una organización inteligente", Procedimiento de la asociación para los sistemas de información, Tercera conferencia americana de los sistemas de información.
- Mancera Ernst & Young 2002 "Encuesta Global de seguridad informática"
- Mancera Ernst & Young 2003 "Encuesta Global de seguridad informática"
- Mancera Ernst & Young 2004 "Encuesta Global de seguridad informática"
- Mancera Ernst & Young 2005 "Encuesta Global de seguridad informática"
- Mancera Ernst & Young 2006 "Encuesta Global de seguridad informática"
- Nelson, R. and Winter, S. (1982), An Evolutionary Theory of Economic Change, Harvard University Press
- Nonaka, I y Takeuchi, H (1995): The Knowledge-creating company. How Japanese companies create the dynamics of innovations. Oxford University Press, New York.
- Pavitt, K. (1984), "Sectoral Patterns of Technical Change: Towards a Taxonomy and a Theory", Research Policy, Vol. 13, no. 9, pp. 343-373. Pavitt, K. (2004), "The processes of innovation", en Fagerberg, F., Mowery, M. Y R. Nelson (eds), Oxford Handbook of Innovation, Oxford University Press.
- Pavitt, K; Patel, P. (1988). The internacional distribution and determinants of technological activities. Oxford reviw of Economic Plicy, Vol 4 no 4
- Perez, C (2000), Cambio de paradigma y rol de la tecnología en el desarrollo, Charla en el Foro de apertura del ciclo "La ciencia y la tecnología en la construcción del futuro del país" organizado por el MCT, Caracas, Junio de 2000.
- Porter, M. (1982), "Estrategia Competitiva", C.E.C.S.A., México.
- Porter, M. (1996). What is Strategy ?. Harvard Business Review.
- Rodrigues, H (2001), "Trayectoria Innovativa y Estrategias Tecnológicas en los Procesos FCC: un Análisis de Patentes Otorgadas en Estados Unidos 1976-2000" Tesis, UAM-Xochimilco
- Rozga, L (2004), "Sistemas Regionales de innovación. Antecedentes, origen y perspectivas" Convergencia, Revista de Ciencias Sociales FCPyAP UAEM.

- Sancho, J. M. et al (1992): Aprendiendo de las innovaciones en los centros: la perspectiva interpretativa de investigación aplicada a tres estudios de casos. MEC. Madrid.
- Spinak, E. (1998). Indicadores cuantitativos. Ciencia de la Información, v. 27, n. 2, Brasil.
- Spinak, E. (1996). Diccionario enciclopédico de bibliometría, cuantimetría e informetría. UNESCO/PGI, Caracas.
- Tapsacott, D.(1997) La economía digital. Editorial McGraw-Hill, Bogotá-Colombia
- Teece D. (1994), "Strategies by which Technological importers can Profit from innovation", Hass School of Business, University of California at Berkeley
- Teece and Pisano (1994), The dynamic capabilities of firms: an introduction, en Industrial and Corporate Change.
- Teece, D.J., Pisano, G., Shuen, A. (1997): "Dynamic capabilities and strategic management". Strategic Management Journal, 18 (7).
- Teece, Pisano and Shuen (1990), Firm capabilities, resources and the concept of strategy, CCC Working Paper No 90-8.
- Tsujii. S. (2004) Paradigm of information Security as Interdisciplinary Comprehensive Science. Proc of the 2004 International Conference on Cyberwords (CW'4), IEEE Computer Society.
- Yin, R. (1994). *Case study research. Design and methods*. Sage Publications
- Yoguel, G., Novick, M., Catalano, A. y Albornoz, F. (2002) "Adaptación de modelos productivos en países emergentes. El caso de la industria automotriz en la Argentina" LITTEC – Universidad Nacional de General Sarmiento. EPaper N°12
- Westphal, L. Kim y Dahlman, C (1985) "Reflexions of the Republic of Korea's Acquisition of Technological Capabilities", en Rosenberg y C. Frischtak, International Technology, NY, Praeger.

ANEXO A Listado de Fuentes de Información usado en la etapa preliminar de la investigación, resaltado en encuesta y el año de aplicación de la encuesta

Título / País.	México	España	Colombia	Argentina
CSI/FBI COMPUTER CRIME AND SECURITY SURVEY				
ENCUESTA A HOGARES ESPAÑOLES SOBRE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN		2003		
ENCUESTA AIMC A USUARIOS DE INTERNET		2000, 2001, 2003, 2004, 2005		
ENCUESTA DE SEGURIDAD INFORMÁTICA EN ARGENTINA				2002, 2003, 2004
ENCUESTA DE SEGURIDAD INFORMÁTICA ERNST & YOUNG				
ENCUESTA NACIONAL DE SEGURIDAD INFORMATICA ASIS			2004	
ESTUDIO AMIPCI DE Hábitos de los usuarios de Internet en México	2002, 2003, 2004			
ESTUDIO DEL PERFIL DE LA INDUSTRIA MEXICANA DE SOFTWARE	2002			
ESTUDIO SOBRE EL ESTADO ACTUAL DE LA SEGURIDAD DE LOS SISTEMAS DE LA INFORMACIÓN EN LAS EMPRESAS ENTREVISTADAS, DE ACUERDO CON LA NORMA ISO/IEC17799:2000 (2003)		2003		
LA INNOVACIÓN EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES COTEC				
LA SEGURIDAD RED DE CATLUÑA		2002		
LA SOCIEDAD DE LA INFORMACION EN ARGENTINA				2003
LOS CAMINOS HACIA UNA SOCIEDAD DE LA INFORMACIÓN EN AMÉRICA LATINA Y EL CARIBE ORGANIZACIÓN DE NACIONES UNIDAS ONU				

Anexo B análisis preliminar realizado por el programa “Matheo Patent”



Figura AnB1 Hoja inicial al abrir el programa de Matheo Patent

La metodología de uso es sencilla:

- Se abre el programa de Matheo Patent (AnB1)
- Se hace clic a “New”, para definir un nuevo proyecto del programa.
- Se le da un nombre al proyecto
- Posterior a ello, el programa abre una ventana de búsqueda (AnB2), en ella, se puede definir distintos tipos y formas de búsqueda, entre las que se tiene:
 - Por título
 - Por nombre del invento
 - Por aplicación
 - Número de patente
 - Número (Clasificación) de aplicación
 - Número de alta prioridad
 - IPC y EC

The screenshot shows a 'New request...' dialog box with the following fields and options:

- Title:** A text input field with a magnifying glass icon.
- Abstract:** A checkbox.
- Inventor:** A text input field with a magnifying glass icon.
- Applicant:** A text input field with a magnifying glass icon.
- Patent Number:** A text input field with a magnifying glass icon.
- Application Number:** A text input field with a magnifying glass icon.
- Priority Number:** A text input field with a magnifying glass icon.
- IPC*:** A text input field with a magnifying glass icon.
- EC*:** A text input field with a magnifying glass icon.
- * IPC and EC Format :** e.g. A61B008/10
- Source:**
 - ☒ Esp@cenet
 - ☐ U.S.P.T.O. Issued
 - ☐ U.S.P.T.O. Pub.
- Requested information:**
 - ☐ Description
 - ☐ Claims
 - ☐ Download Patent Family
 - ☐ First Page
 - ☐ Drawing
- Date:**
 - ☒ Search patents from 2004 to 2006
 - ☐ Only start year
 - ☐ By month

Buttons at the bottom: Reset, Test my request, Ok, Cancel.

Figura AnB2 Hoja de búsqueda del programa de Matheo Patent

Como se puede observar en ésta poderosa herramienta, la búsqueda puede hacerse en al menos 2 bases de datos:

- ESPACENET (Base de datos europea que concentra a las patentes de todo el mundo)
- USPTO (base de datos de la oficina de patentes de los Estados Unidos de Norteamérica).

Otra característica importante de la herramienta es la posibilidad de definición de “búsqueda especializada”, donde ésta (la búsqueda) se puede delimitar en apartados como “Description” o “Clams”

Pero quizá una de las características mas importantes (dado nuestro interés por determinar elementos de evolución y trayectoria) del presente

programa es precisamente que se puede definir el rango de tiempo, esto es, que la herramienta tiene la facilidad de delimitar el rango de tiempo de inspección de las patentes, en nuestro caso, de 1980 a 2006 (Como se puede observar en la Figura AnB1).

Al momento de insertar los datos de búsqueda, se despliega los resultados como se muestra en la figura AnB2, donde se puede notar algunos datos generales de las patentes solicitadas, es aquí cuando se puede hacer el análisis cambiando de formato en el cuadro “Patent Analysis”, donde se muestra, de entrada, el análisis “preliminar” de los datos como se puede ver en la figura AnB3 y AnB4.

The screenshot shows the Mathéo Patent 7.1 software interface. The top menu bar includes File, Edit, Show, Statistics, Reports, Exports, Tools, Scores, Window, and Help. The toolbar contains icons for New, Open, Save, Add patents, Update, Patent Analysis, Patent Info, Patent filter, All read, Graphics, and Report. The main window displays a search results table with columns: S, C, D, Pertinence, Number, Title, PR.D, F..., and Score. The table lists various patents related to security modules and information storage. Below the table, there is a detailed view of a specific patent, showing its title, user comment, patent number, publication date, inventors, applicants, and IPC classification.

S	C	D	Pertinence	Number	Title	PR.D	F...	Score
				HK1020629	METHOD FOR STORING AND OPERATING SENSITIVE INFORMATION IN A SECURITY MODULE, AND ASSOCIATED SECURITY MODULE	13/03/1997	9	
				US2006118738	SECURITY MARKERS FOR ASCERTAINING NAVIGATIONAL INFORMATION	26/06/2003	8	
				EP1467366	SECURITY SYSTEM USING OPTICAL INFORMATION RECORDING MEDIUM	11/01/2002	7	
				US2004123311	SECURITY DEVICE FOR INFORMATION STORAGE MEDIA	10/11/2000	6	
				HK1039507	SECURITY ROOM FOR INFORMATION TECHNOLOGY FACILITIES	17/11/1998	6	
				DE10252521	BANK OR PREPAYMENT CARD SECURITY CODE DISTRIBUTION DEVICE HAS SECURE INFORMATION UNDER RUB OFF LAYER WITH ADDITIONAL LOW	12/11/2002	6	
				AU2005201002	METHOD AND SYSTEM FOR DISPLAYING AND MANAGING SECURITY INFORMATION	23/04/2004	6	
				US2005289062	DATA STORAGE DEVICE CAPABLE OF STORING MULTIPLE SETS OF HISTORY INFORMATION ON INPUT/OUTPUT PROCESSING OF SECURITY DATA	25/07/2002	5	
				US2004076147	VARIABLE SIZED INFORMATION FRAME SWITCH FOR ON-BOARD SECURITY NETWORKS	16/03/2001	5	
				EP1546300	NETWORK ACCESSIBLE APPARATUS, SECURITY METHOD USED BY THE APPARATUS, AND INFORMATION STORAGE MEDIUM THAT IS REPRODUCIB	30/09/2002	5	
				EP1497799	INTEGRATED VISUALIZATION OF SECURITY INFORMATION FOR AN INDIVIDUAL	18/04/2002	5	
				EP1418485	SECURITY AND AUTHENTICATION OF INFORMATION PROCESSING APPARATUS	06/11/2002	5	
				CN1748405	COMMUNICATION SYSTEM FOR INFORMATION SECURITY AND RECOVERY AND METHOD THEREFOR	15/01/2003	5	
				CN1466841	SMART CARD ENABLED MOBILE PERSONAL COMPUTING ENVIRONMENT SYSTEM	28/07/2000	5	
				US6795553	METHOD AND APPARATUS FOR MODULAR INVERSION FOR INFORMATION SECURITY AND RECORDING MEDIUM WITH A PROGRAM FOR IMPLEMENT	04/11/1997	4	
				US2006074917	SCALABLE AND FLEXIBLE INFORMATION SECURITY FOR INDUSTRIAL AUTOMATION	30/09/2004	4	
				US2006016000	METHOD AND DEVICE FOR ANALYZING AN INFORMATION SYSTEM SECURITY	14/01/2003	4	

Bibliographic Data	
User Comment :	
Patent number :	HK1020629
Publication date :	18/06/2004
Inventors :	HAZARD, MICHEL (-);
Applicants :	BULL CPB (FR);
IPC (4 Digits) :	G06F, H04L, G07F;

Figura AnB3 Hoja de resultados de la búsqueda en el programa de Matheo Patent

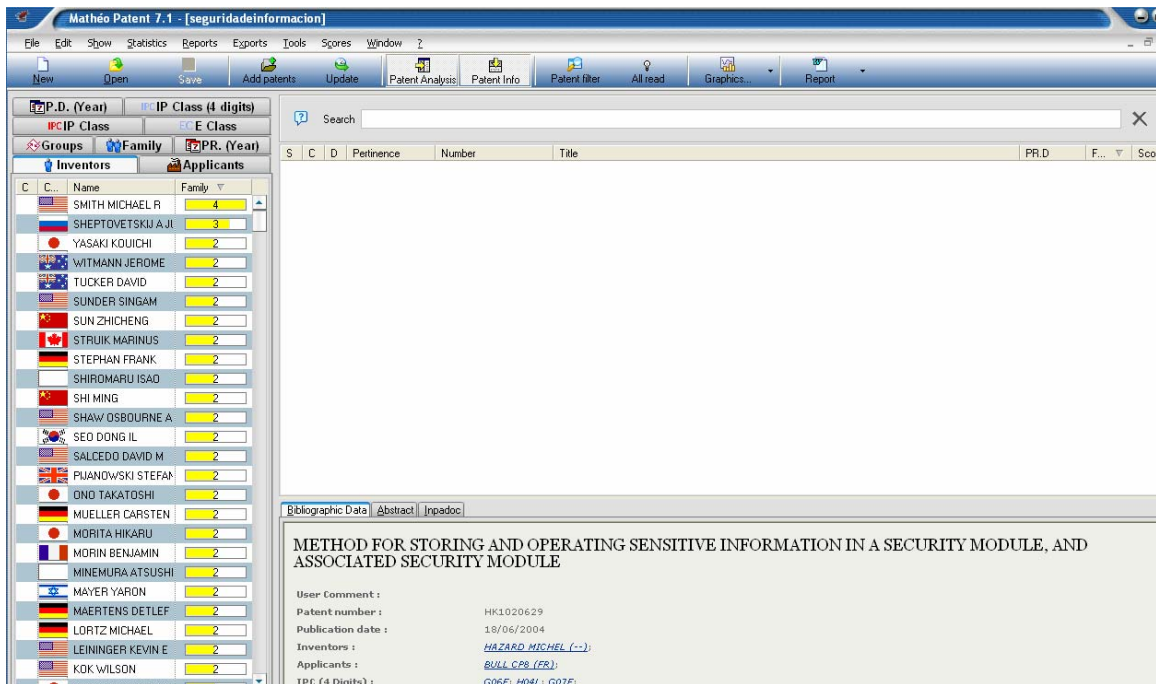


Figura AnB4 Hoja de resultados analíticos de la búsqueda en el programa de Matheo Patent

Anexo D. Composición actual de la coordinación de la RENASEC por Regiones.

Directorio de Responsables de los Nodos RENASEC Regionales de la ANUIES			
	Institución Responsable Regional	Persona Responsable	Teléfono
NOROESTE	Universidad Autónoma de Baja California	Juan Manuel Macías Jefe del Dpto. de Seguridad en Cómputo	1744666 ext. 6
	Universidad de Sonora	Ma. Antonieta Zamora Directora de Informática	(01-662) 259-2 tonyz@guayma
NORESTE	Universidad Autónoma de Coahuila	Juan Carlos Cedillo Coordinador de Seguridad en Cómputo	(844) 4164876 jcedillo@mail.
	Universidad Autónoma de Zacatecas	José de Jesús Hernández Coordinador Institucional del Centro Universitario de Computo	(01-492) 923-9 jherber@canter
CENTRO-OCCIDENTE	Universidad de Guadalajara	Arturo Gómez NOC - Network Operation Center	3331342220 ar
	Universidad de Colima	Raymundo Buenrostro Director General de Servicios Telemáticos.	01 312 316100
CENTRO-SUR	Benemérita Universidad Autónoma de Puebla	Rafael Campos Pérez Director del Sistema de Información Universitaria	(01 2) 229550 rafael@siu.bua
	Universidad Autónoma del Estado de México	Gerardo Ávila V.	(01-722)214-23 geav@coatepe
	Universidad Autónoma del Estado de México	Juan Carlos Matadamas	(01-722)214-23 jcmg@coatepe
METROPOLITANA	Universidad Autónoma Metropolitana	Gabriel Aguilar	gaguilar@corre
	El Colegio de México		
SUR-SURESTE	Universidad Autónoma de Yucatán	Carmen Díaz	23-74-28 carm
	Universidad Autónoma de Yucatán	Juan Antonio Herrera	23-74-28 hcorr
	Universidad Veracruzana	Gustavo Balderas	01-228-842179
	Universidad Veracruzana	Gabriel Lozano	01-228-842179
COORDINACIÓN	UNAM-CERT	Juan Carlos Guel Departamento de Seguridad en Cómputo - UNAM	56228169 cguel
	ANUIES	José Luis Ponce Director de Cómputo y Sistemas	54204948 jlpon

Anexo E. Resultados de las encuestas aplicadas a las IES en los años 2002, 2004 y 2006

Pregunta	Año	2002		2004	
		SI	NO	SI	NO
1. ¿Su organización contempla algún modelo de gestión de seguridad de la información?		44%	56%	53%	47%
2. ¿Usa Terceros (Outsourcing) para la gestión de la seguridad de información?		52%	48%	33%	67%
3. ¿En su organización tiene alguna forma de jerarquizar el acceso a los diferentes fuentes de información (digital)?		10%	90%	22%	78%
4. ¿Se posee las capacidades humanas suficientes para atender problemas de seguridad de la información?		28%	72%	34%	66%
5. ¿Existen redes de intercambio de información en elementos relacionados con la seguridad de la información?		44%	56%	53%	47%
6. ¿La dirección conoce las actividades de gestión de seguridad de la información?		12%	88%	42%	58%
7. ¿La dirección participa en las actividades de gestión de seguridad de la información?		11%	89%	39%	61%
8. ¿La dirección apoya las acciones de seguridad de manera económica o de recursos?		8%	92%	41%	59%
9. ¿La dirección esta involucrado y apoya en todos los niveles las acciones encaminadas a seguridad de la información?		6%	94%	30%	70%
10. ¿La dirección esta conciente de los riesgos que involucran la inseguridad de la información?		19%	81%	44%	56%
11. ¿La IES dispone de una persona (Directivo) a quien se asigne únicamente las responsabilidades de la gestión de la seguridad de la información?		5%	95%	11%	89%
12. ¿La IES dispone de recursos humanos, financieros, materiales enfocados al área de gestión tecnológica en seguridad de la información?		14%	86%	21%	79%
13. ¿Esta contemplada la Seguridad de la Información en el organigrama estructural de la organización?		0%	100%	6%	94%

	2002			2004			
	Bajo	Medio	Alto	Bajo	Medio	Alto	Baj
El IES ¿Qué nivel de gestión de seguridad de la información en Medios Digitales tiene?	70%	12%	18%	55%	32%	13%	30%
De usar outsourcing, ¿Cuál es el nivel de flujo de información que se tiene con dicho proveedor (Comunicación Proveedor Usuario)?	28%	49%	23%	11%	56%	33%	25%
	SI	No	No sabe	SI	No	No sabe	SI
El proveedor de outsourcing en seguridad ¿posee algún tipo de certificación en seguridad de la información?	15%	19%	66%	33%	22%	45%	70%
¿Sabe usted si su proveedor usa algún modelo de gestión tecnológica de la información?	0%	26%	74%	10%	24%	66%	50%
	Al momento o semanal	Mensual	Anual o nunca	Al momento o semanal	Mensual	Anual o nunca	Al mome o sem
¿Cada cuando se reporta a niveles directivos un incidente de seguridad de información digital?	23%	11%	66%	34%	25%	41%	30%

Anexo F Resultados del estudio de patentes “Palabras Claves”

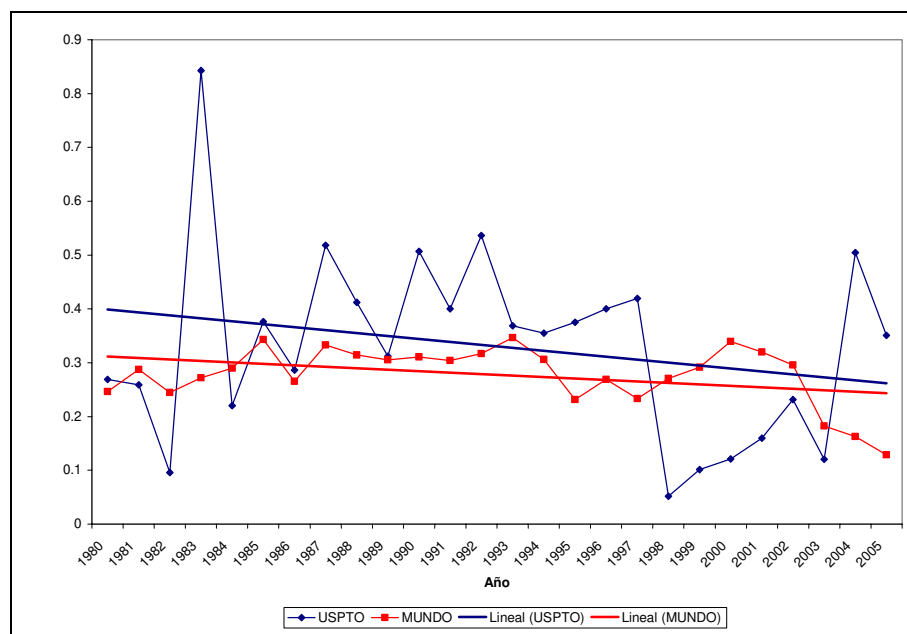


Figura c.1 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con la palabra “sistemas”, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

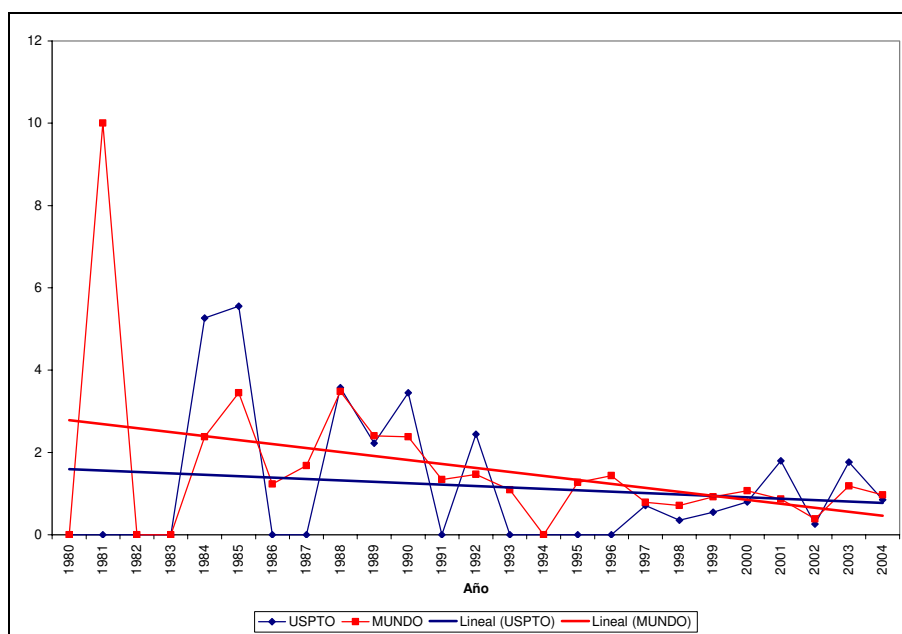


Figura c2 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con las palabras “software or hardware”, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

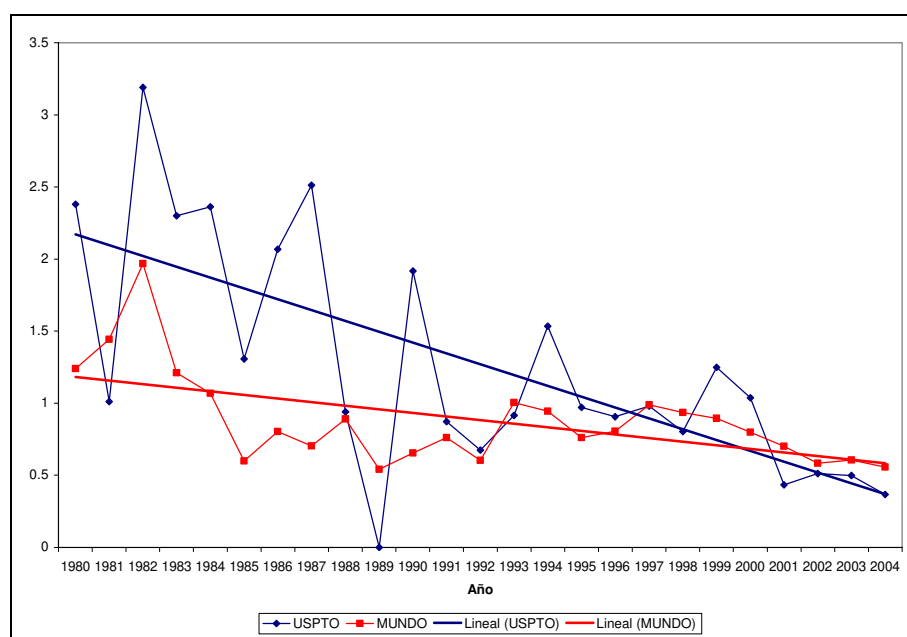


Figura c3 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con las palabras “Computer or Computing”, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

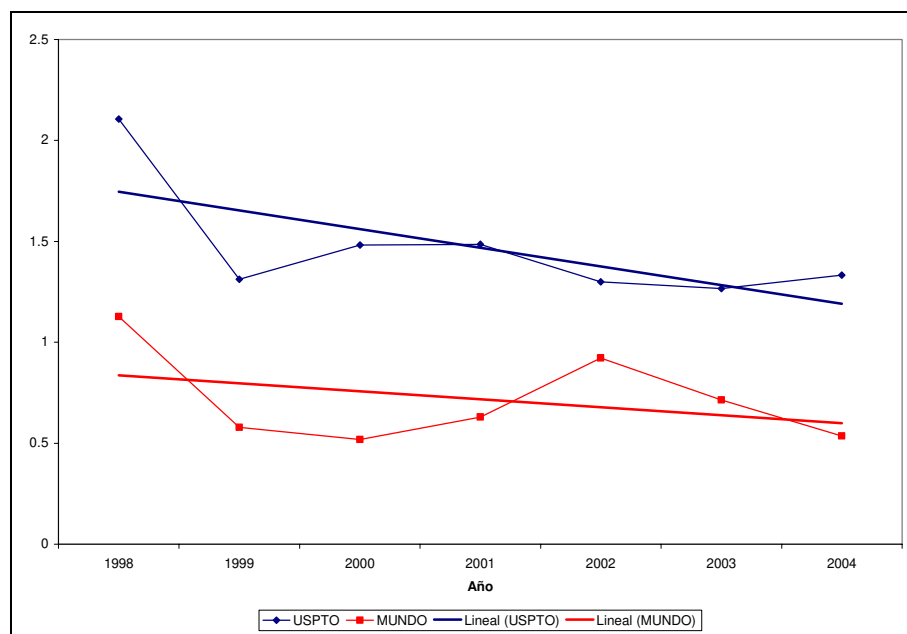


Figura c4 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con la palabra “Internet”, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

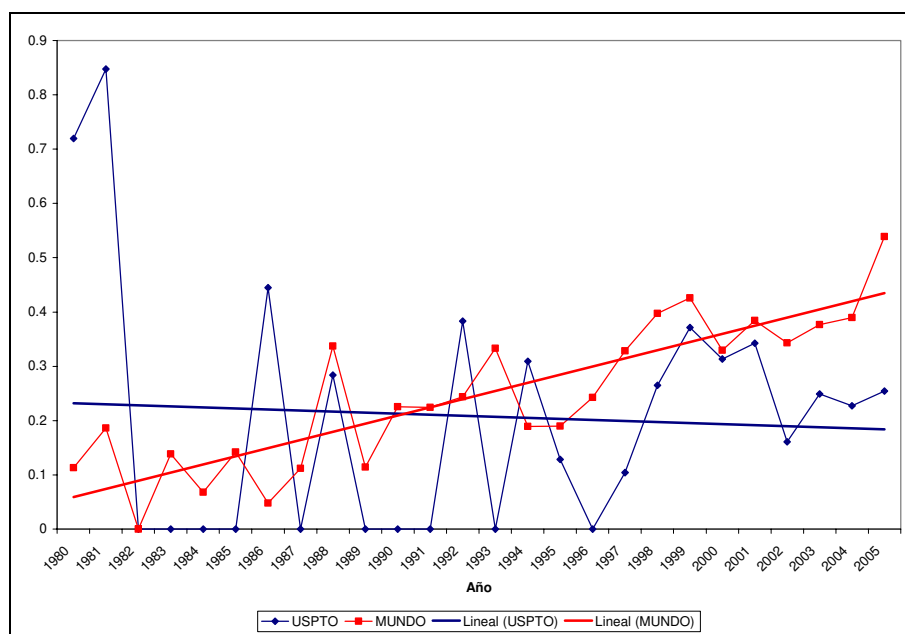


Figura c5 Tendencia de la intensidad inventiva de patentes solicitadas relacionadas con la seguridad de la Información en Medios Digitales que son correspondientes con la palabra “Information”, tanto en la USPTO como en el Mundo. Realización Propia, Fuente: Uso del software Matheo Patent que hace consultas de las bases de datos de la USPTO y de ESPaNET

