

III Encuesta Nacional sobre Seguridad Informática en México 2009

Análisis de resultados y estudio comparativo 2007-2008-2009



Autor: MDOH. Gabriela María Saucedo Meza*
Mayo 2009

Análisis de resultados y estudio comparativo 2007-2008-2009

Conocer posturas, analizar tendencias e inferir posibles riesgos, todo en materia de Seguridad Informática dentro de las organizaciones, es el ejercicio que por tercera ocasión realiza el Departamento de Sistemas e Industrial de la Universidad del Valle de Atemajac (UNIVA), Campus Guadalajara – México – en colaboración con la Asociación Colombiana de Ingenieros en Sistemas (ACIS).

A esta práctica de análisis se integra también el Centro de Atención de Incidentes de Seguridad Informática y Telecomunicaciones – ANTEL de Uruguay quien tendrá la tarea de evaluar los resultados de las participaciones en Uruguay.

● ● ●
Aceptar nuestra vulnerabilidad en lugar de tratar de ocultarla es la mejor manera de adaptarse a la realidad.
David Viscott

La información recopilada tanto de México como de Uruguay, ha sido insumo para la elaboración del estudio de la Primer Encuesta Latinoamericana de Seguridad Informática 2009, misma que se llevó a cabo mediante el esfuerzo conjunto entre ACIS, ANTEL y UNIVA.

● ● ●
El presente informe, corresponde exclusivamente al análisis de datos proporcionados por empresas mexicanas, quienes, fueron convocadas vía electrónica para participar como colaboradoras del estudio, respondiendo, en línea, una encuesta con 32 rubros clasificados en las categorías: *demografía, Presupuesto, Fallas de Seguridad, Herramientas y prácticas de seguridad informática, Políticas de seguridad y Capital Intelectual.*

Este 2009, se logró la participación de 48 empresas voluntarias, de los estados de Aguascalientes, Baja California Norte, Chihuahua, Colima, Distrito Federal, Estado de México, Guanajuato, Jalisco, Oaxaca, Puebla, Querétaro, Quintana Roo y Yucatán, con cuya participación se ha podido realizar un sondeo de cuál es el estado que guarda el tema de la Gestión de la Seguridad de la Información, reflejando de alguna manera las vulnerabilidades que, desde una visión proactiva, permitirán en este estudio, adicional al estudio comparativo 2007-2008-2009, establecer las tendencias de gestión y la presentación de algunas recomendaciones que coadyuven a las organizaciones en su proceso de adaptación ante las realidades que la inseguridad informática presenta hoy en día.

Categoría: Demografía

Este 2009, la participación de las pequeñas empresas fue la más fuerte (43.8%) al igual que en los años anteriores, seguida de las grandes empresas (más de 1000 empleados) con un 29.2%.

Se observó un visible incremento de participación en la mayoría de los giros, destacando nuevamente el sector educativo y figurando por primera ocasión el de la Consultoría con un 10.4%. Con los resultados mostrados en la tabla No. 1, se entiende que, el área de las TIC'S es ya considerada en todos los giros, independientemente del tamaño de la empresa.

	2007	2008	2009
Educación	18%	19.4%	20.8%
Gobierno / Sector público	8%	3.2%	16.7%
Construcción / Ingeniería	8%	6.5%	12.5%
Telecomunicaciones	4%	3.2%	12.5%
Otra	52%	48.4%	12.5%
Consultoría			10.4%
Servicios Financieros y Banca	0%	6.5%	6.3%
Manufactura	4%	6.5%	4.2%
Hidrocarburos	0%	0.0%	2.1%
Alimentos	0%	0.0%	2.1%
Salud	6%	6.5%	0.0%

Llama la atención el notorio incremento -del 3% en el 2008 al 20.83% en el 2009- sobre la presencia del puesto de Director de Seguridad Informática, lo que podría llevar a deducir que, efectivamente la información está siendo ya considerada como un valioso activo por el que bien vale la pena hacer inversiones en la estructura organizacional, y que las responsabilidades están tomando ya un rumbo de especialización, dato que puede corroborarse con un 0% de atención de la SI por parte de las gerencias ejecutivas y de finanzas, quienes, derivado quizá de la situación económica actual en México, su interés está centrado en la creación de estrategias que permitan salvaguardar el negocio desde la postura económica.

	2007	2008	2009
Director Departamento de Sistemas/Tecnología	38.9%	29%	31.25%
No se tiene especificado formalmente	14.8%	26%	25.00%
Director de Seguridad Informática	11.1%	3%	20.83%
Auditoría interna	1.9%	6%	10.41%
Otra (Por favor especifique)	14.8%	3%	8.33%
Gerente de Operaciones	0.0%	3%	4.16%
Gerente Ejecutivo	1.9%	29%	0.00%
Gerente de Finanzas	0.0%	0%	0.00%

● ● ●

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

● ● ●

Uno de los puntos de interés fue conocer a cargo de quién están las tareas de Gestión de la Seguridad. Coincidiendo con años anteriores, la tarea es para el personal de tecnologías de información, sin embargo, aún destaca un 25% señalado por los participantes en cuyas empresas no se define un puesto en particular para esta actividad.

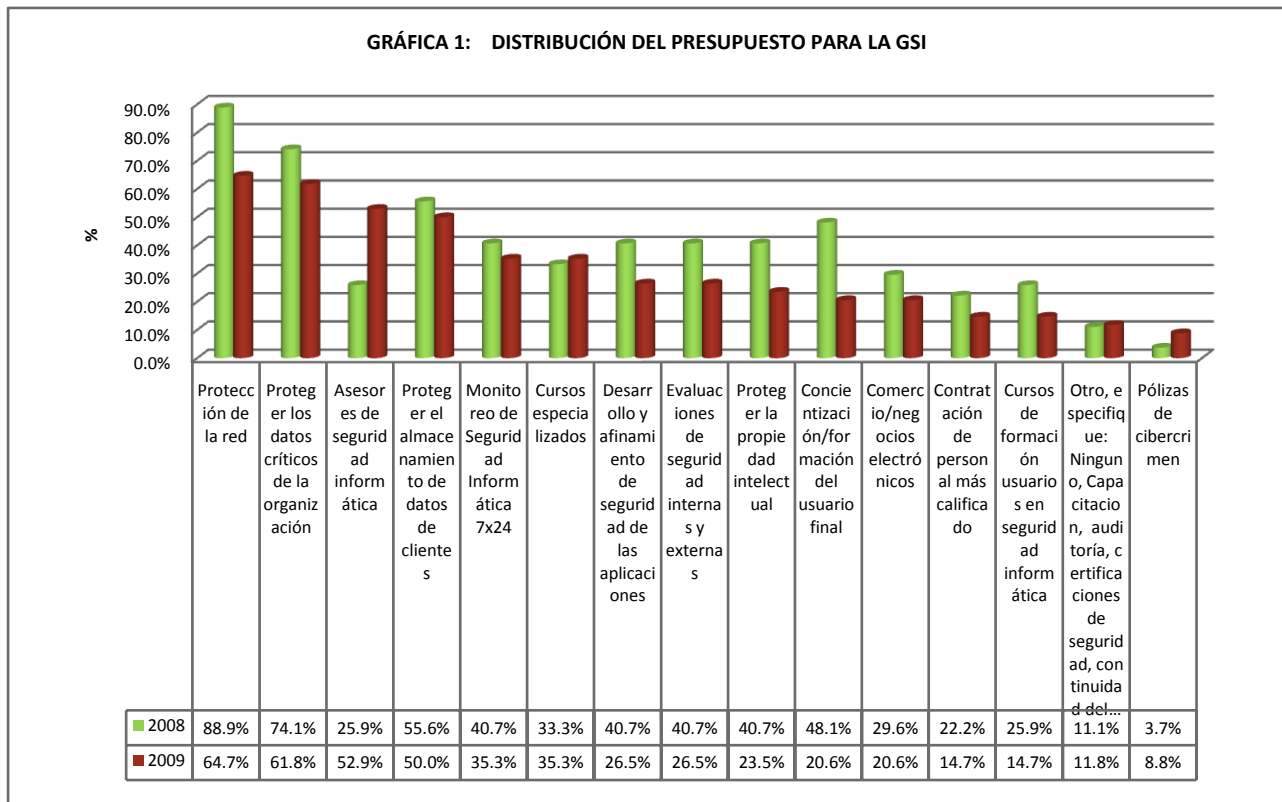
Categoría: Presupuesto

La distribución de presupuestos para cubrir las necesidades de todas las áreas de una organización, se ha ido consolidando, en particular para la gestión de la seguridad informática, sin embargo, parece que es necesario que los responsables de dicha gestión insistan aún más pues el promedio de empresas que aún no lo incluyen, de acuerdo a nuestro sondeo y comparativo 2007 a 2009, es del 23.5%.

Para este 2009, el presupuesto asignado por aspectos, puede analizarse en la gráfica 1:

Propósito:

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



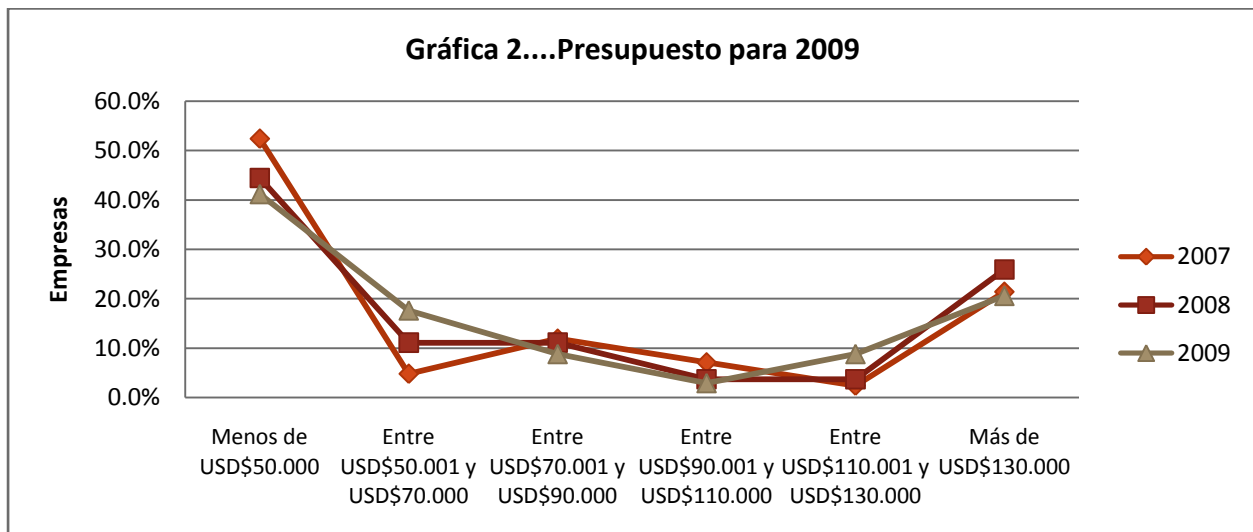
Salvo en dos casos, la distribución de presupuesto tiende a la baja durante este 2009 en relación al año anterior, derivado posiblemente de la crisis económica global. Los aspectos que resaltan con un considerable incremento y que pueden ser vistos como un área de oportunidad son: *pago a asesores de seguridad informática*, que en este 2009 muestra un incremento al 52.9% contra 25.9% del 2008 y *cursos de especialización* con un ligero aumento del 2%. Esta distribución durante el 2009, habla también del interés de las organizaciones en contar tanto con personal más preparado sobre SI, como en la apertura para recibir orientación de cómo mejorar los procesos de SI.

En relación a la cantidad de presupuesto asignado, vemos en las tablas 3 y 4 cómo fue distribuido por el área financiera en el 2008 y para este 2009. En ambas puede apreciarse que la tendencia es a la baja, coincidiendo como lo señalan en artículo de la revista CIO de México “Los CIOs continuarán haciendo frente a presupuestos y planes de inversión cada vez más reducidos, esto de acuerdo con la Confederación de la Industria británica (Confederation of British Industry)”¹.

En el gráfico puede apreciarse que en su mayoría, las empresas asignan menos de 50,000 USD para la atención de la inseguridad, que si bien en comparación con el rango siguiente (Entre 50 y 70 mil USD) que tuvo un aumento significativo en relación al 2007. 2008, sigue estando por debajo de la cantidad de empresas que han realizado esta distribución.

TABLA 3 PRESUPUESTO DE SEGURIDAD DURANTE EL 2008	2007	2008	2009
Menos de USD\$50.000	54.8%	48.1%	50.0%
Más de USD\$130.000	21.4%	18.5%	25.1%
Entre USD\$50.001 y USD\$70.000	14.3%	18.5%	14.7%
Entre USD\$70.001 y USD\$90.000	2.4%	7.4%	5.9%
Entre USD\$110.001 y USD\$130.000	0.0%	7.4%	5.9%
Entre USD\$90.001 y USD\$110.000	7.1%	0.0%	2.9%

TABLA 4 PROYECCIÓN DE PRESUPUESTO PARA EL AÑO ACTUAL	2007	2008	2009
Menos de USD\$50.000	52.4%	44.4%	41.2%
Más de USD\$130.000	21.4%	25.9%	20.6%
Entre USD\$50.001 y USD\$70.000	4.8%	11.1%	17.6%
Entre USD\$70.001 y USD\$90.000	11.9%	11.1%	8.8%
Entre USD\$110.001 y USD\$130.000	2.4%	3.7%	8.8%
Entre USD\$90.001 y USD\$110.000	7.1%	3.7%	2.9%



Categoría: Fallas de seguridad

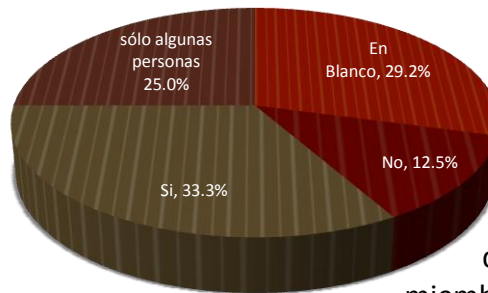


Propósito:

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..



El primer aspecto que en esta categoría se quiso evaluar, es sobre la percepción que se tiene en relación al valor de la información, considerando ésta como un activo (se define así dado que la información se ha vuelto un factor de peso para el crecimiento de las organizaciones).



Los resultados que refleja este gráfico resultan preocupantes pues menos de la mitad de participaciones señalan que efectivamente todos los miembros de la empresa

consideran que la información es un activo más a proteger. Esta situación se confirma por un escaso 12.5% como respuesta al nivel de conciencia de las organizaciones sobre la importancia de la Seguridad Informática.

Otro dato que resulta interesante es la disminución de identificación de intrusiones, que en buena medida puede obedecer a los niveles de seguridad que se han ido estableciendo y al

	2007	2008	2009
Ninguna	44.4%	25.9%	0.0%
Entre 1-3	31.1%	37.0%	8.3%
Entre 4-7	8.9%	11.1%	10.4%
Más de 7	11.1%	25.9%	14.5%

crecimiento en cultura informática de la sociedad. De hecho, en la tabla No. 6 puede apreciarse también una baja en situaciones críticas detectadas, aún en el caso de los virus que en el 2008 fue preocupación del 88.9% de los participantes contra un 50% manifestado en este año.

Los medios de información juegan un papel importante para la corrección, mejora y mitigación de violaciones a la información, donde la tendencia al incremento se centra en el Análisis de registros de auditoría/sistema de archivos/registros Firewall (33%) al igual que los

	2008	2009
Virus	88.9%	50.00%
Instalación de software no autorizado	50.0%	31.25%
Accesos no autorizados al web	44.4%	27.08%
Manipulación de aplicaciones de software	11.1%	18.75%
Pérdida de información	22.2%	12.50%
Negación del servicio	11.1%	10.41%
Phishing	22.2%	10.41%
Otra: fuga de información	5.6%	10.41%
Robo de datos	11.1%	8.33%
Monitoreo no autorizado del tráfico	5.6%	8.33%
Caballos de troya	44.4%	6.25%
Ninguno	5.6%	4.16%
Pérdida de integridad	5.6%	4.16%
Suplantación de identidad	16.7%	4.2%
Pharming	5.6%	4.16%
Fraude	5.6%	2.08%

sistemas de detección de intrusos empleados (33%) que si bien, han disminuido en porcentaje respecto al 2007, 2008, ocupan un primer puesto en su uso.

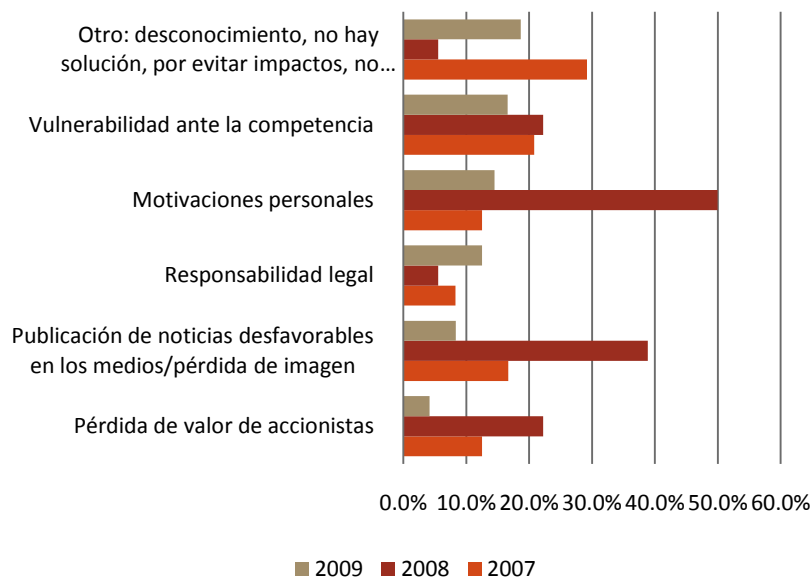
Figura, en esta ocasión, el apoyo que brindan los colaboradores de la empresa (22.9%) al equipo de atención de incidentes, quienes de acuerdo a la tabla No. 7, se mantiene desde el 2007, como un grupo que goza con credibilidad.

ENTIDAD DE NOTIFICACIÓN DE DENUNCIA	2007	2008	2009
Equipo de atención de incidentes	48.0%	44.4%	22.9%
Ninguno: No se denuncian	40.0%	38.9%	22.9%
Asesor legal	8.0%	16.7%	12.5%
Autoridades locales/regionales	4.0%	16.7%	10.4%
Autoridades nacionales	0.0%	0.0%	8.3%

Aún cuando existen diversos medios para denunciar los incidentes, la tendencia es a no hacerlo, sin embargo, esta situación puede modificarse si, las Autoridades Nacionales, que en este ejercicio son ya

consultadas por el 8.3% de los participantes, van realizando acciones que, ante los ojos de los usuarios, los presenten como instancia competente para la resolución y control de delitos informáticos, pues, como se aprecia en el siguiente gráfico, se opta por no denunciar debido a que, en la percepción de los participantes este 2009, no sucede nada o bien, se desconoce ante quien denunciar.

Gráfica 3...Motivos principales de no denuncia



Categoría: Herramientas y prácticas de seguridad informática



Propósito:

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



Los resultados que se expondrán a continuación, se puede decir, marcan ya una diferencia con los años anteriores en cuanto a la asimilación de la importancia de cuidar los activos informáticos tanto los de la organización como los personales.

En la tabla No. 8, puede apreciarse, aún con la falta de respuestas, que la frecuencia de pruebas de seguridad ahora es más activa, esto pudiera deberse a lo que anteriormente se señaló: se cuenta con profesionales

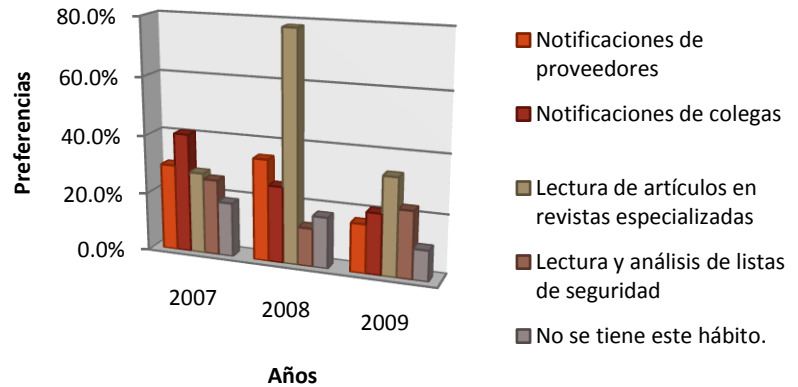
	2007	2008	2009
Una al año	25.0%	21.7%	12.50%
Entre 2 y 4 al año	27.5%	21.7%	18.75%
Más de 4 al año	20.0%	21.7%	8.33%
Ninguna	27.5%	34.8%	16.66%
Sin respuesta			43.75%

especializados dentro de la empresa, hay más herramientas para la aplicación de pruebas y más conciencia sobre el cuidado de los datos.

	2007	2008	2009
Antivirus	70.4%	91.3%	50.00%
Contraseñas	68.5%	87.0%	47.91%
Firewalls Software	59.3%	65.2%	39.58%
Firewalls Hardware	44.4%	56.5%	35.41%
VPN/IPSec	40.7%	60.9%	33.33%
Cifrado de datos	50.0%	52.2%	31.25%
Sistemas de detección de intrusos - IDS	25.9%	17.4%	29.16%
Filtro de paquetes	31.5%	30.4%	25.00%
Biométricos (huella digital, iris, etc)	9.3%	26.1%	25.00%
Administración de logs	0.0%	34.8%	22.91%
Firmas digitales/certificados digitales	31.5%	30.4%	22.91%
Web Application Firewalls	0.0%	43.5%	20.83%
Proxies	37.0%	39.1%	20.83%
Monitoreo 7x24	29.6%	30.4%	20.83%
Sistemas de prevención de intrusos - IPS	14.8%	30.4%	18.75%
Smart Cards	9.3%	26.1%	14.58%
Herramientas de validación de cumplimiento con regulaciones internacionales			6.25%
ADS (Anomaly detection systems)	13.0%	13.0%	4.16%

Complementario a la cantidad de pruebas de seguridad, se indagó sobre las herramientas que se emplean para garantizarla. El análisis si bien muestra que la herramienta más utilizada son los antivirus, de hecho se ha vuelto una buena práctica obligada, no es la única opción elegida; a diferencia de años anteriores, la selección se muestra sobre diversas alternativas dando la impresión del interés que se tiene en conocer los alcances de cada mecanismo que se pone a disposición para la protección de los sistemas informáticos.

Gráfica 4...Medios de información



En la gráfica siguiente (No. 4) pueden observarse algunas similitudes entre los 3 años y algunas tendencias:

Similitudes: continúan siendo pocos (10.4%) los profesionales que no tienen el hábito de informarse sobre los sucesos que se presentan en materia de seguridad: tecnologías,

tendencias, nuevos ataques, etc.,

las notificaciones por parte de colegas ha disminuido también (40.7% - 26.1% - 20.83%).

Tendencias: el trabajo colaborativo de profesionales mediante la creación y difusión de artículos, blogs y avisos en listas de seguridad se está manteniendo como uno de los medios de mayor consulta (56.24%), no obstante que se observa una baja en la lectura de artículos. En contraste, los proveedores de herramientas de seguridad han sido los menos consultados con fuerte tendencia a la baja 29.6%, 34.8%, 16.66% durante 2007, 2008, 2009 respectivamente.

Categoría: Políticas 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.



Luego de revisar los rubros anteriores en los que se refleja el interés de las organizaciones por garantizar la salvaguarda de los recursos informáticos, disponiendo para ello recursos financieros y personal de apoyo, podría esperarse que se cuente con una gobernabilidad adecuada reflejada en el establecimiento de la misión y políticas de seguridad², sin embargo, la realidad refleja un panorama distinto pues sólo el 20.8% señalan contar con políticas formales y el 14.6% indican estar en proceso de desarrollo, en tanto que un 64.4% de participantes no han iniciado la tarea de diseño o se abstuvieron de responder.

Otro punto de especial análisis es el relacionado a la operación de una adecuada Gestión de la Seguridad Informática; diversas son las razones que se exponen para que ésta pueda operar, destacando, al igual que en años anteriores, la *falta de cooperación entre diversas áreas* (ver gráfico No. 5), contrastando este resultado con el 64.4% mencionado en el párrafo anterior, relacionado con la inexistencia de políticas de SI, podría deducirse que la responsabilidad de creación de políticas dependiera de diversas áreas, al respecto se plantearán algunas reflexiones en el apartado final de este informe.

En relación al comparativo en este punto entre los años 2007, 2008, 2009 la tendencia va a la baja en los seis últimos aspectos que se visualizan en la gráfica No. 5, mientras que la falta de apoyo directivo sigue figurando como uno de los obstáculos en la gestión de la SI.

Sobre el soporte que tienen las organizaciones para asegurar sus procesos de seguridad, el sondeo muestra que es el modelo COBIT el más empleado (12.5%) durante este 2009, que en buena medida apoya, por su enfoque integral no sólo el proceso del área de TI, sino al área estratégica y

Gráfico 5.....Obstáculos para lograr una adecuada gestión de la S.I.

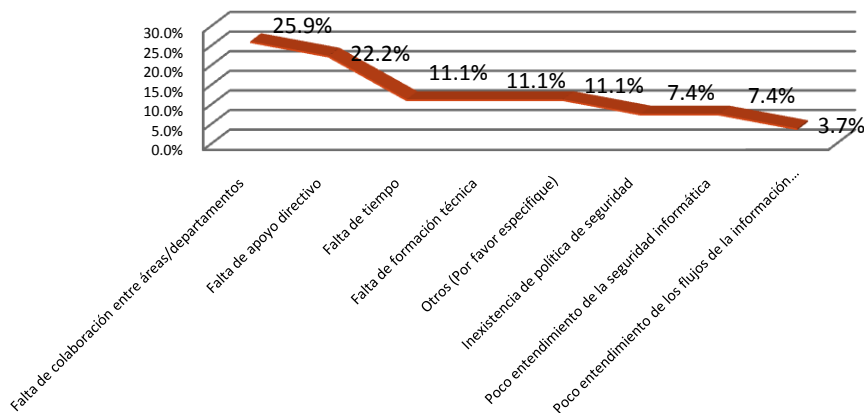


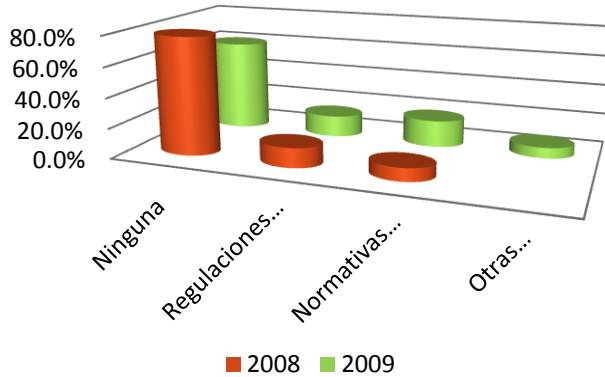
TABLA 10 ESTÁNDARES Y BUENAS PRÁCTICAS UTILIZADOS EN EL SGSI	2008	2009
No se consideran		31.3%
Cobit 4.1	17.4%	12.5%
OSSTM - Open Standard Security Testing Model	13.0%	10.4%
ITIL		10.4%
ISO 27001	26.1%	8.3%
ISM3 - Information Security Management Maturity Model	8.7%	6.3%
Otra - Especifique: BASC, ISO 17799, BS2599, COBIT, GAISP, DRII PP, FFIEC	47.8%	4.2%
Common Criteria	17.4%	4.2%
Guías del NIST (National Institute of Standards and Technology) USA	17.4%	4.2%
Top 20 de fallas de seguridad del SANS	13.0%	4.2%
Magerit	4.3%	2.1%
Octave	4.3%	2.1%
Guías de la ENISA (European Network of Information Security Agency)	0.0%	0.0%

financiera. De manera adicional se emplean otros estándares, llamando la atención la disminución del seguimiento de la SI con apoyo del ISO 270001. Finalmente se hace notar que, aunque existen diversidad de buenas prácticas sugeridas mediante modelos y estándares, aún el 31.3% de los participantes señala no considerarlas.

En lo que respecta a la aplicación de regulaciones o

normativas implementadas en la organización para la seguridad informática, se refleja un incremento tanto en la consideración de regulaciones internacionales (SOX, BASILEA II, Sarbanes-Oxley), como en normativas aprobadas por entes de supervisión (Institutos gubernamentales) y otras como normatividad interna, Código Penal, Ley de protección de derechos de autor; el porcentaje que indica la no aplicación de ninguna de éstas disminuyó en un 18%, sin embargo, sigue siendo alto (60.7%).

Gráfico 6...Regulación/normativa aplicada



Sobre la vinculación con autoridades dedicadas a la atención de incidentes informáticos, hay un ligero incremento en relación al año anterior 2008-13%, 2009 14.8%, esto obedece en buena medida, al mayor involucramiento de dichos organismos ante situaciones de delito informático, aunque la difusión de dichos organismos ahora es más frecuente, aún hay un 48.1% que no establece esta relación.

Categoría: Capital Intelectual

-
-
-

Propósito:

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

-
-
-

Para este apartado los resultados son los siguientes:

Las empresas, según señalan los participantes, consideran la presencia del profesional en SI, aún cuando los resultados señalan en esta ocasión que no hay personal, va seguido de un 18% durante este 2009 con asignación de 1 a 5 personas dedicadas al tema, este dato coincide con los años anteriores.

En opinión de los encuestados, desde el 2007 resaltan los resultados que distinguen la cantidad de tiempo que se requiere para ser un responsable de seguridad informática, con porcentajes de 48.6%,

56.5% y 29.2% (2007, 2008, 2009), dos años o más de experiencia son necesarios para desempeñar cargos relacionados con el tema de SI. En relación a las certificaciones que actualmente tiene el personal del área de TI, se observa una considerable baja en relación al 2007 y 2008, la certificación

	2007	2008	2009
Ninguna	44.2%	39.1%	39.6%
CISSP	11.5%	30.4%	10.4%
CISA	13.5%	26.1%	6.3%
CISM	15.4%	30.4%	6.3%
CFE	3.8%	8.7%	0.0%
CIFI	3.8%	8.7%	0.0%
CIA	7.7%	13.0%	2.1%
SECURITY+	0.0%	13.0%	4.2%
Otras (CCSP, CEH, OPST, OPSA, CCP)	11.5%	34.8%	8.3%
Sin respuesta			22.9%

que más figuró en el último año fue la CISSP con un 10.4%, aunque hay personal certificado, no debe quitarse la vista del 39.6% que indica que ningún profesional se ha certificado.

Un dato que llama la atención y que debe ser analizado es el hecho de la poca importancia que tiene para las organizaciones el que el personal esté certificado; para este 2009 aumentó, para todos los tipos citados, la respuesta “no es importante” ubicándose por encima de los resultados de valoración “muy importante” en cada una de las certificaciones sugeridas, aquí se tiene una fuerte área de oportunidad.

Conclusiones

Es conocido por todos el fuerte impacto que las tecnologías de información representan para el desarrollo de las organizaciones, los nuevos modelos de administración y planeación estratégica, las incluyen ya no sólo como el medio mediante el cual se podrá ingresar datos, procesarlos y generar informes, ahora son un conducto a través del cual se puede generar valor en la organización pasando de una entidad que se deja llevar con el flujo de la economía, a una que de manera estratégica se convierta en insumo para lograr el desarrollo de las naciones, favoreciendo en consecuencia, su propio crecimiento.

A la par de esta visión que se propone, debiera adoptar cualquier organismo sea público o privado e independientemente del sector comercial, se debe ser muy consciente de las realidades críticas que los tiempos actuales presentan, motivadas por la falta de una adecuada gobernabilidad no sólo en el plano económico y social, sino también en el tecnológico, en el que por “adecuada”, debe entenderse la suma de principios, políticas y estrategias que integren los aspectos administrativos, financieros, tecnológicos y sociales como la educación y formación valoral.

La ausencia de este estilo de gobernar señalado en el párrafo anterior aunado al crecimiento de los diversos esquemas tecnológicos, ha desatado una ola de peligros a los que diariamente se enfrentan cualquiera que en su haber, tenga para su uso, recursos financieros, materiales y tecnológicos y por supuesto, datos.

La postura ante esta circunstancia debe ser de una visión tal que permita, como se señala en el libro *El arte de la Guerra solucionar los problemas antes de que se presenten...salir victoriosos antes que las advertencias de los enemigos se hagan realidad*,³ y es precisamente la Gestión de la Seguridad de la Información lo que puede apoyar ante la actual realidad donde se integran las necesidades de permanencia, el urgente fortalecimiento de la economía y la lucha para controlar la vulnerabilidad de las empresas ante la avalancha de delitos informáticos que se cometen en su interior y exterior.

Los resultados que esta investigación generan, hablan del interés por considerar a la Seguridad de la Información como una estrategia que coadyuve al desarrollo organizacional, reflejándose en primer instancia por el reconocimiento del valor de la información, en la incorporación de políticas de control, en la integración de personal especializado en el tema dentro de la

estructura organizacional, realizando inversión financiera, sin embargo, debe reconocerse, que México aún tiene un camino largo por recorrer en el terreno de la seguridad, tarea que sólo podrá despegar cuando todos los miembros de las organizaciones consideren a las TIC'S y a la Información como columna y base que sostengan el proceso de planeación operativa y estratégica.

Afortunadamente los apoyos están al alcance de la mano, convendría que el personal dedicado a las tecnologías de información, sea aún más proactivo en la presentación de propuestas, en el análisis de riesgos, en la sensibilización a directivos sobre las tendencias que ocasiona la inseguridad, si bien la palabra de los directivos es la definitiva y en buena medida, señala el Dr. Cano, la junta directiva es la primera responsable de la inseguridad⁴, es un hecho que a quien tiene la especialización, esto es, el profesional de las tecnologías de información, le corresponde el trabajo de investigar, formar, sensibilizar y proponer las estrategia y políticas necesarias para garantizar además de la mitigación de los riesgos, el desarrollo del potencial del negocio⁵.

“Dinero llama a dinero”, cita una frase del dominio popular, y se ha comprobado con diversos testimonios que efectivamente, así sucede, por tanto, se concluye este apartado señalando que la inversión en el rubro de la seguridad de la información – adquisición e implementación de buenas prácticas, fortalecimiento del capital intelectual, vinculación interinstitucional – es una estrategia que podría, previo análisis de factibilidad, mejorar el desempeño de las organizaciones.

Llamados....

A los directivos como responsables de establecer la visión de la empresa e iniciar estrategias a largo plazo. Considerar dentro de su modelo organizacional a la seguridad informática, no será otro aspecto a controlar, o un gasto con el que se tendrá que lidiar, es la visión de incorporar un apoyo más que permita garantizar, desde la perspectiva del aseguramiento de la información, la estabilidad del negocio, el crecimiento del mismo, y el desarrollo del país desde una dimensión económica y social⁶.

A los profesionales de TI como promotores del cambio. La Seguridad Informática, el Control Interno, es una disciplina de las Tecnologías de Información que con el paso del tiempo están siendo más valoradas. Son muchas las áreas de oportunidad que se presentan, dependerá de cada profesional el cambio en los resultados, buscando, aprovechando y desarrollando los apoyos que ya están al alcance; la búsqueda de la excelencia y la trascendencia, sólo se logran cuando salimos de la zona de confort de manera permanente, sea cada profesional un medio para el desarrollo.

A los proveedores de servicios de TI, como soporte del crecimiento del negocio. La perspectiva del negocio en la actualidad, debe ir más allá de una generación de utilidades; los nuevos esquemas económicos⁷ y los modelos de planeación que están adoptando las empresas, son rubros que bien valdría la pena incorporar en las propuestas comerciales, creando con ellas valor agregado pasando de ser una solución emergente a una solución de negocio.

A la academia, como generador del conocimiento. Las tendencias económicas y oportunidades de negocio, exigen la formación de un profesional con nuevas líneas de pensamiento y generación de estrategias que hagan frente a los retos que la visible inseguridad de nuestro entorno presenta, situación a la que la información no es ajena. Atender esta situación en la creación de nuevos programas de formación continua o especialización, es urgente; la formación de seres humanos éticos, responsables, solidarios y proactivos es una responsabilidad social inminente; buscar la colaboración permanente con empresas y gobierno para analizar tendencias en la línea de delitos, de crecimiento económico, de transferencia de información y creación de nuevas tecnologías, para luego transformarlas en programas educativos, es una labor que apoyará desde las aulas, en la transformación de la sociedad.



Agradecimientos:

A ACIS por las facilidades otorgadas para la realización de este ejercicio. A cada uno de los participantes por su confianza y apoyo para el logro de esta investigación.

****Sobre el autor:** Lic. en Sistemas Computacionales, 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, Educación e Ingeniería de Software.*



REFERENCIAS

¹ <http://www.cio.com.mx/Articulo.aspx?id=324> última fecha de consulta lunes 1 de junio 2009.

² Daltabuit Enrique, Vázquez Jesús, LA SEGURIDAD DE LA INFORMACIÓN: políticas de seguridad, pag. 221, LIMUSA, 2ª. Edición, México, 2007

³ Tzu Sun, EL ARTE DE LA GUERRA, pag. 29, Ediciones Leyenda, México

⁴ Compilación Mercè Molist 2006 en <http://ww2.grn.es/merce/2006/congresosek.html>, última fecha de consulta lunes 1 de junio 2009

⁵ Cano, Jeimy; EVALUACIÓN DE LAS PREDICCIONES EN SEGURIDAD INFORMÁTICA PARA EL 2008 Y EL RIESGO DE LAS PREDICCIONES DEL 2009, en http://www.criptored.upm.es/guiateoria/gt_m142i1.htm

⁶ Senge, Peter, THE NECESSARY REVOLUTION. How individuals and organizations are working together to create a sustainable world. DOBULEDAY, 1a. Edición, USA, 2008

⁷ http://www.seplan.gob.mx/des/pla/perspectivas_2009_indetec.pdf, última fecha de consulta martes 2 de junio 2009.