I Encuesta Nacional sobre Seguridad Informática en México – 2007 -

Se llevó a cabo en México la primer Encuesta Nacional sobre Seguridad Informática, con el fin de conocer el nivel de aplicación que sobre este tema, se hace en las empresas mexicanas.

M.A.Jorge E. Macías Garza
MDOH. Gabriela María Saucedo Meza, Asesor

"A medida que se aumentan los usuarios de sistemas de información basados en computadora, la integridad de los datos y la confiabilidad de la información en organizaciones pueden verse mermadas, riesgos que las empresas deben afrontar con seriedad"[1]

Con el fin de conocer precisamente la forma en que las organizaciones han asumido estos riesgos a través de la implementación de estrategias que minimicen el nivel de inseguridad que pueda tener su información, los participantes de la asignatura Auditoría de Sistemas, de la Maestría en Ingeniería de Software de la Universidad del Valle de Atemajac (UNIVA), Campus Guadalajara, en coordinación con la Asociación Colombiana de Ingenieros en Sistemas (ACIS), se llevó a cabo la Primer Encuesta Nacional sobre Seguridad Informática en México.

La convocatoria de participación fue enviada mediante correo electrónico a diversas empresas de 27 estados de la República Mexicana, obteniéndose un total de 54 participaciones.

Los datos recabados en esta encuesta, servirán de base para ir determinando tendencias mediante un estudio comparativo con datos de encuestas de los años sucesivos.

Estructura de la encuesta

Para este estudio, se diseñaron 32 preguntas, mismas que para su análisis, fueron agrupadas en las siguientes categorías:

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

Por cada una de estas categorías se mencionará:

- El propósito de la sección
- Los resultados obtenidos
- Comentarios de la categoría
- Datos específicos (opcional, según sea necesario)

Categoría: demografía

Propósito de la sección: esta sección identifica los sectores que participan, el tamaño de la organización, el personal dedicado de tiempo completo al área de seguridad, la dependencia organizacional de la seguridad, los cargos de las personas que respondieron las preguntas y su ubicación geográfica.

Resultados obtenidos

La siguiente tabla nos muestra que el 42% de participación corresponde al sector de las Tecnologías de Información seguidas en un 18% por la participación del sector educativo, mientras que la participación de la banca fue nula, siendo la participación muy homogénea entre empresas pequeñas, medianas y grandes (considerando el número de empleados):

Sector	Empresa	Representación
Servicios Financieros	0	0%
Construcción / Ingeniería	4	8%
Educación	9	18%
Gobierno / Sector público	4	8%
Salud	3	6%
Manufactura	2	4%
Asesoría, capacitación, consultoría	3	6%
Desarrollo de Software	4	8%
Servicios de informática	4	8%
Servicios Profesionales	2	4%
Sistemas	1	2%
Tecnologías de Información	6	12%
Telecomunicaciones	2	4%
Otras	6	12%

Cantidad de empleados	Representación
1 a 50	26%
51 a 100	14%
101 a 200	0%
201 a 300	8%
301 a 500	14%
501 a 1000	10%
Más de 1000	28%

Comentarios de la categoría

El 42% de las empresas participantes pertenece a algún ramo de la Informática, participación esperada de acuerdo al porcentaje de invitaciones enviadas para este sector, sin embargo, creemos que la participación en cada uno de los demás sectores podría ser mayor dado que en México existen suficientes empresas para todas las combinaciones sector-número de empleado. Con la publicación de estos resultados se espera una mayor participación de las empresas en la encuesta 2008.

Llama la atención la no participación de la banca, considerando que es el sector más ocupado en brindar formación y protección a los usuarios de manera gratuita a través de sitios web diseñados específicamente en esta labor en coordinación con empresas de otros giros como IBM, TELMEX, MICROSOFT, LINKSYS, apoyados por la CONDUSEF[2]

En relación a la responsabilidad de la seguridad informática, se puede observar que no hay una persona dedicada exclusivamente a esta tarea, pues de acuerdo a lo que señalan los participantes, en su mayoría profesionales del departamento de sistemas (55.60%), la actividad recae exclusivamente en la Dirección de Sistemas (46.70%); el 13.30% indica la presencia de un Director de Seguridad, contra un 17.80% de los casos que no tienen definido una persona específica para esta labor.

Categoría: presupuesto

Propósito de la sección: mostrar si las organizaciones consideran a la información como activo y por ende, si han destinado un rubro para la seguridad informática. Permite revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad informática

Resultados obtenidos:

Hacia el año 1989, Meyer y Boone mencionaban que “la disponibilidad de la información desempeña un papel clave para reducir el riesgo y la incertidumbre en la toma de decisiones”[3], casi 20 años después, en este análisis se observa que sólo el 65% de los participantes consideran que la información debe ser considerada como un activo a proteger y por tal motivo han dedicando una partida de su presupuesto global a aspectos de seguridad informática, correspondiente, tanto en el 2006, como en el 2007 a un monto menor a los 50,000 dólares.

La inversión señalada, se distribuye de la siguiente manera:

Principales causas del gasto en seguridad	Representación	Principales causas del gasto en seguridad	Representación
Protección de la red	86.70%	Desarrollo y afinamiento de seguridad de las aplicaciones	33.30%
Proteger los datos críticos de la organización	73.30%	Asesores de seguridad informática	24.40%

Proteger el almacenamiento de datos de clientes	53.30%	Evaluaciones de seguridad internas y externas	24.40%
Proteger la propiedad intelectual	42.20%	Comercio/negocios electrónicos	22.20%
Monitoreo de Seguridad Informática 7 x 24	40%	Contratación de personal más calificado	17.80%
Concientización/formación del usuario final	35.60%	Otra	4.40%

Comentarios de la categoría

Son buenas noticias que casi las tres cuartas partes de las empresas participantes destinen parte del presupuesto global a cuestiones de seguridad informática, ya que es común no pensar en esto cuando se hacen presupuesto, o inclusive hay muchos casos en que no se autoriza presupuesto para este fin, o bien se restringe mucho.

Protección de la red y de los datos críticos de las organizaciones son los dos aspectos que mayor porcentaje alcanzaron; le sigue el proteger almacenamiento de datos de clientes y debajo de ellos están el proteger la propiedad intelectual y el tener sistemas de monitoreo las 24 horas durante los 7 días de la semana. Esto justifica el apartado que sigue, ya que trata sobre incidentes.

En cuanto al manejo de presupuestos, más de la mitad de las empresas destina menos de 50,000 dólares en 2006 y en 2007, sin embargo llama la atención que otro alto porcentaje lo forman las empresas que invierten más de 130,000 dólares.

Datos específicos

Muchas de las empresas que tienen de 1 a 50 empleados son precisamente quienes invierten menos de 50,000 dólares al año. Lo mismo pasa con las empresas que tienen más de 1000 empleados, pues casi todas ellas son quienes invierten más de 130,000 dólares al año. Son muy similares los presupuestos de 2006 y 2007 en cada empresa. Esto podría dar pie a la hipótesis de que por cada empleado de la organización hay que invertir 1000 dólares o menos, pero se necesitaría analizar más variables para poder hacer la hipótesis correcta.

Será tarea de las propias organizaciones, la concientización del valor de la información, el porcentaje total entre desconocimiento y no consideración de que efectivamente debe ser un activo a proteger, arrojó un resultado del 34.65%.

Categoría: fallas de seguridad

Propósito de la sección: 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.

Resultados obtenidos

Es alentador saber que el 98% de los participantes, menciona que en la organización existe plena consciencia sobre la importancia que reviste la seguridad informática y la evidencia digital, sin embargo, congruente con el 45.50% de participantes que señalan no denunciar las intrusiones entre otros motivos por sentirse vulnerables ante la competencia (22.70%), mala imagen (18.20%) o por perder valor frente a sus accionistas (13.60%), sólo el 79% de los participantes respondieron al rubro de intrusiones, del cual el 46.50% menciona no haber tenido dificultades por este motivo durante el año anterior, mientras que el 53.50% indican haber tenido entre 1 y al menos 7 intrusiones.

Los casos referidos se detallan a continuación:

Casos de violaciones de seguridad	Representación	Casos de violaciones de seguridad	Representación
Virus	72.70%	Negación del servicio	13.60%
Caballos de Troya	54.50%	Phishing	13.60%
Accesos no autorizados al web	50%	Ninguno	9.10%
Pérdida de información	31.80%	Pharming	4.50%
Monitoreo no autorizado del tráfico	22.70%	Otra	4.50%
Manipulación de aplicaciones de software	18.20%	Fraude	0%
Robo de datos	13.60%	Pérdida de integridad	0%

Comentarios de la categoría

Más de la mitad de las empresas que colaboraron tuvieron una intrusión o más. Esto hablaría muy bien, sin embargo debemos recordar que día con día nacen nuevas estrategias y herramientas para intrusos, y en muchos casos podríamos no saber que tenemos intrusiones.

En coincidencia con un estudio realizado recientemente por Joint Future Systems con motivo del análisis de percepción sobre la seguridad informática en México[4], las intrusiones más comunes fueron los virus (en general), los caballos de Troya y accesos no autorizados a la web, situación que ha permanecido constante según se manifiesta en los estudios que desde el 2004, ha realizado la empresa señalada[5]. Aquí la pregunta reflexiva sería ¿Tenemos conocimiento total de todas las intrusiones? ¿Son

concientes todos los usuarios de computadoras de una organización sobre lo que tienen que hacer en caso de virus, o puede llegarse al extremo en que el usuario hace caso omiso de la advertencia? y más aún, ¿tenemos la total seguridad de que los usuarios dentro de nuestra organización no intentan hacer intrusiones a otras partes?

El Firewall detecta más de la mitad de estos intentos de intrusión (59.10%), esto puede hablar bien de la herramienta empleada, sin embargo, más del 30% de las veces la intrusión se detecta además, cuando se perdió información y en igual proporción por notificación de terceros.

De acuerdo con los datos obtenidos en otro de los rubros, más del 45% de las intrusiones no se denuncian, y sin embargo, en más del 50% de las empresas participantes hay un equipo de atención a incidentes.

En cuanto a denunciar incidentes a instancias nacionales y/o estatales jurídicas, el 33% indica que sí lo harían en contraste el 67% mencionan que se pierde mucho tiempo o bien que no se considera importante hacer denuncias.

Es recomendable que se estudie más a fondo las implicaciones de hacer denuncias así como la forma en que este proceso sea menos complejo, tarea en la que podrían integrarse las autoridades locales/nacionales del país.

Categoría: herramientas y prácticas de seguridad informática

Propósito de la sección: identificar la frecuencia, mecanismos, herramientas y políticas que utilizan comúnmente las empresas participantes con el fin de garantizar la seguridad informática en sus organizaciones.

Los resultados obtenidos

Los datos indican que la diversidad de mecanismos de protección empleados es amplia, siendo los antivirus el que cuenta con un mayor porcentaje en su uso.

Una práctica adicional son precisamente las pruebas de seguridad, detectando que el 72.5% de participantes mencionan realizar al menos de una a cuatro pruebas al año, en tanto que el 27.5% no realiza dicha práctica, porcentaje muy similar al obtenido al revisar los hábitos para conocer las fallas y/o riesgos que pudieran presentarse, en el que los Colegas figuran como la principal fuente de información (55%), seguido por los proveedores (40%) y en porcentajes muy similares, la revisión de boletines, revistas, y participación en listas de seguridad, con un 37.50 y 35% respectivamente.

Mecanismos de protección que se utilizan actualmente	Representación	Mecanismos de protección que se utilizan actualmente	Representación
Antivirus	95%	Firmas digitales/certificados digitales	42.50%
Contraseñas	92.50%	Monitoreo 7x24	40%
Firewalls Software	80%	Sistemas de	35%

		detección de intrusos – IDS	
Encripción de datos	67.50%	Sistemas de prevención de intrusos - IPS	20%
Firewalls Hardware	60%	ADS (Anomaly detection systems)	17.50%
VPN/IPSec	55%	Smart Cards	12.50%
Proxies	50%	Biométricos (huella digital, iris, etc.)	12.50%
Filtro de paquetes	42.50%	Otro (Por favor especifique)	0%

Comentarios de la categoría:

La incorporación de estos mecanismos de protección señala la correcta aplicación de las buenas prácticas de seguridad. Los mecanismos más comunes son antivirus, contraseñas y FireWalls a nivel software, sin embargo en la categoría anterior se ve que los virus son la causa más común de intrusión. ¿Será entonces suficiente con tener estos tres mecanismos?

Igual que en la categoría anterior, los colegas y ahora los proveedores juegan un papel muy importante en cuanto a notificación de fallas de seguridad. La pregunta en cuestión es ¿por qué son agentes externos a la empresa quienes lo detectan?, ¿podrán nuestras empresas, por sí mismas, ser quienes puedan detectar estas fallas y aportarlas en grupos de colaboración?

Categoría: políticas de seguridad

Propósito de la sección: esta sección busca indagar sobre la formalidad en la implementación de políticas de seguridad en la organización; los principales obstáculos para lograr una adecuada seguridad y los contactos y relaciones que se mantienen con autoridades nacionales e internacionales en un esquema de colaboración en el caso de persecuciones a intrusos.

Resultados obtenidos y Comentarios de la categoría

Descripción de la política de seguridad	Representación
No se tienen políticas de seguridad definidas	20%
Actualmente se encuentran en desarrollo	40%
Política formal, escrita documentada e informada a todo el personal	40%

El aspecto de la documentación se visualiza como un área de oportunidad; en la tabla se visualiza que por el momento el 60% de los participantes no cuentan con este criterio, mismo que señala Alan Calder, se considera como punto de referencia y como la base para garantizar que existe aplicación coherente con el paso del tiempo y hacer posible la mejora continua.[6]

Obstáculos para la seguridad	Representación
Falta de colaboración entre áreas/departamentos	40%
Falta de formación técnica	37.50%
Falta de apoyo directivo	35%
Falta de tiempo	32.50%
Inexistencia de política de seguridad	30%
Complejidad tecnológica	22.50%
Poco entendimiento de la seguridad informática	22.50%
Otros	12.50%

En cuanto a los obstáculos para la seguridad predomina la falta de colaboración entre departamentos, la falta de formación técnica, la falta de apoyo directivo y la falta de tiempo. Esto puede deberse a lo intangible que es la seguridad informática, sobretodo para usuarios que usan la computadora como una herramienta de apoyo sin tener plena consciencia de los riesgos informáticos que pudieran existir.

En esta categoría, se presenta un alarmante 77.5% de las empresas que no tiene datos de las autoridades a quienes se puede acudir para pedir asistencia en cuanto a posibles delitos y cómo combatirlos, o bien, que no están interesados en contactarles. Es muy distinta la respuesta de que no se haya podido solucionar el caso por parte de las Autoridades responsables a que no se conozca quienes son, se reitera por tanto la recomendación de intervención por parte de las autoridades jurídicas gubernamentales como entidades socializadoras del apoyo que puedan brindar.

Categoría: capital intelectual

Propósito de la sección: finalmente esta sección analiza la situación de desarrollo profesional en torno a conocimientos relacionados con tareas propias de tecnologías de la información: personal dedicado a esta tarea, personal certificado, importancia de las certificaciones y años de experiencia en el rubro de seguridad informática

Resultados obtenidos

La mayoría de las empresas participantes (52%) no tiene más de 5 empleados dedicados a la seguridad informática. No es sencillo obtener un puesto así, dado el grado de experiencia requerido señalado por el 48.60% de los participantes como más de dos años, la visión de que el responsable debe ser directivo y los conocimientos exigidos que deben ser avalados por una certificación.

La siguiente tabla muestra el nivel de importancia, que para las empresas participantes, tienen las diversas certificaciones en materia de seguridad informática y a la par, en la segunda columna se señala qué cantidad de su personal cuenta con alguna de éstas:

		IMPORTANCIA DE LA CERTIFICACIÓN			
Certificación	**Personal certificado**	**Muy Importante**	**Importante**	**No es Importante**	**No sabe**
CISSP - Certified Information System Security Professional	16.20%	**46% (17)**	27% (10)	5% (2)	22% (8)
CISA - Certified Information System Auditor	18.90%	**37% (13)**	26% (9)	11% (4)	26% (9)
CISM - Certified Information Security Manager	21.60%	**41% (15)**	32% (12)	11% (4)	16% (6)
CFE - Certified Fraud Examiner	5.40%	24% (8)	26% (9)	**29% (10)**	21% (7)
CIFI - Certified Information Forensics Investigator	5.40%	**26% (9)**	24% (8)	24% (8)	**26% (9)**
CIA - Certified Internal Auditor	10.80%	26% (9)	**38% (13)**	15% (5)	21% (7)
MCSE/ISA-MCP (Microsoft)	Sin dato	**40% (14)**	23% (8)	17% (6)	20% (7)

Unix/Linux LP1	Sin dato	**33% (12)**	22% (8)	28% (10)	17% (6)
Otras	16.20%				
Ninguna	62.20%				

Comentarios a la categoría

Ciertamente para asignar un puesto de esta índole con todas las implicaciones legales, de responsabilidad, de confianza, de liderazgo y de conocimientos tecnológicos de vanguardia que se requieren, salvo que la empresa tenga pocos meses de haberse constituido, no es cuestión de suerte.

Se puede ver que más de la mitad de las empresas participantes (62.20%) no tiene certificación como tal en materia de seguridad informática. Tal vez para muchos el estar certificado en esta materia no sea tan significativo, sin embargo es cuestionable la razón por la que no se consideraría importante obtener una certificación como tal.

No se pueden todavía hacer juicios acerca de las posibles razones, ni tampoco se investigó en esta encuesta si ya se inició con este proceso. Sin embargo la mayoría de las empresas considera que es muy importante obtener certificaciones, aunque también es muy elevado el número de personas que no saben si determinada certificación es o no importante.

Conclusiones generales

En nuestros días la consideración de que la información es un activo a proteger debería marcar el 100% o al menos un índice mayor, pero lamentablemente muchos usuarios confían más en los correos que les envían sus amigos con diapositivas que solo confunden más al usuario, haciéndole creer que está aprendiendo cosas nuevas, cuando en realidad están colaborando con la ingeniería social y siendo víctimas de fraudes.

Es razonable bajo este panorama que el índice de empresas que no consideran la información como un activo a proteger sea tan alto; existen muchos riesgos de que se pierda información o no se respete su confidencialidad pero a pesar de que existen cursos y certificaciones en seguridad informática, así como herramientas para prevenir intrusiones, éstas no serán suficientes si no se han aprovechado tanto como se podría o como bien señala el Dr. Jeimy Cano, la formación y práctica constante de los profesionales responsables no se hace evidente en el proceso de investigación y registro de evidencias provocadas.[7]

De acuerdo a los resultados obtenidos, el apoyo por parte de otras áreas de la organización y de directivos es muy poco y parece haber una cultura de dejar todo en manos del personal de informática o bien en el hardware y software especializados[8], pero no invertir demasiado dinero en proteger la información como activo de la empresa, en la capacitación del personal o en el diseño e implementación de procesos de documentación de evidencias que incluyan estrategias y políticas para establecer medidas de seguridad en ambientes altamente expuestos[9], esta es sin duda una de las

más grandes áreas de oportunidad no solo para el Departamento de Sistemas, sino para los Directivos de la organización.

Se conocen muchos mecanismos para proteger la información, pero en muchos casos no se tiene tecnología de vanguardia (los intrusos sí la tienen). A modo de analogía podemos decir que esto es tan peligroso o más que dejar un auto estacionado con las llaves pegadas en la puerta y sin que tenga alarmas ni seguro contra robos.

Por último, cabe señalar que no podemos confiar todo al personal de seguridad informática, ni los departamentos de Seguridad Informática pueden ser independientes ni estar aislados; se requiere que las autoridades jurídicas, las instituciones educativas, los proveedores de servicios y la empresa privada unan esfuerzos en una lucha por desarrollar cada día mejores sistemas y tecnologías para prevención de ataques, así como despertar el interés por denunciar a quienes intenten cometer delitos y sobre todo, por generar nuevos códigos de conducta a favor de una cultura de respeto a la privacidad, a la paz y al desarrollo social.

***Jorge E. Macias Garza**; Ing. Mecánico Electricista por la Universidad Anáhuac del Sur (México D.F.). Master en Administración de Empresas y Master en Computación por parte de la Universidad del Valle de Atemajac (UNIVA). Tutor en el Departamento de Computación, Sistemas y Electrónica; Catedrático de lenguajes de programación a nivel superior y de negocios electrónicos a nivel postgrados.*

***Gabriela Maria Saucedo Meza**; Lic. en Sistemas Computacionales y Master en Desarrollo Organizacional y Humano por la Universidad del Valle de Atemajac (UNIVA); Coordinador de Proyectos Institucionales en UNIVA; Catedrática en las áreas de Sistemas e Ingeniería Industrial en Educación Superior, y a nivel Postgrados en Desarrollo Organizacional y Humano, Educación e Ingeniería de Software.*

Guadalajara, Jalisco, México. 7 de mayo 2007

Referencias

[1] OZ EFFY, Administración de sistemas de información, 2ª. Edición, Thomson Learning, Pennsylvania State University, 2001. Pág. 618
[2] http://www.navegaprotegido.org.mx/default.aspx; última fecha de consulta: Mayo 6, 2007
[3] MEYER, N.DEAN; BOONE MARY E., La informática en la Gerencia, una inversión estratégica y productiva, 2ª. Edición, Editorial Legis, Colombia, 1990, pág. 25
[4] http://www.esemanal.com.mx/articulos.php?id_sec=2&id_art=4839, 20 marzo del 2007
[5] JOINT FUTURE SYSTEMS S.C, http://www.jfs.com.mx/estudios_publicados_1.htm
[6] 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
[7] CANO, JEIMY J.; Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas; Boletín de los Sistemas Nacionales Estadístico y de Información Geográfica; INEGI, Vol. 1, Num. 1, mayo-agosto 2005; México.
[8] STAIR RALPH M, REYNOLDS GEORGE W.; Principios de Sistemas de Información, 4a. edición, Thomson, USA, 2000
[9] Insecurity Governance: Decisiones basadas en la inseguridad de la información, http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450000911, 22 de abril 2007, última fecha de consulta: mayo 6, 2007.