IV ENCUESTA NACIONAL SOBRE SEGURIDAD INFORMÁTICA EN MÉXICO 2010

Análisis de resultados y estudio comparativo 2007-2008-2009-2010

AUTORES: MDOH. Gabriela María Saucedo Meza, Universidad del Valle de Atemajac, Campus Guadalajara*
MAED. Celso Retama Guzmán, Colegio de Profesionales de Computación, Hidalgo**

ÍNDICE

Introducción

El interés por conocer el estado que actualmente guardan las organizaciones en el ámbito de las tecnologías de la información, específicamente en lo que respecta a Seguridad de la Información, es un tema que resulta de importancia tal, que todos los profesionales en tecnología deberíamos conocer y participar en el proceso para estar al tanto de los resultados que derivan de ello.

La Encuesta Nacional de Seguridad Informática, cuyos resultados se muestran en este documento respecto a su cuarto estudio, ha sido un ejercicio anual de reflexión en torno a las aplicaciones y percepciones de profesionales en cuestión de Seguridad Informática. Dicho ejercicio lo realiza la Facultad de Ingenierías de la Universidad del Valle de Atemajac Campus Guadalara, en colaboración con la Asociación Colombiana de Ingenieros en Sistemas (ACIS) y el Colegio de Profesionistas en Computación del Estado de Hidalgo.

En su versión 2010 México contó con la participación de 34 profesionales de Aguascalientes, Coahuila, Distrito Federal, Estado de México, Hidalgo, Jalisco, Morelos, Monterrey, Puebla y Sinaloa, quienes fueron convocados mediante invitación electrónica a contestar un instrumento con 32 preguntas clasificadas en seis rubros: demografía, presupuesto, fallas de seguridad, herramientas y buenas prácticas, políticas y capital intelectual.

Las participaciones, además de insumo para el estudio de México, se convierten también en elementos importantes para el análisis e integración de resultados de la II Encuesta Latinoamericana de Seguridad Informática.

La pregunta fundamental para entender las motivaciones de este ejercicio es la siguiente: ¿por qué es importante conocer lo que se ha realizado en el tema de la seguridad de la información?, porque al ser la información el punto clave de toda organización, se podrían dar por hecho algunos supuestos, entre otros el que el interés primordial se centra en la alta dirección y por ende de las áreas financieras, administrativas y obviamente, la de tecnología; es claro que con supuestos no se resuelve nada en claro, por tal motivo es menester indagar acerca del nivel de importancia de las actividades de seguridad de la información en las

….continuación

organizaciones, reflexionar acerca de la postura que éstas tienen y proponer acciones que coadyuven al desarrollo.

Lo anterior justifica el hecho de involucrar a profesionales de diversos sectores que puedan ser reflejo de lo que en términos generales sucede o se percibe por quienes se desarrollan en el área de TI dentro de la seguridad de la información.

Vale la pena insistir en que las actividades que conlleva la seguridad de la información, no son un ejercicio que deba realizarse por única ocasión, si la intención es minimizar el riesgo de inseguridad, tendrán que efectuarse permanentemente, y como lo indican los estándares en esta materia, son tareas perpetuas de mejora continua mismas que conforme los procesos maduran requieren ser mantenidas para el soporte de las funciones que se hallan diseñado para tal propósito, por lo que los recursos económicos y humanos deberán estar disponibles para soportar los procesos que deben ser parte de la solución a las problemáticas identificadas. De esta manera, la coordinación oportuna de los recursos humanos, procesos administrativos y las aplicaciones son parte fundamentan que coadyuvan para proporcionar estabilidad en la continuidad de las operaciones del negocio.

Lo mencionado en el párrafo anterior son apenas tópicos que si bien es cierto, no son la solución a la problemática de la seguridad de la información, son buen inicio para incursionar en este difícil proceso de su gestión.

Los usuarios de los recursos informáticos, deberíamos tener conocimiento sobre los riesgos informáticos y las amenazas más comunes a las que el personal y procesos de cualquier organización, están expuestos, mismos que pueden mitigarse cuando el personal sigue las indicaciones recibidas por los administradores de Tecnología. Estas indicaciones pueden encontrarse en políticas de seguridad de la información, reglamentos, responsabilidades, prácticas y procesos, entre otros documentos normativos que dictan las directrices de las buenas prácticas, de tal manera que, conforme se forma parte o se participa de este proceso, poco a poco estaremos generando integralmente la cultura de las buenas prácticas encaminadas a salvaguardar los activos de la organización.

El análisis que a continuación se presenta, dará cuenta del grado actual y nivel de avance que se tiene en las empresas de diversos giros en materia de seguridad.

El estudio presenta en primer instancia un análisis por cada uno de los seis rubros, posteriormente un apartado de conclusiones, cerrando con una lista de llamados a diversos grupos con la intención de buscar mejoras en ese tema en México. Adicionalmente se facilita como documento anexo, el detalle de las tablas con resultados comparativos del 2007 al 2010.

Propósito:
Identificar sectores de participación y el cargo de quién tiene asignada la responsabilidad de la seguridad informática de la organización.

ANÁLISIS DEMOGRAFÍA

Los participantes en la versión 2010 correspondieron a diversos sectores y tamaños de empresa, siendo las grandes empresas (más de 1000 empleados) las que lograron mayor intervención con un 41.1%, seguidas de las micros (de 1 a 50 empleados) con un 23.5% de participación. Estos datos llaman la atención en virtud del notorio incremento en relación a las grandes empresas.

En relación a los giros participantes se destaca el perteneciente a la educación con un 35.3% también con notorio incremento en relación a investigaciones anteriores, y con un 14.7% se presentó la participación del sector gobierno y grupos dedicados a servicios de desarrollo de software, logística y tecnologías.

Entre los respondientes se destaca con un 44.1% la participación de profesionales del departamento de sistemas en general , el punto relevante se centra en el incremento de participación de profesionales del departamento de Seguridad Informática así como de Directores o Jefes de Seguridad Informática que en conjunto suman 26.4%, casi 8 puntos porcentuales más que años anteriores, esto refleja un cambio en las organizaciones de las que se percibe han comenzado a formalizar el tema al menos en estructura organizacional. En los siguientes puntos de análisis veremos si esta realidad es consistente.

RESPONSABILIDAD DE LA S.I.	2007	2008	2009	2010
Director Departamento de Sistemas/Tecnología	38.9%	29.0%	31.3%	32.4%
No se tiene especificado formalmente	14.8%	25.8%	25.0%	14.7%
Director de Seguridad Informática	11.1%	3.2%	20.8%	**35.3%**
Auditoría interna	1.9%	6.5%	10.4%	0.0%
Otra: redes, telecomunicaciones	14.8%	3.2%	8.3%	14.7%
Gerente de Operaciones	0.0%	3.2%	4.2%	2.9%
Gerente Ejecutivo	1.9%	29.0%	0.0%	0.0%
Gerente de Finanzas	0.0%	0.0%	0.0%	0.0%

Tabla 1. Responsables de la Seguridad Informática

Otro referente para justificar un presumible cambio en la atención al tema de Seguridad en la organizaciones, es el señalamiento que hacen los participantes relacionado con el área responsable de atenderla (tabla 1), siendo en esta ocasión con un 35.3% el señalamiento de que dicha responsabilidad está en manos del Director de Seguridad Informática dato que, comparado con el 2007 refleja un incremento de 24.1 puntos y en congruente descenso con un 14.7% el señalamiento de no tener aún especificado a cargo de quién está esta tarea comparado con un 25% del 2009.

ANÁLISIS PRESUPUESTO

La gestión de la Seguridad Informática es todo un proyecto que requiere inversión tanto para infraestructura como para la preparación de responsables y usuarios. El primer aspecto a diagnosticar es si precisamente en la organización reconocen a la información como un activo a proteger, paso fundamental para evaluar el nivel de importancia que se le dan a las prácticas necesarias para una exitosa gestión. En el estudio realizado el 61.8% de los participantes manifestaron que en la organización si se reconoce a la información como un activo a proteger, un notable incremento con el año anterior que fue sólo del 47.1%.

El reconocimiento es en sí un paso importante, así como lo es la inclusión del concepto de seguridad informática en presupuesto, sobre esto el 82.4% refiere que si se está incluyendo con un porcentaje mayoritario (27.6%-Tabla 2) de entre el 3 y 5% del presupuesto destinado a TI.

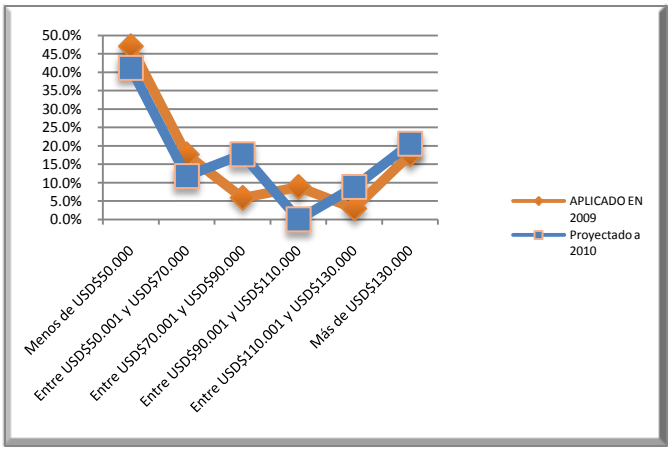
POCENTAJE DE PRESUPUESTO DE TI PARA SEGURIDAD INFORMÁTICA	2010
Entre el 0 y el 2%	20.7%
Entre el 3 y el 5%	**27.6%**
Entre el 6 y el 8%	13.8%
Entre el 9 y el 11%	20.7%
Más del 11%	17.2%

Tabla 2 Porcentaje considerado para SI en presupuesto TI

Propósito:

Revisar el presupuesto financiero destinado por las organizaciones a la gestión de la seguridad informática: distribución y montos.

En la Gráfica 1 puede observarse una tendencia a la alta en proyección del presupuesto en relación a la aplicación de éste sobre aspectos de seguridad durante el 2009, sin embargo, aunque los datos reflejan una alza y se ha señalado que es mayor la conciencia sobre la necesidad de proteger la información, el 41.2% de las empresas continúan destinando menos de cincuenta mil dólares para la gestión, en este aspecto no hay variación respecto a años anteriores.



Gráfica 1 Presupuesto ejercido y proyectado

La aplicación del presupuesto se enfoca a diferentes aspectos siendo en mayor porcentaje (88.2%) el destinado a la protección de la red, de manera general el 70.6% señala que se enfocan al cuidado de la seguridad de la información, y el 58.8% refiere que además procuran la protección de datos críticos de la organización. Entre los aspectos que por el momento menos partida presupuestaria tienen es la adquisición de pólizas de cibercrimen (8.8%) y la adquisición de bibliografía (2.9%).

ENFOQUE DEL GASTO DE SEGURIDAD EN LA ORGANIZACIÓN	2010
Protección de la red	88.2%
Proteger los datos críticos de la organización	**58.8%**
Proteger la propiedad intelectual	23.5%
Proteger el almacenamiento de datos de clientes	47.1%
Concientización/formación del usuario final	29.4%
Comercio/negocios electrónicos	11.8%
Desarrollo y afinamiento de seguridad de las aplicaciones	32.4%
Seguridad de la Información	**70.6%**
Contratación de personal más calificado	17.6%
Evaluaciones de seguridad internas y externas	20.6%
Pólizas de cibercrimen	8.8%
Cursos especializados	23.5%
Cursos de formación usuarios en seguridad informática	17.6%
Monitoreo de Seguridad Informática 7x24	38.2%
Otro, especifique: adquisiciòn bibliografía	2.9%

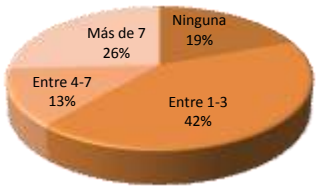
Tabla 3 Gasto en la organización

Propósito:

Revisar los tipos de ataques e incidentes de seguridad más frecuentes, así como la manera como las empresas participantes se enteran sobre ellas y a quién las notifican. También se busca conocer las causas por las cuales pueden no denunciarse estos incidentes y si se conoce lo suficiente sobre la evidencia digital.

ANÁLISIS FALLAS DE SEGURIDAD

Las buenas prácticas de seguridad, el cuidado en las comunicaciones, redes e internet, son aspectos que nos hablan de la consciencia que se tiene sobre la seguridad informática en la organización, al respecto los participantes refieren, con un 67.7% que sólo algunas personas son conscientes y si bien este porcentaje representa un avance de 30 puntos en relación a años anteriores, aún no se llega al nivel de "muy conscientes" el cual se reflejó sólo con un 25.8%. Un aspecto que estuvo a la alza fue la cantidad de intrusiones detectadas durante el 2009 (gráfica 2) que en total suman 80.6% (de 1 a más de 7) contra un 19.4% señalando que no se detectó ninguna.



Gráfica 2: Intrusiones detectadas 2009

En relación a los casos de violación , nuevamente los Virus sobresalen con una presencia del 58.8%, seguidos por la problemática que enfrentan las organizaciones al señalar que un 50% de participantes han detectado instalación de software no autorizado.

Otras violaciones referidas han sido Accesos no autorizados (29.4%), Caballos de troya (26.5%) y pérdida de información (17.6%) entre otras. En su mayoría las violaciones detectadas son comunicadas por un empleado (35.5%, tabla 4) y en porcentaje más bajo(5.9%) por seminarios o conferencias. El 44.1% indica que la denuncia se hace a equipo de atención de incidentes, pero

MEDIO DE COMUNICACIÓN DE VIOLACIONES	2010
Sistema de detección de intrusos	**32.4%**
Alertado por un cliente/proveedor	11.8%
Seminarios o conferencias Nacionales e internacionales	5.9%
Alertado por un empleado/colaborador	**35.3%**

Tabla 4. Medios de comunicación

ENTIDAD DE NOTIFICACIÓN DE DENUNCIA	2010
Autoridades nacionales	8.8%
Equipo de atención de incidentes	**44.1%**
Ninguno: No se denuncian	**20.6%**

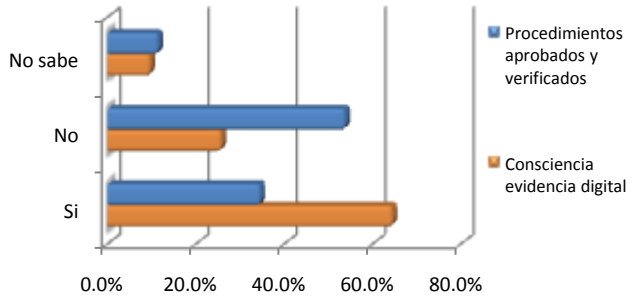
Tabla 5. Entidad de notificación

MOTIVOS PRINCIPALES DE NO DENUNCIA	2010
Motivaciones personales	**26.5%**
Vulnerabilidad ante la competencia	**23.5%**
Otro: desconocimiento, percepción no atención, falta de instrumentos legales	8.8%

Tabla 6. Motivos para no denunciar

Aún subsiste un considerable 20.6% de no denuncia (tabla 5), mencionando que el motivo principal es tanto por motivaciones personales como por visión de vulnerabilidad ante la competencia (tabla 6).

Otro aspecto importante a analizar es la consciencia en las organizaciones sobre la identificación, aseguramiento y análisis de la evidencia digital como parte del proceso de atención de incidentes relacionados con la seguridad informática, y también, detectar si existen procedimientos aprobados y verificados para administrar dicha evidencia; los resultados (gráfica 3) nos refieren que si bien hay buen nivel de consciencia en un alto porcentaje (64.5%), sólo el 34.6% manifiesta que en su organización sí se cuenta con un procedimiento aprobado y verificado.



Gráfica 3. % de Conciencia de evidencia digital y existencia de procedimientos

ANÁLISIS HERRAMIENTAS Y PRÁCTICAS DE SEGURIDAD INFORMÁTICA

En relación a la frecuencia de pruebas de seguridad aplicadas, se obtuvo un total global de 55.7% entre quienes aplican de una a más de 4, teniendo mayor porcentaje (20.4%) aquellas organizaciones que sólo realizan una al año. Con un 23.5% se encuentran organizaciones que no realizan pruebas y un 11.8% se abstuvo de contestar.

Entre los mecanismos de seguridad aplicados por las organizaciones, se observan en la tabla 7 una lista considerable, en este apartado, los participantes podían señalar todos los que utilizan. Entre los más usados están las contraseñas (76.5%), seguidas por antivirus (73.5%) y firewalls hardware (58.8%); los menos aplicados son las smartd cards y biométricos, ambos con un 17.6%, herramientas de validación de regulaciones (14.7%) y ADS (11.8%).

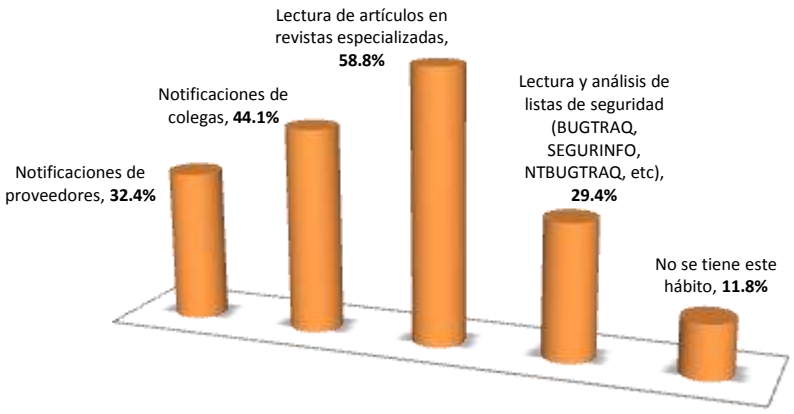
MECANISMOS UTILIZADOS PARA PROTECCIÓN DE LOS S.I	2010
Contraseñas	**76.5%**
Antivirus	**73.5%**
Firewalls Hardware	58.8%
VPN/IPSec	52.9%
Cifrado de datos	50.0%
Firewalls Software	47.1%
Monitoreo de Bases de datos	44.1%
Monitoreo 7x24	38.2%
Sistemas de prevención de intrusos - IPS	38.2%
Firmas digitales/certificados digitales	35.3%
Filtro de paquetes	32.4%
Administración de logs	29.4%
Web Application Firewalls	29.4%
Proxies	26.5%
Sistemas de detección de intrusos - IDS	26.5%
Smart Cards	17.6%
Biométricos (huella digital, iris, etc)	17.6%
Herramientas de validación de cumplimiento con regulaciones internacionales	14.7%
ADS (Anomaly detection systems)	11.8%
Otro: Tokens	2.9%

Tabla 7. Mecanismos de protección

Propósito:

Identificar la frecuencia de pruebas de la seguridad, herramientas y mecanismos para mantenerse actualizado sobre las posibles vulnerabilidades de los sistemas de información.

Se consultó a los participantes sobre los medios que utilizan para mantenerse informados en cuanto a fallas de seguridad en los sistemas utilizados, la tendencia a mantenerse informado en relación a años anteriores va en aumento, con algunas diferencias sobre el medio, pero cada vez con más bajo porcentaje entre aquellos que no tienen ese hábito (11.8% en 2010). El medio más utilizado continúa siendo la lectura de artículos en revistas especializadas (58.8%), seguido de diálogo entre colegas (44.1%) que en relación a años anteriores tuvo un incremento de 20 puntos más en promedio. En la gráfica número 4 pueden verse a detalle los resultados.



Gráfica 4. Medios informativos utilizados para conocer sobre fallas de seguridad

Propósito:

Conocer el estado que conserva la implementación de políticas de seguridad en la organización considerando su aplicación, estándares o regulaciones aplicadas, y la colaboración con autoridades nacionales/internacionales.

ANÁLISIS POLÍTICAS DE SEGURIDAD

Con resultados similares a versiones anteriores de este estudio, el 23.3% de los participantes refiere no contar aún con políticas de seguridad definidas, con un porcentaje más alto (43.3%) están las empresas que actualmente están desarrollándolas y con un 33.3% se presentan aquellas que ya cuentan con políticas bien definidas.

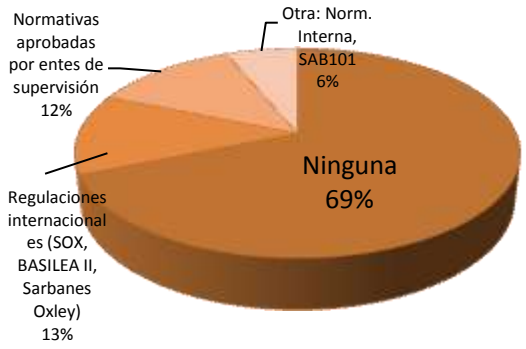
La definición de políticas es un primer paso para lograr una adecuada gestión de la seguridad informática, pero también se requiere de otros apoyos y circunstancias; en la tabla 8 pueden observarse motivos por los que las empresas consideran no han podido avanzaren este tema, siendo con un 20% la falta de apoyo directivo el obstáculo más referido.

OBSTÁCULOS PARA LOGARAR UNA ADECUADA SEGURIDAD INFORMÁTICA EN LA ORGANIZACIÓN	2010
Inexistencia de política de seguridad	13.3%
Falta de tiempo	10.0%
Falta de formación técnica	6.7%
Falta de apoyo directivo	**20.0%**
Falta de colaboración entre áreas/departamentos	**16.7%**
Complejidad tecnológica	3.3%
Poco entendimiento de la seguridad informática	13.3%
Poco entendimiento de los flujos de la información en la	6.7%
Otros:	6.7%

Tabla 8. Obstáculos para la gestión de la SI

Otro aspecto consultado fue sobre la relación o contacto con autoridades nacionales e internacionales a las que se acude para colaborar o recibir asistencia en caso de persecuciones de intrusos, al respecto el 13.3% refiere que sí, nombrándose a la Red de seguridad de ANUIES, Verisign y la Policía Cibernética, en tanto que el 53.3% refiere no contar con alguna asistencia.

Sobre las regulaciones o normativas aplicadas en la gestión de la seguridad informática, los resultados resultaron similares a investigaciones de años anteriores, ocupando el primer lugar aquellas empresas que refieren no contar con ninguna regulación (69%). En la gráfica 5 pueden analizarse en detalle los resultados del 2010.



ESTÁNDARES O BUENAS PRÁCTICAS UTILIZADOS EN LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA ORG.	2010
ITIL	44.1%
ISO 27001	29.4%
No se consideran	26.5%
Cobit 4.1	23.5%
Servicios de auditoría externa especializada	8.8%
OSSTM - Open Standard Security Testing Model	8.8%
Guías del NIST (National Institute of Standards and Technology) USA	8.8%
Otra	5.9%
Top 20 de fallas de seguridad del SANS	2.9%
Octave	2.9%
Common Criteria	2.9%

Tabla 9 Estándares y buenas prácticas aplicadas

Finalmente, podemos revisar en la tabla 9 que nos habla de las buenas prácticas empleadas por las organizaciones participantes cómo un 26.5% no considera aún su aplicación, el 44.1% se inclina por el uso de ITIL, seguido de un 29.4% que aplican el ISO2700 y COBIT con un 23.5% entre los que más destacan.

Cabe aclarar que de esta lista que se presenta, los participantes pudieron seleccionar más de una opción.

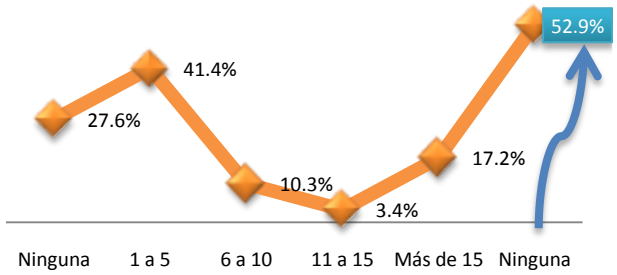
ANÁLISIS CAPITAL INTELECTUAL

En relación a los planteamientos consultados sobre la demanda de profesionales dedicados a la Seguridad Informática y su perfil, se visualizan resultados distintos a años anteriores, todos ellos con porcentajes superiores.

El 86% de los participantes comentan que es importante que el profesional dedicado a las labores de seguridad informática cuente al menos de uno a más de dos años de experiencia, el 13.8% considera que con menos de un año ya podrían dedicarse a esta labor.

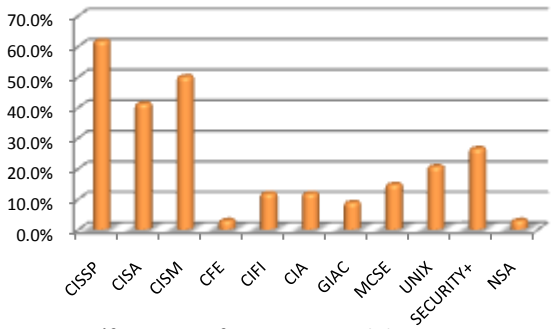
En la gráfica siguiente se muestra una relación entre el personal dedicado de tiempo completo a la seguridad y qué porcentaje de éste no cuenta con alguna certificación o especialidad, punto en donde se observa un área de oportunidad (52.9%).

Personal dedicado a SI
VS
Personal no certificado



Propósito:
Conocer la demanda del profesional en Seguridad Informática y la importancia que tiene para las organizaciones las certificaciones en este tema

El análisis reflejó que las certificaciones si tienen importancia, siendo la CISSP (Certified Information System Security Profesional) la más importante (61.8%). En la Gráfica 7 se muestran resultados detallados. De esta lista se pudieron seleccionar diversas opciones.



Gráfica 7. Certificaciones: nivel de importancia

Como aspecto final se indagó acerca de la opinión que se tiene sobre el papel de las Instituciones de Educación Superior de México en cuanto a la formación en el área de la Seguridad Informática. En ningún caso se considera la falta de motivación, el porcentaje se inclina a señalar que en su percepción la oferta es poca, escasa o nula 41.4%. La tabla 10 muestra a detalle las opiniones.

TABLA 10: Opinión sobre el papel de las Instituciones de Educación Superior en cuanto a la formación de profesionales en Seguridad de la Información.	2010
Hay poca oferta (o nula) de programas académicos en esta área	**20.7%**
La formación es escasa y sólo a nivel de cursos cortos	**20.7%**
Hacen poca difusión sobre estos temas	17.2%
Los profesores tienen poca formación académica en el tema	13.8%
Están ofreciendo programas académicos formales en esta área	10.3%
No han pensado adelantar programas académicos o cursos cortos en esta área	6.9%
Se han dejado desplazar por certificaciones generales y de producto	3.4%
Hay poca investigación científica en el área	3.4%
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	3.4%
Hay poca motivación de los estudiantes para estudiar el tema	0.0%
Los estudiantes no conocen las oportunidades laborales en esta área	0.0%
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o agremiaciones relacionadas con el tema	0.0%

CONCLUSIONES

El desarrollo de este ejercicio sólo es posible gracias a la participación de quienes atendiendo la invitación dedican su tiempo para compartir la vivencia que tienen en torno al tema de Seguridad Informática, es ésta la forma que hace posible evidenciar al menos en una muestra, cuál es el estado que dicho tema guarda en el país y nos permite además generar comentarios y llamados con la esperanza de que sean revisados y en lo posible atendidos.

La ENSI 2010 México, refleja un interesante cambio[1] a nivel de ocupación del tema de seguridad en las organizaciones pues se observa que ha crecido la necesidad de cuidar el valioso activo "información" motivo por el cual varios de los rubros consultados han tenido incremento entre ellos: la figura de un responsable de la seguridad informática tanto a nivel directivo como en tareas específicas; la asignación de presupuesto en TI va incorporando mayor porcentaje y monto para adquirir instrumentos que promuevan la seguridad, y cada vez son más y en mayor porcentaje las medidas organizacionales aplicadas.

Por otro lado, lamentablemente se observa que la inseguridad también va en aumento, dato muy acorde con las predicciones e informes que señalan por ejemplo McAfee, Pandalabs o Symantec[2]. Las organizaciones cada vez son más vulnerables, prueba de ello es el alza en el porcentaje de detección de intrusiones y las fallas informáticas encontradas desde el permanente problema de virus, como el de robo de información.

Ante esta realidad, las empresas si bien están considerando que conservar evidencias y denunciar es importante, aún permanece el paradigma de que al hacer esto último el riesgo es mayor sea personal u organizacional.

Si preguntáramos a cualquier empresario o colaborador en una organización durante cuánto tiempo desea que su empresa o la empresa en la que labora permanezca activa, seguramente un alto porcentaje contestaría que todo el tiempo posible, esto nos lleva a pensar que en sus planes no está definitivamente el que las operaciones se detengan y con ello venga la quiebra con una consecuente pérdida de empleo cuando se trata de colaboradores.

Centrado en esto es importante hacer énfasis en el papel que juega el capital intelectual, cuyos resultados en este estudio se ven favorecidos en el nivel de importancia que ahora tienen los especialistas en materia de seguridad, más no en la inversión para que éstos existan.

La falta de capacitación en esta área no permite tener la visión amplia para por lo menos saber que la información es la materia más importante y vulnerable de la organización y por tanto, el desarrollo de proyectos para resolver problemáticas en esta área llámese adopción de normativas, implementación de políticas, aplicación de presupuesto en mayor escala, elaboración e implementación de un plan de continuidad de operaciones o en su escenario ideal, la implementación de un Sistema de Gestión de Seguridad Informática, no son exitosos debido a la carencia de evidencia que apoye a la justificación de estas peticiones, entendiendo por evidencia la existencia de un adecuado presupuesto con visión de inversión y no de gasto[3], la integración de un equipo de trabajo especialista, el trabajo colaborativo entre organizaciones, la apertura a la aplicación de buenas prácticas, el interés en una permanente formación autogestiva basada en la investigación, entre otras tareas.

Finalmente, sino propiciamos y generamos la cultura del cuidado de la información como el recurso más importante de las organizaciones, el avance que se tenga en esta materia será lento, tanto que estaremos siendo rebasados por el avance tecnológico y por la evidente organización y proactiva preparación de quienes se dedican a poner en riesgo a la organización.

El interés de los directamente involucrados (personal de TI) existe, es necesario que éste sea compartido por la dirección y que en conjunto, considerando las condiciones actuales del entorno, se impongan nuevas reglas[4], sólo así, el desarrollo en las organizaciones podrán hacer frente a los nuevos desafíos informáticos.

LLAMADOS

A LAS ORGANIZACIONES

Es importante identificar la necesidad de propiciar la cultura de la seguridad de la información, si este primer paso se ha dado, entonces deben darse los pasos necesarios para asegurar que esta cultura sea aplicada por todas las áreas y en todos los niveles, esto garantiza en buena medida la continuidad de operaciones del negocio.

La vinculación es una acción no sólo de buena fe, si no de garantía de un trabajo conjunto con el que se obtengan resultados contundentes, si se ha de gestionar un plan integral de seguridad informática, es mejor tenerlo contando con apoyos gubernamentales, de proveedores y de la academia

INSTITUCIONES EDUCATIVAS

Los profesionales egresados tienen en sus manos la posibilidad de acelerar los cambios o frenarlos, se ha visto que en este momento se carecen de programas integrales en materia de Seguridad Informática, incluso existe la percepción de la falta de preparación de profesores en esta línea. Es urgente por tanto incluir en sus planes de estudios y capacitación asignaturas relacionadas con este tema al menos en las áreas financiera, administrativa e ingenieril, así como la inclusión de programas especializados que permitan al personal de TI ampliar su visión, formalizar temas vistos en cursos cortos y formar un buen juicio y ética, para la aplicación de acciones que además de mitigar riesgos, potencialicen a la organización mediante una adecuada custodia de recursos tecnológicos.

PROVEEDORES DE SERVICIOS INFORMÁTICOS

La comunicación que se tenga con los clientes es punto de partida para la creación de nuevos proyectos, valdría la pena repensar su esquema de relación con el cliente buscando que más allá de la relación comercial, se genere una alianza de apoyo basada en una permanente comunicación acerca de los riesgos, amenazas y estrategias de mitigación.

GOBIERNO

México no se ha visto envuelto en problemas críticos de ciberterrorismo pero esto no significa que no exista el riesgo, es importante y necesario reforzar los grupos de apoyo y adicionalmente contar con un plan de difusión con la intención de que lo creado sea conocido y goce de credibilidad ante las empresas.

PROFESIONALES DE TI

La actualización permanente es fundamental para enfrentar los retos y riesgos que los avances tecnológicos traen consigo, por ello es importante incluir entre las metas de desarrollo personal y profesional, hábitos de lectura, de investigación, de evaluación de metodologías, de participación en listas especializadas; conocer los conceptos, empaparse de las tendencias.

Analizar estudios estadísticos, les permitirán tener propuestas más claras para la dirección, además de convertirse en un colaborador activo que aporte información que sirva de justificación para la gestión de recursos financieros mismos que pueden tener su aplicación inmediata.

Existe una gran cantidad de informes estadísticos, listas, recomendaciones, es importante, iniciar y conservar el hábito de la lectura e investigación, sólo con profesionales preparados, podrá lograrse un auténtico desarrollo en nuestro país .

AGRADECIMIENTOS

A la Asociación Colombiana de Ingenieros en Sistemas (ACIS) por brindarnos la oportunidad de ser parte del ejercicio de investigación y análisis, y por las facilidades otorgadas para su realización y publicación.

A las personas y organismos promotores de este estudio principalmente al Dr. Manuel Mora de la Universidad Autónoma de Aguascalientes y al Colegio de Profesionistas en Computación del estado de Hidalgo.

A cada uno de los participantes por darnos su voto de confianza aportando su opinión y comentarios .

www.acis.org.co
jcano@acis.org.co

www.univa.mx
gabrielamaria.sau@univa.mx

www.copceh.org.mx
cretama@hotmail.com

REFERENCIAS

1 I ENSI México 2007, II ENSI México 2008, III ENSI México 2009
2 Consultados en http://www.securecorner.net/2009/12/informes-y-estadisticas-de-seguridad.html, última fecha de consulta 5 de junio de 2010
3 Geer, Daniel E. Jr. ScD, Economics and Strategies of Data Security, Ed. Verdasys, USA, 2008
4 Castillo Héctor, Soluciones para el desarrollo, una perspectiva organizacional; Ediciones Castillo, México, 1994

SOBRE LOS AUTORES

Celso Retama Guzmán

Lic. en Computación por la UAEH. Maestro en Administración Educativa por Universidad La Salle. Académico en la UAEH. Presidente del Colegio de Profesionistas en Computación del Estado de Hidalgo. Representante Institucional de Seguridad en Cómputo del Consejo Regional Centro - Sur de la ANUIES. Miembro de la Red de Conocimiento y Tecnologías de la Información del Consejo de Ciencia y tecnología del Estado de Hidalgo.

Gabriela María Saucedo Meza

Lic. en Sistemas Computacionales y Master en Desarrollo Organizacional y Humano por la Universidad del Valle de Atemajac; Certificación en Consultoría General por el CONOCER. Coordinador de Proyectos Institucionales en UNIVA Campus Guadalajara; Catedrática en las áreas de Sistemas e Ingeniería Industrial en Educación Superior, y a nivel Posgrados en Desarrollo Organizacional y Humano, Administración e Ingeniería de Software.

ANEXO 1

Resultados comparativos 2007-2008-2009-2010

DEMOGRAFÍA

TAMAÑO EMPRESA (por núm. de empleados)	2007	2008	2009	2010
1 a 50	26.0%	29.0%	43.8%	23.5%
51 a 100	14.0%	25.8%	6.3%	5.9%
101 a 200	0.0%	3.2%	4.2%	5.9%
201 a 300	8.0%	6.5%	4.2%	5.9%
301 a 500	14.0%	3.2%	6.3%	11.7%
501 a 1000	10.0%	3.2%	6.3%	5.9%
Más de 1000	28.0%	29.0%	29.2%	**41.1%**

SECTOR	2007	2008	2009	2010
Educación	18%	19.4%	20.8%	**35.3%**
Gobierno / Sector público	8%	3.2%	16.7%	14.7%
Construcción / Ingeniería	8%	6.5%	12.5%	0.0%
Telecomunicaciones	4%	3.2%	12.5%	2.9%
Otra (alta tecnología, Logística, Sistemas, Software)	52%	48.4%	12.5%	14.7%
Consultoría Especializada			10.4%	11.8%
Servicios Financieros y Banca	0%	6.5%	6.3%	5.9%
Manufactura	4%	6.5%	4.2%	5.9%
Hidrocarburos	0%	0.0%	2.1%	0.0%
Alimentos	0%	0.0%	2.1%	2.9%
Salud	6%	6.5%	0.0%	2.9%
Sector Energía				2.9%
Fuerzas Armadas				0.0%

RESPONSABILIDAD DE LA S.I.	2007	2008	2009	2010
Director Departamento de Sistemas/Tecnología	38.9%	29.0%	31.3%	32.4%
No se tiene especificado formalmente	14.8%	25.8%	25.0%	14.7%
Director de Seguridad Informática	11.1%	3.2%	20.8%	**35.3%**
Auditoría interna	1.9%	6.5%	10.4%	0.0%
Otra: redes, telecomunicaciones	14.8%	3.2%	8.3%	14.7%
Gerente de Operaciones	0.0%	3.2%	4.2%	2.9%
Gerente Ejecutivo	1.9%	29.0%	0.0%	0.0%
Gerente de Finanzas	0.0%	0.0%	0.0%	0.0%

CARGOS DE LOS PARTICIPANTES EN LA ENSI	2007	2008	2009	2010
Profesional de Departamento de Sistemas/Tecnología	51.9%	33.3%	41.7%	**44.1%**
Profesional del Departamento de Seguridad Informática	1.9%	7.4%	14.6%	17.6%
Auditor Interno	0.0%	0.0%	10.4%	0.0%
Otra: Administrativo, Asistente, Docente, Jefe de área	20.4%	25.9%	10.4%	8.8%
Presidente/Gerente General	5.6%	7.4%	8.3%	8.8%
Director Ejecutivo	5.6%	7.4%	6.3%	0.0%
Director/Jefe de Seguridad Informática	1.9%	11.1%	4.2%	8.8%
Asesor externo	0.0%	0.0%	4.2%	8.8%
Director/Vicepresidente	1.9%	7.4%	0.0%	2.9%

PRESUPUESTO

PRESUPUESTO: inclusión de concepto de seguridad informática	2007	2008	2009	2010
Si	76.6%	77.8%	45.8%	**82.4%**
No	23.4%	22.2%	25.0%	17.6%

PORCENTAJE DE PRESUPUESTO DE TI PARA SEGURIDAD INFORMÁTICA	2007	2008	2009	2010
Entre el 0 y el 2%				20.7%
Entre el 3 y el 5%				**27.6%**
Entre el 6 y el 8%				13.8%
Entre el 9 y el 11%				20.7%
Más del 11%				17.2%

RECONOCIMIENTO DE LA INFORMACIÓN COMO ACTIVO A PROTEGER	2007	2008	2009	2010
Si			47.1%	**61.8%**
No			17.6%	8.8%
Sólo algunas personas			35.3%	29.4%

PRESUPUESTO

ENFOQUE DEL GASTO DE SEGURIDAD EN LA ORGANIZACIÓN	2007	2008	2009	2010
Protección de la red		88.9%	64.7%	**88.2%**
Proteger los datos críticos de la organización		74.1%	61.8%	**58.8%**
Proteger la propiedad intelectual		40.7%	23.5%	23.5%
Proteger el almacenamiento de datos de clientes		55.6%	50.0%	47.1%
Concientización/formación del usuario final		48.1%	20.6%	29.4%
Comercio/negocios electrónicos		29.6%	20.6%	11.8%
Desarrollo y afinamiento de seguridad de las aplicaciones		40.7%	26.5%	32.4%
Seguridad de la Información				**70.6%**
Contratación de personal más calificado		22.2%	14.7%	17.6%
Evaluaciones de seguridad internas y externas		40.7%	26.5%	20.6%
Pólizas de cibercrimen		3.7%	8.8%	8.8%
Cursos especializados		33.3%	35.3%	23.5%
Cursos de formación usuarios en seguridad informática		25.9%	14.7%	17.6%
Monitoreo de Seguridad Informática 7x24		40.7%	35.3%	38.2%
Otro, especifique: adquisiciòn bibliografía		11.1%	11.8%	2.9%
Asesores de seguridad informática		25.9%	52.9%	

PRESUPUESTO DE SEGURIDAD DURANTE EL AÑO ANTERIOR (2009)	2007	2008	2009	2010
Menos de USD$50.000	54.8%	48.1%	50.0%	**47.1%**
Entre USD$50.001 y USD$70.000	14.3%	18.5%	14.7%	17.6%
Entre USD$70.001 y USD$90.000	2.4%	7.4%	5.9%	5.9%
Entre USD$90.001 y USD$110.000	7.1%	0.0%	2.9%	8.8%
Entre USD$110.001 y USD$130.000	0.0%	7.4%	5.9%	2.9%
Más de USD$130.000	21.4%	18.5%	25.1%	17.6%

PROYECCIÓN DE PRESPUESTO PARA EL AÑO ACTUAL (2010)	2007	2008	2009	2010
Menos de USD$50.000	52.4%	44.4%	41.2%	**41.2%**
Entre USD$50.001 y USD$70.000	4.8%	11.1%	17.6%	11.8%
Entre USD$70.001 y USD$90.000	11.9%	11.1%	8.8%	17.6%
Entre USD$90.001 y USD$110.000	7.1%	3.7%	2.9%	0.0%
Entre USD$110.001 y USD$130.000	2.4%	3.7%	8.8%	8.8%
Más de USD$130.000	21.4%	25.9%	20.6%	**20.6%**

FALLAS DE SEGURIDAD

CONSCIENCIA SOBRE SEGURIDAD INFORMÁTICA EN LA ORGANIZACIÓN: Buenas prácticas de seguridad, comunicaciones, redes y Seguridad en Internet	2007	2008	2009	2010
Muy conscientes	52.0%	54.8%	12.5%	25.8%
Algunas personas son conscientes	46.0%	38.7%	35.4%	**67.7%**
Nadie es consciente	0.0%	6.5%	10.4%	3.2%
No sabe/en blanco	2.0%	0.0%	41.7%	3.2%

INTRUSIONES IDENTIFICADAS AÑO ANTERIOR	2007	2008	2009	2010
Ninguna	44.4%	25.9%	0.0%	19.4%
Entre 1-3	31.1%	37.0%	8.3%	**41.9%**
Entre 4-7	8.9%	11.1%	10.4%	12.9%
Más de 7	11.1%	25.9%	14.5%	25.8%

CASOS DE VIOLACIONES AÑO ANTERIOR	2007	2008	2009	2010
Ninguno		5.6%	4.2%	11.8%
Manipulación de aplicaciones de software		11.1%	18.8%	11.8%
Instalación de software no autorizado		50.0%	31.3%	**50.0%**
Accesos no autorizados al web		44.4%	27.1%	29.4%
Fraude		5.6%	2.1%	8.8%
Virus		88.9%	50.0%	**58.8%**
Robo de datos		11.1%	8.3%	8.8%
Caballos de troya		44.4%	6.3%	**26.5%**
Monitoreo no autorizado del tráfico		5.6%	8.3%	8.8%
Negación del servicio		11.1%	10.4%	11.8%
Pérdida de integridad		5.6%	4.2%	2.9%
Pérdida de información		22.2%	12.5%	17.6%
Suplantación de identidad		16.7%	4.2%	5.9%
Phishing		22.2%	10.4%	14.7%
Pharming		5.6%	4.2%	5.9%
Espionaje				**11.8%**
Fuga de información				8.8%
Otra: Intento ataque Firewall, SPAM		5.6%	10.4%	5.9%

FALLAS DE SEGURIDAD

MEDIO DE COMUNICACIÓN DE VIOLACIONES	2007	2008	2009	2010
Material o datos alterados	15.9%	33.3%	16.7%	23.5%
Análisis de registros de auditoría/sistema de archivos/registros Firewall	29.5%	66.7%	33.3%	26.5%
Sistema de detección de intrusos	25.0%	44.4%	33.3%	**32.4%**
Alertado por un cliente/proveedor	15.9%	16.7%	10.4%	11.8%
Alertado por un colega	6.8%	22.2%	8.3%	23.5%
Seminarios o conferencias Nacionales e internacionales	2.3%	5.6%	0.0%	5.9%
Alertado por un empleado/colaborador			22.9%	**35.3%**
Otra: antivirus, no ha habido intrusiones	4.5%	5.6%	8.3%	11.8%

ENTIDAD DE NOTIFICACIÓN DE DENUNCIA	2007	2008	2009	2010
Asesor legal	8.0%	16.7%	12.5%	11.8%
Autoridades locales/regionales	4.0%	16.7%	10.4%	17.6%
Autoridades nacionales	0.0%	0.0%	8.3%	8.8%
Equipo de atención de incidentes	48.0%	44.4%	22.9%	**44.1%**
Ninguno: No se denuncian	40.0%	38.9%	22.9%	**20.6%**
Otra: Director, Eq. Seguridad, Corporativo, Solución interna, grupo seguridad institucional				17.64

MOTIVOS PRINCIPALES DE NO DENUNCIA	2007	2008	2009	2010
Pérdida de valor de accionistas	12.5%	22.2%	4.2%	11.8%
Publicación de noticias desfavorables en los medios/pérdida de imagen	16.7%	38.9%	8.3%	17.6%
Responsabilidad legal	8.3%	5.6%	12.5%	20.6%
Motivaciones personales	12.5%	50.0%	14.5%	**26.5%**
Vulnerabilidad ante la competencia	20.8%	22.2%	16.6%	**23.5%**
Otro: desconocimiento, percepción no atención, falta de instrumentos legales	29.2%	5.6%	18.7%	8.8%

CONSCIENCIA SOBRE EVIDENCIA DIGITAL: identificación, aseguramiento y análisis como parte del proceso de atención de incidentes de SI	2007	2008	2009	2010
Si	80.0%	65.2%	29.2%	**64.5%**
No	20.0%	13.0%	20.8%	25.8%
No sabe	0.0%	21.7%	8.3%	9.7%

PROCEDIMIENTO APROBADO Y VERIFICADO PARA LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL	2007	2008	2009	2010
Si			12.5%	34.6%
No			25.0%	**53.8%**
No sabe			8.3%	11.5%

HERRAMIENTAS

FRECUENCIA DE PRUEBAS DE SEGURIDAD EN LA ORGANIZACIÓN	2007	2008	2009	2010
Una al año	25.0%	21.7%	12.5%	20.4%
Entre 2 y 4 al año	27.5%	21.7%	18.8%	17.6%
Más de 4 al año	20.0%	21.7%	8.3%	17.6%
Ninguna	27.5%	34.8%	16.7%	**23.5%**
Sin respuesta			43.8%	11.8%

MEDIO INFORMATIVO SOBRE FALLAS DE SEGURIDAD EN LOS SISTEMAS	2007	2008	2009	2010
Notificaciones de proveedores	29.6%	34.8%	16.7%	32.4%
Notificaciones de colegas	40.7%	26.1%	20.8%	44.1%
Lectura de artículos en revistas especializadas	27.8%	78.3%	33.3%	**58.8%**
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)	25.9%	13.0%	22.9%	29.4%
No se tiene este hábito	18.5%	17.4%	10.4%	11.8%

HERRAMIENTAS

MECANISMOS UTILIZADOS PARA PROTECCIÓN DE LOS S.I	2007	2008	2009	2010
Smart Cards	9.3%	26.1%	14.6%	17.6%
Biométricos (huella digital, iris, etc)	9.3%	26.1%	25.0%	17.6%
Antivirus	70.4%	91.3%	50.0%	**73.5%**
Contraseñas	68.5%	87.0%	47.9%	**76.5%**
Cifrado de datos	50.0%	52.2%	31.3%	50.0%
Filtro de paquetes	31.5%	30.4%	25.0%	32.4%
Firewalls Hardware	44.4%	56.5%	35.4%	**58.8%**
Firewalls Software	59.3%	65.2%	39.6%	47.1%
Firmas digitales/certificados digitales	31.5%	30.4%	22.9%	35.3%
VPN/IPSec	40.7%	60.9%	33.3%	52.9%
Proxies	37.0%	39.1%	20.8%	26.5%
Sistemas de detección de intrusos – IDS	25.9%	17.4%	29.2%	26.5%
Monitoreo 7x24	29.6%	30.4%	20.8%	38.2%
Sistemas de prevención de intrusos – IPS	14.8%	30.4%	18.8%	38.2%
Administración de logs	0.0%	34.8%	22.9%	29.4%
Web Application Firewalls	0.0%	43.5%	20.8%	29.4%
Monitoreo de Bases de datos				44.1%
ADS (Anomaly detection systems)	13.0%	13.0%	4.2%	11.8%
Herramientas de validación de cumplimiento con regulaciones internacionales			6.3%	14.7%
Otro: Tokens				2.9%

POLÍTICAS

DESCRIPCIÓN DE POLÍTICAS DE SEGURIDAD EN LA ORGANIZACIÓN	2007	2008	2009	2010
No se tienen políticas de seguridad definidas	20.0%	43.5%	20.8%	23.3%
Actualmente se encuentran en desarrollo	40.0%	26.1%	14.6%	**43.3%**
Política formal, escrita documentada e informada a todo el personal	40.0%	30.4%	20.8%	33.3%

OBSTÁCULOS PARA LOGRAR UNA ADECUADA SEGURIDAD INFORMÁTICA EN LA ORGANIZACIÓN	2007	2008	2009	2010
Inexistencia de política de seguridad	22.2%	39.1%	7.4%	13.3%
Falta de tiempo	24.1%	52.2%	11.1%	10.0%
Falta de formación técnica	27.8%	30.4%	11.1%	6.7%
Falta de apoyo directivo	25.9%	26.1%	22.2%	**20.0%**
Falta de colaboración entre áreas/departamentos	29.6%	26.1%	25.9%	**16.7%**
Complejidad tecnológica	16.7%	17.4%	7.4%	3.3%
Poco entendimiento de la seguridad informática	16.7%	13.0%	7.4%	13.3%
Poco entendimiento de los flujos de la información en la organización			3.7%	6.7%
Otros:	9.3%	13.0%	3.7%	6.7%

ESTÁNDARES O BUENAS PRÁCTICAS UTILIZADOS EN LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA ORG.	2007	2008	2009	2010
ISO 27001		26.1%	8.3%	29.4%
Common Criteria		17.4%	4.2%	2.9%
Cobit 4.1		17.4%	12.5%	23.5%
Magerit		4.3%	2.1%	0.0%
Octave		4.3%	2.1%	2.9%
Guías del NIST (National Institute of Standards and Technology) USA		17.4%	4.2%	8.8%
Guías de la ENISA (European Network of Information Security Agency)		0.0%	0.0%	0.0%
Top 20 de fallas de seguridad del SANS		1.3%	4.2%	2.9%
OSSTM - Open Standard Security Testing Model		13.0%	10.4%	8.8%
ISM3 - Information Security Management Maturiy Model		8.7%	6.3%	0.0%
ITIL			10.4%	**44.1%**
Servicios de auditoría externa especializada				8.8%
No se consideran			31.3%	26.5%
Otra		47.8%	4.2%	5.9%

POLÍTICAS

ASISTENCIA EN CASO DE PERSECUCIONES DE INSTRUSOS: contactos o relaciones con autoridades nacionales e internacionales	2007	2008	2009	2010
No	42.5%	65.2%	48.1%	**53.3%**
Si, ¿Cuáles?: Red Seg ANUIES, Verisign, Policía Cibernética	22.5%	13.0%	14.8%	13.3%

REGULACIÓN O NORMATIVA APLICADA EN GESTIÓN DE SEGURIDAD DE INFORMACIÓN	2007	2008	2009	2010
Ninguna		78.3%	60.7%	**64.7%**
Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)		0.0%	17.9%	11.8%
Otra: Norm. Interna, SAB101		8.7%	7.1%	5.9%

CAPITAL INTELECTUAL

PERSONAL DE TIEMPO COMPLETO DEDICADO A LA SEGURIDAD INFORMÁTICA	2007	2008	2009	2010
Ninguna	18.0%	25.8%	20.8%	27.6%
1 a 5	52.0%	45.2%	18.8%	**41.4%**
6 a 10	10.0%	3.2%	4.2%	10.3%
11 a 15	4.0%	3.2%	4.2%	3.4%
Más de 15	16.0%	22.6%	8.3%	17.2%

AÑOS DE EXPERIENCIA MÍNIMA PARA OBTENER UN CARGO EN EL ÁREA DE SEGURIDAD INFORMÁTICA	2007	2008	2009	2010
Ninguno	5.4%	13.0%	51.9%	0.0%
Menos de un año de experiencia	10.8%	4.3%	11.1%	13.8%
Uno a dos años	35.1%	26.1%	22.2%	**44.8%**
Más de dos años de experiencia	48.6%	56.5%	14.8%	41.4%

PERSONAL CON CERTIFICACIONES RELACIONADAS CON SEGURIDAD INFORMÁTICA, EN LAS ORGANIZACIONES	2007	2008	2009	**2010**
Ninguna	44.2%	39.1%	39.6%	**52.9%**
CISSP - Certified Information System Security Professional	11.5%	30.4%	10.4%	23.5%
CISA - Certified Information System Auditor	13.5%	26.1%	6.3%	14.7%
CISM - Certified Information Security Manager	15.4%	30.4%	6.3%	14.7%
CFE - Certified Fraud Examiner	3.8%	8.7%	0.0%	2.9%
CIFI - Certified Information Forensics Investigator	3.8%	8.7%	0.0%	2.9%
CIA - Certified Internal Auditor	7.7%	13.0%	2.1%	2.9%
GIAC – SANS Institute				5.9%
SECURITY+	0.0%	13.0%	4.2%	5.9%
NSA IAM/IEM				0.0%
Otra: OPSA, OPST, CEH, OPSA, ISO27001 Lead Auditor	11.5%	34.8%	8.3%	8.8%

CERTIFICACIONES SEGURIDAD INFORMÁTICA: nivel de importancia para que sean recibidas por los empleados	2007	2008	2009	**2010**
CISSP – Certified Information System Security Professional			44.0%	**61.8%**
CISA – Certified Information System Auditor			39.0%	**41.2%**
CISM – Certified Information Security Manager			37.2%	**50.0%**
CFE - Certified Fraud Examiner			31.7%	2.9%
CIFI – Certified Information Forensics Investigator			28.2%	11.8%
CIA - Certified Internal Auditor			33.9%	11.8%
GIAC – SANS Institute				8.8%
MCSE/ISA-MCP (Microsoft)			30.5%	14.7%
Unix/Linux LP1			30.1%	20.6%
Security+			29.4%	26.5%
NSA IAM/IEM				2.9%