II Encuesta Nacional sobre Seguridad Informática en México – 2008 –

- Análisis de resultados y comparativo 2007-2008 -

MDOH. Gabriela María Saucedo Meza*

Conscientes de la importancia que reviste el contar con un adecuado Sistema de Gestión de Seguridad de la Información, el Departamento de Sistemas e Industrial de la Universidad del Valle de Atemajac (UNIVA) Campus Guadalajara, en coordinación con la Asociación Colombiana de Ingenieros en Sistemas (ACIS), llevaron a cabo la Segunda Encuesta Nacional sobre Seguridad Informática en México versión 2008, con el fin de conocer el estado que guarda la Seguridad Informática en las organizaciones mexicanas.

Los datos recabados en esta encuesta, se compararán con los resultados obtenidos en el estudio aplicado el 2007.

Estructura de la encuesta

Para analizar la información, se establecieron las siguientes categorías:

- Demografía
- Presupuesto
- Fallas de Seguridad
- Herramientas y prácticas de seguridad informática
- Políticas de Seguridad
- Capital Intelectual

Se realizó invitación vía electrónica para que los interesados ingresaran a un sitio preparado por ACIS con los 32 rubros que deseaban evaluarse según la categorías enunciadas. En esta ocasión se contó con la participación de 32 de voluntarios de los estados de Jalisco, Michoacán, Edo. de México, Campeche, Aguascalientes y el Distrito Federal. Los resultados obtenidos y su análisis por categoría, se describen a continuación; las conclusiones y posibles recomendaciones se señalarán al final del documento.

Categoría: Demografía

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

Análisis de resultados:

SECTOR	2007	2008
Servicios Financieros y Banca	0%	6.5%
Construcción / Ingeniería	8%	6.5%
Telecomunicaciones	4%	3.2%
Hidrocarburos	0%	0.0%
Salud	6%	6.5%
Alimentos	0%	0.0%
Educación	18%	19.4%
Gobierno / Sector público	8%	3.2%
Manufactura	4%	6.5%
Otro	52%	48.4%

Los resultados del 2008 muestran un interesante incremento de participación en el sector de servicios financieros y la banca lográndose un 6.5%; se refleja también un incremento en el sector educativo y el de la salud. Llama la atención el decremento en la participación de otros sectores incluso el señalado como “Otro” en el que se incluyen servicios de consultoría en TI, desarrollo de tecnologías, servicios de TI y seguridad, considerando que se incrementó el número de convocatorias para participar en este estudio.

TAMAÑO EMPRESA (por num. de Empl.)	2007	2008
1 a 50	26%	29.0%
51 a 100	14%	25.8%
101 a 200	0%	3.2%
201 a 300	8%	6.5%
301 a 500	14%	3.2%
501 a 1000	10%	3.2%
Más de 1000	28%	29.0%

El patrón de participación en cuanto al tamaño de la empresa considerando número de empleados, se mantiene similar al año 2007 con un porcentaje muy equilibrado entre la micro, pequeña y gran empresa de entre los sectores participantes, a la par, se refleja la poca participación de la mediana empresa.

CARGOS DE LOS PARTICIPANTES EN LA ENSI	2007	2008
Presidente/Gerente General	5.6%	7.4%
Director Ejecutivo	5.6%	7.4%
Director/Vicepresidente	1.9%	7.4%
Director/Jefe de Seguridad Informática	1.9%	11.1%
Profesional del Departamento de Seguridad Informática	1.9%	7.4%
Profesional de Departamento de Sistemas/Tecnología	51.9%	33.3%
Asesor externo	0.0%	0.0%
Auditor Interno	0.0%	0.0%
Otra	20.4%	25.9%

En las siguientes dos tablas se destaca la notable participación de Directores y profesionales de Seguridad Informática, así como el avance en la ubicación de responsabilidades de seguridad (véase apartado "otra" en la tabla de Responsabilidad de la S.I."), en esta ocasión fue posible contactar a un mayor número de profesionales dedicados a la Seguridad, lo que definitivamente incidió en el incremento de participación con un 11.1%.

Puede observarse que al igual que en el 2007, la tareas de Gestión de la Seguridad Informática (GSI) aún forman parte del perfil de puestos de la Dirección/Gerencia de Sistemas, y que a diferencia del año anterior, Auditoría Interna ya comienza a identificarse con un porcentaje considerable en relación al seguimiento de la GSI.

RESPONSABILIDAD DE LA S.I.	2007	2008
Auditoria interna	1.9%	11.1%
Director de Seguridad Informática	11.1%	14.8%
Director Departamento de Sistemas/Tecnología	38.9%	44.4%
Gerente Ejecutivo	1.9%	11.1%
Gerente de Finanzas	0.0%	0.0%
Gerente de Operaciones	0.0%	0.0%
No se tiene especificado formalmente	14.8%	14.8%
Otra	31.5%	3.7%

Categoría: Presupuesto

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

Análisis de resultados:

Como resultado del primer punto a evaluar acerca de la integración de aspectos de seguridad dentro del presupuesto global de informática en las organizaciones, los resultados se mantienen sin variación en relación al año 2007, esto es, tanto en 2007 como en el 2008 el 77.8% responde de manera positiva a este planteamiento en tanto que el 22.2% menciona que aún no se integra.

En la tabla distribución de la inversión en Seguridad se muestra presupuesto puede observarse que en todos los aspectos se refleja un incremento las incidencias del presupuesto asignado a cada rubro, destacando una mayor asignación en el tema de cursos de especialización que se señalan en el 2008 con un 33.3%, los siguientes incrementos que en promedio son del 20% corresponden a la

concientización/ formación de usuarios en general y las evaluaciones de seguridad internas y externas, y un 10% al 5% mayor en los temas restantes

Distribución de la inversión en Seguridad	2007	2008
Protección de la red	72.2%	88.9%
Proteger los datos críticos de la organización	61.1%	74.1%
Proteger la propiedad intelectual	35.2%	40.7%
Proteger el almacenamiento de datos de clientes	44.4%	55.6%
Concientización/formación del usuario final	29.6%	48.1%
Comercio/negocios electrónicos	18.5%	29.6%
Desarrollo y afinamiento de seguridad de las aplicaciones	27.8%	40.7%
Asesores de seguridad informática	20.4%	25.9%
Contratación de personal más calificado	14.8%	22.2%
Evaluaciones de seguridad internas y externas	20.4%	40.7%
Pólizas contra cibercrimen	0.0%	3.7%
Cursos especializados en seguridad informática(cursos cortos, diplomados, especializaciones, maestrías)	0.0%	33.3%
Cursos de formación de usuarios en seguridad informática	0.0%	25.9%
Monitoreo de Seguridad Informática 7 x 24	33.3%	40.7%
Otra (Por favor especifique)	3.7%	11.1%

De relevante importancia es el hecho de que las organizaciones han asignado un mayor presupuesto para las gestiones de seguridad informática tanto en lo que se invirtió en el año anterior como en las proyecciones para el año actual:

PRESUPUESTO DE SEGURIDAD DURANTE EL AÑO ANTERIOR	2007	2008
Menos de USD$50.000	54.8%	48.1%
Entre USD$50.001 y USD$70.000	14.3%	18.5%
Entre USD$70.001 y USD$90.000	2.4%	7.4%
Entre USD$90.001 y USD$110.000	7.1%	0.0%
Entre USD$110.001 y USD$130.000	0.0%	7.4%
Más de USD$130.000	21.4%	18.5%

PROYECCIÓN DE PRESPUESTO PARA EL AÑO ACTUAL	2007	2008
Menos de USD$50.000	52.4%	44.4%
Entre USD$50.001 y USD$70.000	4.8%	11.1%
Entre USD$70.001 y USD$90.000	11.9%	11.1%
Entre USD$90.001 y USD$110.000	7.1%	3.7%
Entre USD$110.001 y USD$130.000	2.4%	3.7%
Más de USD$130.000	21.4%	25.9%

Si bien la tendencia es a la baja en la asignación de un presupuesto menor a USD$50,000, el incremento para el año en curso (2008) se ve incrementado a montos de entre 50,001 a 70,000USD en un 6.3%, seguido de un 4.5% arriba en la proyección con más de 130,000USD y, finalmente, un 1.4% más en presupuestos proyectados con un monto entre 110,001 USD y 130,000USD.

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.

Análisis de resultados:

A diferencia del año anterior, en esta ocasión un 6.5% de participantes señala no haber conciencia sobre la seguridad informática en su organización, dato que comparado con un 93.5% de efectividad resulta no tan alarmante, sin embargo, desglosando los datos se detecta que apenas un 54.8% señala que en la organización se es muy consciente. Estos datos van muy de la mano con el conocimiento y valoración de las evidencias digitales que con un 65.2% refleja que aún falta trabajar en la formación y concientización de usuarios.

INTRUSIONES IDENTIFICADAS AÑO ANTERIOR	2007	2008
Ninguna	44.4%	25.9%
Entre 1-3	31.1%	37.0%
Entre 4-7	8.9%	11.1%
Más de 7	11.1%	25.9%

Congruente con el nivel de consciencia y con las inversiones financieras para cuestiones de seguridad, se observa que los gestores de SI han podido detectar mayor número de intrusiones, si bien esto es alentador, no deja de preocupar que el número de intrusiones va a la alza de un 51.1% en el 2007 a un 74.1% en el 2008.

Los casos referidos de intrusión/violación son los siguientes:

CASOS DE VIOLACIONES DETECTADAS	2007	2008
Manipulación de aplicaciones de software	18.2%	11.1%
Instalación de software no autorizado	0.0%	50.0%
Accesos no autorizados al web	50.0%	44.4%
Fraude	0.0%	5.6%
Virus	72.7%	88.9%
Robo de datos	13.6%	11.1%
Caballos de Troya	54.5%	44.4%
Monitoreo no autorizado del tráfico	22.7%	5.6%
Negación del servicio	13.6%	11.1%
Pérdida de integridad	0.0%	5.6%
Pérdida de información	31.8%	22.2%
Suplantación de identidad	0.0%	16.7%
Phishing	13.6%	22.2%
Pharming	4.5%	5.6%

La violación o alteración por presencia de virus señala una significativa vulnerabilidad de la organización, al igual que el año anterior, su porcentaje se mantiene en primer lugar, seguido por un 50% de detección de instalaciones de software no autorizado.

Revisando los medios utilizados para detectar las intrusiones/violaciones, ha sido el análisis de registros de auditoría/sistema de archivos/registros Firewall el método más común que con un 66.7% de aplicación se ubica en primer lugar, seguido de sistemas de detección de intrusos con un 44.4%; llama la atención que la colaboración de clientes, proveedores y colegas ha resultado también un medio valioso de comunicación sumando en el estudio del 2008 un 38.9% contra el 22.7% del 2007.

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

MOTIVOS PRINCIPALES DE NO DENUNCIA	2007	2008
Pérdida de valor de accionistas	12.5%	22.2%
Publicación de noticias desfavorables en los medios/pérdida de imagen	16.7%	38.9%
Responsabilidad legal	8.3%	5.6%
Motivaciones personales	12.5%	50.0%
Vulnerabilidad ante la competencia	20.8%	22.2%
Otro (Por favor especifique)	29.2%	5.6%

Un punto más de análisis es el proceso de comunicación del incidente hecho que si bien se lleva a cabo en un 77.8%, aún existe un 38.9% que refieren no denunciar por decisión personal o por temor a perder imagen de calidad ante los clientes. Resultaría conveniente evaluar posteriormente los motivos para considerar en tan bajo porcentaje la posibilidad de comunicar la intrusión ante el asesor legal o autoridades locales y el por qué de la nula comunicación ante autoridades nacionales.

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.

Análisis de resultados:
Contrario a lo esperado dado el incremento en presupuesto para temas de seguridad, este año se refleja una disminución en el porcentaje de aplicación de pruebas de seguridad, señalándose que el 34.8% manifestó no haber realizado pruebas durante el año anterior, situación que pudiera deberse a la sensación de seguridad que se genera al adquirir herramientas de seguridad, hecho que se destaca con un notorio incremento de hasta un 20% entre el 2007 y 2008 de acuerdo al listado que enseguida se presenta.

Este incremento en la adquisición y uso de herramientas, reflejan congruencia con lo ya comentado sobre la distribución del presupuesto.

Un resultado que llama también la atención es la proactividad de los usuarios para la búsqueda y actualización de información a través de los proveedores quienes, al ser más consultados – 5.2% más que en el 2007 - se deduce su buena disposición para compartir información, y mediante la revisión de revistas especializadas que con una participación del 78.3% rebasa en 50% lo señalado el año anterior.

Se visualizan como áreas de oportunidad erradicar el no hábito de búsqueda de información (17.4%) y lograr mayor motivación para integrarse a listas de seguridad donde se pudieran presentar recomendaciones y experiencias de entre los mismos participantes (13%).

HERRAMIENTAS UTILIZADAS PARA PROTECCIÓN	2007	2008
Smart Cards	9.3%	26.1%
Biométricos (huella digital, iris, etc)	9.3%	26.1%
Antivirus	70.4%	91.3%
Contraseñas	68.5%	87.0%
Cifrado de datos	50.0%	52.2%
Filtro de paquetes	31.5%	30.4%
Firewalls Hardware	44.4%	56.5%
Firewalls Software	59.3%	65.2%
Firmas digitales/certificados digitales	31.5%	30.4%
VPN/IPSec	40.7%	60.9%
Proxies	37.0%	39.1%
Sistemas de detección de intrusos - IDS	25.9%	17.4%
Monitoreo 7x24	29.6%	30.4%
Sistemas de prevención de intrusos – IPS	14.8%	30.4%
Administración de logs	0.0%	34.8%
Web Application Firewalls	0.0%	43.5%
ADS (Anomaly detection systems)	13.0%	13.0%
Otro (Por favor especifique)	0.0%	0.0%

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.

Análisis de resultados:

La aplicación de políticas de seguridad es un punto que requiere mayor atención por parte de los directivos de la organización, al 2008 los resultados hablan sólo de un 56.5% de aplicación o actual desarrollo, contra un 80% que se informó en el 2007. Esta baja resulta inquietante pero lógica en el sentido de que la tarea, en su mayoría, está asignada a personal no especializado en temas de seguridad quienes además deben distribuir su tiempo en otras gestiones de igual importancia, resultando entonces el factor tiempo como uno de los mayores obstáculos – 52.2% - para el logro de la creación, implementación y seguimiento de políticas.

OBSTÁCULOS PARA LOGRAR UN ADECUADO SGSI	2007	2008
Inexistencia de política de seguridad	22.2%	39.1%
Falta de tiempo	24.1%	52.2%
Falta de formación técnica	27.8%	30.4%
Falta de apoyo directivo	25.9%	26.1%
Falta de colaboración entre áreas/departamentos	29.6%	26.1%
Complejidad tecnológica	16.7%	17.4%
Poco entendimiento de la seguridad informática	16.7%	13.0%
Otros (Por favor especifique)	9.3%	13.0%

Adicional a la carencia de políticas de seguridad, el 78.3% de participantes señala no considerar alguna regulación o normativa en temas de seguridad informática como Sarbanes-Oxley que es utilizada en un 13%, seguida por la Normatividad de Telecomunicaciones que es utilizada en un 8.7% .

ESTÁNDARES Y BUENAS PRÁCTICAS UTILIZADOS EN EL SGSI	2008
ISO 27001	26.1%
Common Criteria	17.4%
Cobit 4.1	17.4%
Magerit	4.3%
Octave	4.3%
Guías del NIST (National Institute of Standards and Technology) USA	17.4%
Guías de la ENISA (European Network of Information Security Agency)	0.0%
Top 20 de fallas de seguridad del SANS	13.0%
OSSTM - Open Standard Security Testing Model	13.0%
ISM3 - Information Security Management Maturiy Model	8.7%
Otra - Especifique: BASC, ISO 17799, BS2599, COBIT, GAISP, DRII PP, FFIEC	47.8%

Datos más alentadores presenta la tabla de estándares y buenas prácticas utilizados en el SGSI; la consideración del ISO27001 ha obtenido un alto porcentaje en relación a los otros que se enlistan, sin embargo, no puede hablarse de una tendencia a favor.

Cuando se habla de un SGSI es clara la necesidad de un trabajo conjunto al interior y exterior de la organización, por ello se cuestionó sobre la política de colaboración o búsqueda de asistencia de autoridades nacionales o internacionales, actividad que sólo el 13% de los participantes llevan a cabo, el 21.7% señala desconocer si esta práctica se lleva a cabo en su organización y el 65.2% manifiesta no colaborar ni solicitar asistencia a este tipo de organismos.

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.

Análisis de resultados:

PERSONAL DEDICADO TIEMPO COMPLETO A LA SEG. INF.	2007	2008
Ninguna	18.0%	25.8%
1 a 5	52.0%	45.2%
6 a 10	10.0%	3.2%
11 a 15	4.0%	3.2%
Más de 15	16.0%	22.6%

Se observan variaciones en el porcentaje de ocupación del personal exclusivamente para las tareas de seguridad informática, los datos obtenidos, son congruentes con los resultados mostrados en la categoría "demografía" en el que se indica que dicha actividad forma parte del perfil de puesto del Jefe de Sistemas, actualmente (2008) el 74.2% refleja si contar con personal dedicado a esta actividad.

La opinión de los participantes en relación a los años de experiencia que se requieren para ocupar un cargo en Seguridad Informática, que va entre uno o más años, se mantuvo igual al año 2007 con apenas un punto menos de diferencia: 2007 (83.7%), 2008 (82.6%).

En relación a la importancia que tiene para los participantes el contar con alguna certificación de la lista que se muestra a la derecha, se mantiene un comportamiento similar al año 2007 bajo la clasificación "muy importante", la diferencia específica está en el valor de importancia de la certificación CFE que el año pasado (2007) fue catalogada como "no importante" y este año se ubicó en la categoría de "muy importante".

CISSP - Certified Information System Security Professional
CISA - Certified Information System Auditor
CISM - Certified Information Security Manager
CFE - Certified Fraud Examiner
CIFI - Certified Information Forensics Investigador
CIA - Certified Internal Auditor
MCSE/ISA-MCP (Microsoft)
Unix/Linux LP1
Security+

Un dato de especial relevancia es el incremento en las certificaciones de personal enfocadas al tema de Seguridad, en tanto que el porcentaje de personal no certificado disminuyó en 5.1%. El incremento puede deberse al incremento en la oferta académica de diversos organismos y asociaciones, el aumento en el porcentaje del presupuesto para la formación de usuarios, aunado a la motivación personal del profesional.

CERTIFICACIONES DE PERSONAL DEDICADO AL TEMA DE LA SEG. INF.	2007	2008
Ninguna	44.2%	39.1%
CISSP - Certified Information System Security Professional	11.5%	30.4%
CISA - Certified Information System Auditor	13.5%	26.1%
CISM - Certified Information Security Manager	15.4%	30.4%
CFE - Certified Fraud Examiner	3.8%	8.7%
CIFI - Certified Information Forensics Investigador	3.8%	8.7%
CIA - Certified Internal Auditor	7.7%	13.0%
SECURITY+	0.0%	13.0%
Otra (especificadas): IBM, BSA, CEH, OPST, CBCP, OPSA, OPST, ETHICAL HACKER, AUDITOR LIDER	11.5%	34.8%

CONCLUSIONES GENERALES

Grandes retos enfrentan las organizaciones que desean garantizar el crecimiento de sus negocios y que de manera solidaria, buscan colaborar con el desarrollo sustentable del país, retos que han asumido muchas organizaciones mexicanas manteniéndose atentas a las necesidades del entorno en los diferentes aspectos que marca la sustentabilidad, a saber: ambiental, social y económico.

En la vertiente económica y social influye directamente el concepto de gobernabilidad de las tecnologías, cuyas acciones derivan en la atención del aspecto ambiental y es, dentro del rubro de la gobernabilidad, donde se inserta la seguridad de la información como un mecanismo de control y seguimiento de los indicadores de éxito del negocio, como medio para asegurar la estabilidad de los sistemas de información, como supervisor del cumplimiento de criterios de responsabilidad ética, social y ambiental y como aporte de conclusiones en materia de control y aseguramiento de la estabilidad económica y social del país. [1]

Tales retos implican crecimiento, hecho que se da solamente si se evalúa con oportunidad la información que se genera dentro y fuera de las empresas. Resulta claro que la veracidad, confiabilidad y estabilidad de la información y por ende de los recursos que van a albergarla, sean criterios base a considerar en las políticas organizacionales en cuanto a la protección que se debe dar para que las variables enunciadas se garanticen; esto es, el tema de la Seguridad de la Información, responsable de la protección de la información[2], debe ser considerada por los directivos como una constante dentro de los procesos empresariales y no como un producto[3].

Los resultados de la investigación demuestran que la situación mencionada en el párrafo anterior ha ido tomando fuerza demostrado por un crecimiento en la distribución de presupuesto tanto para la adquisición de herramientas de seguridad como para la capacitación y formación de especialistas en seguridad y usuarios, si este esfuerzo ya se está realizando debe entonces considerarse la posibilidad de integrar al equipo de tecnologías de información personal dedicado de tiempo completo a las tareas de seguridad y proporcionar, además de los recursos financieros, el apoyo absoluto por parte de la dirección y de los departamentos usuarios, pues de otro modo, el círculo quedará siempre con una gran división de tareas con el riesgo de segregar aquellas enfocadas a la implementación y seguimiento de un correcto Sistema de Gestión de Seguridad Informática, hecho que también se hace evidente con este estudio (véase tabla “obstáculos para lograr un adecuado SGSI”).

Valdría la pena que las organizaciones realicen un análisis financiero para demostrar qué resulta más rentable: seguir adquiriendo herramientas para proteger la información sin la garantía de disminución de

riesgos (el estudio muestra un incremento en incidencias de intrusión por diferentes causas) o implementar de lleno una adecuada Gobernabilidad de las Tecnologías mediante la integración de un proceso de seguridad que incluya el plan humano, técnico, organizacional y legislativo[4], en congruencia con los esfuerzos de inversión que se están realizando.

Las organizaciones deben tener la capacidad de reconocerse vulnerables y como tales, buscar apoyos que les permitan ser y sentirse menos inseguras, estos apoyos son precisamente modelos que impulsen la aplicación de estándares y metodologías que mediante gobierno, administración y operación[5] de los recursos participantes y el capital intelectual dispuesto para ello, logran mantener estables los procesos, salvaguardar los recursos y por ende, garantizar la continuidad del negocio.

La diversidad de estándares que se ofrecen actualmente, permiten a los responsables de la seguridad informática pasar de una protección mínima o nula a una protección de verificación[6], actividad que ya es llevada a cabo por los participantes de esta encuesta, esto es, el interés y necesidad de normar procesos internos, de considerar los procesos de TI con mejores niveles de calidad es una realidad en México prueba de ello son además de los porcentajes diferenciadores respecto al 2007 en el tema de la aplicación de estándares y las certificaciones profesionales, la apertura y promoción de distintos organismos, institutos e instituciones académicas que han venido impulsando y motivando la preparación profesional mediante cursos de posgrado, ingenierías, educación continua y certificaciones.

Si bien el interés en la preparación va incrementándose existe aún rezago:

- en la formación profesional y en general de cultura informática sobre seguridad, área de oportunidad para las instituciones de educación superior;
- en la integración de redes de profesionales interesados en la difusión de experiencias y participación en estudios de investigación, en el 2008 el estudio señala que sólo un 38.9% recibe orientación entre colegas y proveedores, área de oportunidad para los sectores de vinculación universidad-empresa;
- en mercadotecnia social y promoción directa de los apoyos legales y formativos que brindan organismos públicos y privados (asociaciones nacionales e internacionales), área de oportunidad para el sector gobierno y empresa privada; y,
- rezago en la confianza para denunciar hechos que atentan contra los recursos informáticos de la organización, área de oportunidad para el sector gobierno, educativo, comercial, tecnológico y asociaciones.

Las posibilidades de lograr un mayor desarrollo nacional son muchas, las necesidades de que este desarrollo sea una realidad es mayor aún; las oportunidades de competir, de contar con nuevas áreas de negocio, de lograr una estabilidad y reconocimiento público son reales, decidirse a entrar en esta carrera obliga a las organizaciones a controlar y administrar sus recursos para conservar el crecimiento[7], la única forma de logarlo es que toda la estructura organizacional se convenza del papel que representan ante el desarrollo del país y del valor que tiene la información para sus propios procesos, dado este paso, las posibilidades de integrar y operar un adecuado Sistema de Gestión de Seguridad Informática serán mayores y, se tornarán permanentes, si se cuenta con un adecuado sistema de vinculación gobierno-educación-empresa que promueva, motive y forme en las buenas prácticas de los sistemas de gestión.

AGRADECIMIENTOS

Se agradece a: ACIS, ALAPSI, ISACA, CANIETI y participantes en general por su compromiso en la participación y promoción de esta encuesta.

---

* ***Gabriela Maria Saucedo Meza****; Lic. en Sistemas Computacionales y Master en Desarrollo Organizacional y Humano por la Universidad del Valle de Atemajac; 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 SAUCEDO, GABRIELA M.; Esquema general de la auditoría y seguridad informática y su relación con la puesta en marcha de la Gobernabilidad de las tecnologías como una línea de acción del Desarrollo Sustentable, Notas del curso Auditoría de Sistemas, 2007.

[2] CALDER, ALAN; Nueve claves para el éxito: una visión general de la implementación de la norma NTC-ISO/IEC27001; IT Governance Publishing-ICONTEC 2006; Reino Unido-Colombia.

[3] GÓMEZ VIEITES, ALVARO; Enciclopedia de la seguridad informática, Alfaomega RAMA, México, 2007.

4 Idem

5 CANO, JEIMY J., "Las organizaciones de cara a la seguridad informática", Revista Sistemas, Colombia, 2006.

[6] OZ EFFY, Administración de sistemas de información, Thomson Learning, México, 2001.

7 CASTILLO, HÉCTOR; Soluciones para el desarrollo: una perspectiva organizacional, Ediciones Castillo, México, 1996.