Estudio de Percepción
Seguridad en Informática México 2005

Ante la necesidad de contar con información específica de México, respecto de la percepción que sobre Seguridad en Informática tienen los usuarios de diferentes sectores, en el año 2004 Joint Future Systems encabezó la realización de un estudio de mercado que permitió evaluar el grado de conocimiento y la percepción que existe al respecto, entre dos segmentos fundamentales: los usuarios corporativos e institucionales, así como expertos en la materia y proveedores líderes en el mercado de soluciones de Tecnología de la Información (TI).

Bajo esta misma mecánica, entre los meses de mayo y agosto de 2005, se llevó a cabo el **Estudio de Percepción sobre Seguridad en Informática México 2005**, con el propósito de dar continuidad a este esfuerzo por generar estadísticas del entorno de nuestro país en la materia, y de contar con parámetros comparativos que permitan vislumbrar las variaciones (avances o rezagos percibidos por los entrevistados) de un año a otro.

De acuerdo a lo mencionado anteriormente, este estudio proporciona información recopilada de dos fuentes complementarias, lo que permite contemplar ambas perspectivas, tanto la del usuario común, como la del experto y proveedor de la industria. Con la finalidad de que los lectores del presente documento obtengan información adicional sobre el tema, al final del mismo se incluye una sección con artículos escritos por algunos de los patrocinadores, que hablan específicamente sobre seguridad en informática y el desempeño de sus empresas dentro de este ámbito. Es así que el contenido del estudio se ha clasificado de la siguiente manera:

A) Estudio de Mercado entre empresas y áreas usuarias de TI.
B) Estudio de opinión y análisis con 21 expertos en diversos rubros de la seguridad en informática
C) Artículos de interés, relacionados con seguridad en informática.

A) Estudio de Mercado entre empresas y áreas usuarias de TI

Levantamiento de información y opiniones de 1,200 ejecutivos de diferentes niveles, pertenecientes a empresas privadas de diversos sectores, empresas paraestatales, dependencias gubernamentales, instituciones educativas, cámaras y asociaciones.

B) Estudio de opinión y análisis con proveedores líderes del mercado de soluciones TI

Cuestionario estructurado, respondido por expertos y directivos de instituciones y organizaciones con amplia experiencia en la materia.

Empresas patrocinadoras

Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C. (ALAPSI)

Cámara Mexicano-Alemana de Comercio e Industria, A.C. (CAMEXA)

Cámara Nacional de la Industria Electrónica de Telecomunicaciones e Informática (CANIETI)

Computer Associates

Intel México

Joint Future Systems

Kio NetWorks México

Sun Microsystems de México

Técnica Comercial Vilsa

JFS

Se agradece asimismo la ayuda de la Fundación Ealy Ortiz, A.C., el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México, el Proyecto Internet ITESM-CEM y la International Association of Financial Crime Investigation (IAFCI).

Las opiniones expresadas en los artículos pueden o no reflejar el punto de vista de los patrocinadores, y son responsabilidad de sus autores.

Los resultados del estudio expresan la opinión de los encuestados y pueden o no reflejar el punto de vista de los patrocinadores.

Contenido

JFS

I. Alcances de la investigación total

1. Conocer los niveles de conciencia que se tienen en las empresas mexicanas, acerca de la Seguridad en Informática.

2. Detectar el grado de conocimiento que se tiene con respecto a los diferentes ámbitos de la Seguridad en Informática (Seguridad Física, Seguridad frente a Agresores Externos y Seguridad frente a Agresores Internos).

3. Identificar aquellos elementos relacionados con la Seguridad en Informática, que son considerados más importantes por los responsables de su implementación dentro de sus organizaciones.

4. Conocer la percepción que tienen diferentes expertos y algunos proveedores cuyas soluciones tienen incidencia directa o indirecta sobre la Seguridad en Informática, respecto del grado de conocimientos y penetración de esta cultura entre las organizaciones de nuestro país.

5. Contar con una herramienta que permita fomentar la conciencia y desmitificación de la Seguridad en Informática, apoyando las labores educativas del país a nivel corporativo e institucional.

6. Crear un entorno que impulse el crecimiento del mercado de productos y servicios de seguridad, así como la correcta implementación de soluciones especializadas.

7. Proveer de estadísticas comparativas que permitan seguir la evolución e identificar los cambios en la percepción que se tiene sobre la Seguridad en Informática, entre los diferentes años de evaluación.

II. Investigación entre empresas y áreas usuarias de TI

Objetivos del estudio

- Determinar el nivel de conocimiento general sobre medidas de Seguridad en Informática, entre directivos y niveles medios de empresas privadas e instituciones gubernamentales.
- Determinar el grado de conocimiento de marcas y empresas en México, involucradas en la seguridad en informática.
- Bosquejar una escala jerárquica de percepción acerca de la importancia de los diferentes rubros, productos y servicios, que intervienen en el concepto global de Seguridad en Informática.
- Conocer la percepción que se tiene (puntos fuertes y deficiencias), acerca de la cultura de seguridad en informática en México.
- Conocer la percepción que se tiene (puntos fuertes y deficiencias), acerca de los diferentes proveedores de productos y servicios de seguridad en México.

JFS

Metodología

Método de investigación
Encuestas telefónicas.

Las encuestas fueron realizadas en el periodo que abarca del 20 de junio al 16 de agosto de 2005.

Instrumento de medición
Cuestionario estructurado.

Características de la muestra
Perfil de los entrevistados

Característica principal	Directivos y niveles medios de diferentes áreas organizacionales, como son Direcciones Generales, Sistemas, Administración y Finanzas, según dimensiones y características de la Organización.	
Edad:	Indistinta	
Sexo:	Indistinto	
Cobertura geográfica:	México, D.F. Guadalajara, Jal. Monterrey, N.L.	50% 25% 25%
N.S.E.	Indistinto	
Especiales:	Usuario de equipo de cómputo con antigüedad mayor a los 2 años y una frecuencia de uso promedio superior a las 10 horas semanales.	

Cuotas por área organizacional

Áreas de Sistemas	30%
Otras áreas	70%

Campo de muestreo
Se utilizaron diversas bases de datos públicas.

Tamaño de la muestra
1,200 entrevistas efectivas con ejecutivos y gerentes de 972 organizaciones, concretadas a partir de procedimientos aleatorios de selección sobre el campo de muestreo.

Codificación de respuestas
Por las características del estudio, la metodología requería la obtención de múltiples respuestas abiertas y espontáneas por parte de los entrevistados. Para una fácil comprensión de las tendencias de las respuestas, todas ellas fueron clasificadas en categorías y subcategorías (proceso de codificación) que describen las opiniones de los entrevistados, agrupadas en términos específicos, y que permiten establecer frecuencias y porcentajes.

Resultados

Composición de la muestra

La composición de la muestra, clasificada bajo tres criterios – por sector, por sexo y por puesto o área de trabajo – se puede observar en la Tabla 1, Tabla 2 y Tabla 3, respectivamente.

Tabla 1

Composición de la muestra por SECTOR		
Giro	**Total**	**Proporción**
Servicios	458	38.2%
Comercio	274	22.8%
Manufactura	191	15.9%
Gobierno	166	13.8%
Instituciones Educativas	55	4.6%
Comunicaciones	28	2.3%
Cámara / Asociación	17	1.4%
Transportación	11	0.9%
Total general	**1,200**	**100.0%**

Tabla 2

Composición de la muestra por SEXO		
Giro	**Total**	**Proporción**
Hombre	856	71.3%
Mujer	344	28.7%
Total general	**1,200**	**100.0%**

Tabla 3

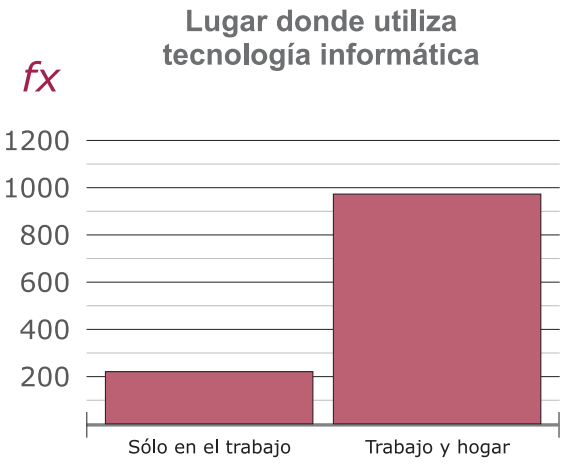
Composición de la muestra por PUESTO/AREA		
Giro	**Total**	**Proporción**
Sistemas	360	30.0%
Admon./Finanzas	373	31.1%
P/VP/DG/Dueño/Estrategia *	111	9.3%
Producción/Operaciones	152	12.7%
Mkt./Publicidad	111	9.3%
Ventas	93	7.8%
Total general	**1,200**	**100.0%**

* P/VP/DG/Dueño/Estrategia.- Este perfil contempla puestos como Presidente, Vicepresidente, Director General, Consejero, Dueño de la empresa, accionista, Director de Área, Oficial Mayor, etc.

Lugar donde utilizan equipo de cómputo

La Gráfica 1 presenta la distribución de la muestra, de acuerdo al lugar en donde utilizan equipo de cómputo, en donde se puede observar que la gran mayoría (81.75%) utiliza computadoras tanto en casa como en el trabajo, mientras el 18.25% lo utiliza únicamente en el trabajo.

Dónde suele utilizar equipo de cómputo



Gráfica 1

Qué se entiende por "Seguridad en Informática"

Pregunta: Hablando del término "Seguridad en Informática", ¿Qué entiende usted por este concepto? ¿Para usted qué significa?

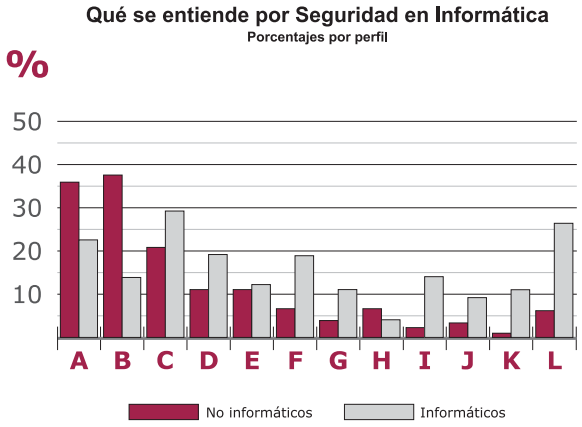
Se registraron todas las respuestas emitidas por los entrevistados, quienes por lo regular mencionaron más de una opción (1.59 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codificadas, pueden apreciarse en la Tabla 4 y la Gráfica 2.

QUE SE ENTIENDE POR SEGURIDAD EN INFORMATICA

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Acceso autorizado	303	81	384	36.1%	22.5%	25.3%	6.8%	32.0%
Protección contra virus	315	51	366	37.5%	14.2%	26.3%	4.3%	30.5%
Integridad / Confiabilidad de la información	173	105	278	20.6%	29.2%	14.4%	8.8%	23.2%
Políticas adecuadas	92	70	162	11.0%	19.4%	7.7%	5.8%	13.5%
Respaldo de información	91	42	133	10.8%	11.7%	7.6%	3.5%	11.1%
Protección contra hackers	59	67	126	7.0%	18.6%	4.9%	5.6%	10.5%
No existe.	34	39	73	4.0%	10.8%	2.8%	3.3%	6.1%
Cuidado de los equipos / energía eléctrica	55	15	70	6.5%	4.2%	4.6%	1.3%	5.8%
Transmisión segura de datos	17	51	68	2.0%	14.2%	1.4%	4.3%	5.7%
Medidas contra Phishing / Ingeniería Social	32	33	65	3.8%	9.2%	2.7%	2.8%	5.4%
Manejo de Identidad	7	40	47	0.8%	11.1%	0.6%	3.3%	3.9%
Disponibilidad de la información	-	12	12	-	3.3%	-	1.0%	1.0%
Otros	51	83	134	6.1%	23.1%	4.3%	6.9%	11.2%

JFS

TABLA 4



GRÁFICA 2

A Acceso autorizado
B Protección contra virus
C Integridad / Confiabilidad de la información
D Políticas adecuadas
E Respaldo de información
F Protección contra "hackers"
G No existe
H Cuidado de los equipos / energía eléctrica
I Transmisión segura de datos
J Medidas contra Phishing / Ingeniería Social
K Manejo de identidad
L Otros

Coincidentemente con el estudio realizado en 2004, de manera general los tres principales conceptos asociados a Seguridad en Informática, son el acceso autorizado (tanto la entrada a los sistemas como a las instalaciones donde se encuentran los equipos), la protección contra virus y la integridad y confiabilidad de la información. Destaca, sin embargo, que las políticas adecuadas muestran un mayor número de respuestas en relación con el año anterior, incluso por encima de las menciones referentes al respaldo de información.

Para el grupo de los Informáticos, Seguridad en Informática tiene más que ver con la integridad y la confiabilidad de la información, que con la protección contra Virus, al revés que con el grupo de los No Informáticos. De hecho, ese concepto es el más mencionado por los Informáticos (29.2%).

Es notoria una mayor preocupación por parte del grupo de los Informáticos, sobre los No Informáticos, por cuestiones como Políticas, protección contra Hackers, transmisión segura de datos y manejo de identidad. Esta última, figura con un alto número de menciones frente al estudio de 2004, siendo considerada por un 11.1% de los mismos Informáticos.

Otra diferencia, es que el uso de software original ya no es considerado como una cuestión relacionada con seguridad. Sin embargo, otros conceptos por primera vez aparecen con una frecuencia considerable, como son las medidas contra Phishing o mayor educación para enfrentar la Ingeniería Social.

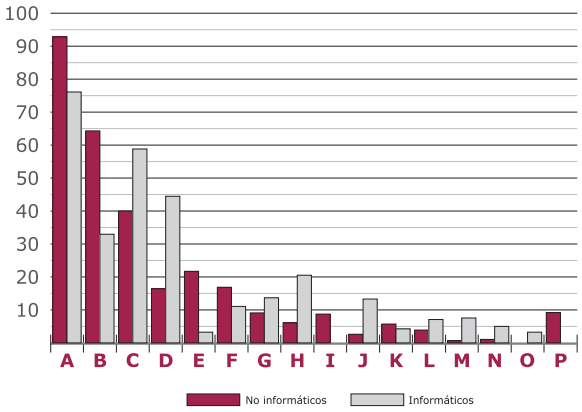
Resulta asimismo notorio que la Disponibilidad de la información es preocupación exclusiva de los Informáticos (3.3% de ese grupo), mientras que no hubo ninguna mención en este sentido por parte de los No Informáticos.

Las 3 principales amenazas que pueden poner en riesgo la Seguridad de equipos de cómputo y su contenido.

Se solicitó a los entrevistados que mencionaran las 3 principales amenazas que consideraban de manera espontánea. Posteriormente se les indicó que las numeraran de acuerdo al nivel de riesgo que percibían para cada una.

Pregunta: Por favor mencione las 3 cosas que más le preocupan, en relación con la seguridad de los equipos de cómputo y de su contenido.

En conjunto, las principales amenazas fueron como se describe en la Tabla 5 y en la Gráfica 3.



GRÁFICA 3

A	Virus
B	Desconocimiento
C	"hackers" y otros agresores externos
D	Agresores internos
E	Fallas de energía
F	Negligencia de usuarios
G	Accesos inalámbricos / Conectividad deficiente.
H	Software deficiente
I	Internet
J	Spyware / Adware
K	Extracción de información
L	Insuficiencia de equipo informático
M	Phishing / Ingeniería social
N	Hardware deficiente
O	Robo de identidad
P	NS/NC

PRINCIPALES AMENAZAS QUE PONEN EN RIESGO LA SEGURIDAD DE LA INFORMACIÓN (3 menciones por entrevistado)

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Virus	781	274	1,055	93.0%	76.1%	65.1%	22.8%	87.9%
Desconocimiento	541	118	659	64.4%	32.8%	45.1%	9.8%	54.9%
Hackers y otros agresores externos	337	210	547	40.1%	58.3%	28.1%	17.5%	45.6%
Agresores internos	138	161	299	16.4%	44.7%	11.5%	13.4%	24.9%
Fallas de energía	183	10	193	21.8%	2.8%	15.3%	0.8%	16.1%
Negligencia de usuarios	143	39	182	17.0%	10.8%	11.9%	3.3%	15.2%
Accesos Inalámbricos / Conectividad deficiente	81	50	131	9.6%	13.9%	6.8%	4.2%	10.9%
Software Deficiente	55	73	128	6.5%	20.3%	4.6%	6.1%	10.7%
Internet	72	-	72	8.6%	-	6.0%	-	6.0%
Spyware / Adware	18	48	66	2.1%	13.3%	1.5%	4.0%	5.5%
Extracción de información	45	15	60	5.4%	4.2%	3.8%	1.3%	5.0%
Insuficiencia de equipo informático	33	26	59	3.9%	7.2%	2.8%	2.2%	4.9%
Phishing / Ingeniería Social	5	27	32	0.6%	7.5%	0.4%	2.3%	2.7%
Hardware Deficiente	10	18	28	1.2%	5.0%	0.8%	1.5%	2.3%
Robo de Identidad	-	11	11	-	3.1%	-	0.9%	0.9%
NS/NC	78	-	78	9.3%	-	6.5%	-	6.5%

TABLA 5

Los ataques de Virus, sin lugar a dudas, siguen ocupando la primera posición en la mente de los usuarios (tanto No Informáticos como Informáticos), como una de las 3 principales amenazas contra la Seguridad de la información, siendo mencionados por el 93.0 % de los entrevistados del primer grupo y por el 76.1% de los del segundo.

JFS

El desconocimiento también sigue figurando como una amenaza importante para ambos grupos, en mayor medida para los No Informáticos (64.4%).

Si bien para los Informáticos el desconocimiento representa también una de las principales amenazas (32.8%), a diferencia de los No Informáticos este grupo considera una amenaza mayor a los "hackers" y otros agresores externos (58.3%).

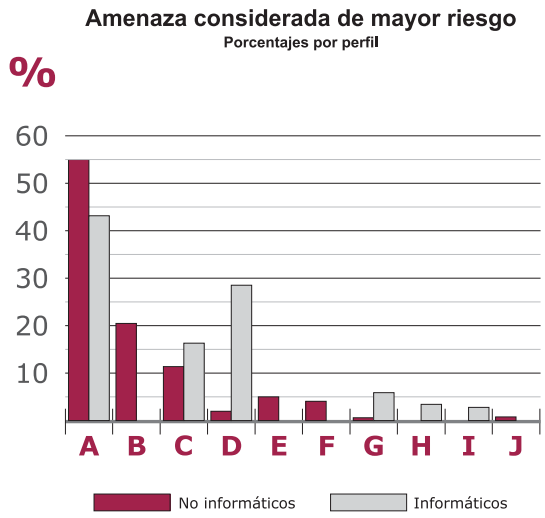
Los agresores internos, a su vez, son considerados como una amenaza importante, en mucha mayor medida por los Informáticos (44.7%) que para los No Informáticos (16.4%).

También en el grupo de Informáticos, destacan menciones alrededor del software deficiente y del spyware / adware. Perciben que las soluciones informáticas, tanto a nivel de hardware como de software, deberían traer de fábrica más elementos de seguridad y no dejar toda la responsabilidad a los administradores de las redes, quienes deben adquirir complejos paquetes de herramientas (suits), estar al pendiente de la aparición de parches que corrigen deficiencias de aplicaciones liberadas con premura, etc.

La amenaza considerada de mayor riesgo

Pregunta complementaria a la anterior: Por favor asigne un número de 1 a 3 a las amenazas que acaba de mencionar, indicando 1 para aquélla que considera más riesgosa y 3 la que dejaría como última prioridad.

La amenaza clasificada con el número 1 (la considerada como de mayor riesgo por los entrevistados), fue como se describe en la Tabla 6 y en la Gráfica 4.



GRÁFICA 4

A Virus
B Desconocimiento
C "hackers" y otros agresores externos
D Agresores internos
E Software deficiente
F Fallas de energía
G Negligencia de usuarios
H Robo de identidad
I Accesos inalámbricos / conectividad deficiente
J Extracción de información

LA AMENAZA CONSIDERADA DE MAYOR RIESGO

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Virus	461	156	**617**	54.9%	43.3%	38.4%	13.0%	**51.4%**
Desconocimiento	172	-	**172**	20.5%	-	14.3%	-	**14.3%**
Hackers y otros agresores externos	97	59	**156**	11.5%	16.4%	8.1%	4.9%	**13.0%**
Agresores internos	18	103	**121**	2.1%	28.6%	1.5%	8.6%	**10.1%**
Software Deficiente	42	-	**42**	5.0%	-	3.5%	-	**3.5%**
Fallas de energía	36	-	**36**	4.3%	-	3.0%	-	**3.0%**
Negligencia de usuarios	4	21	**25**	0.5%	5.8%	0.3%	1.8%	**2.1%**
Robo de Identidad	-	11	**11**	-	3.1%	-	0.9%	**0.9%**
Accesos Inalámbricos / Conectividad deficiente	-	10	**10**	-	2.8%	-	0.8%	**0.8%**
Extracción de información	10	-	**10**	1.2%	-	0.8%	-	**0.8%**
	840	**360**	**1,200**	**100.0%**	**100.0%**	**70.0%**	**30.0%**	**100.0%**

TABLA 6

Virus y desconocimiento son amenazas consideradas como las más significativas dentro del grupo de No Informáticos (75.4% entre ambas menciones).

Virus y agresores internos, representan la amenaza de mayor riesgo para la mayoría de los Informáticos (71.9% entre ambas menciones).

Es notorio que si bien los Informáticos también perciben el Desconocimiento como una fuente de riesgo (mencionado entre las 3 principales amenazas), ninguno lo consideró como la amenaza de mayor riesgo.

Principales medidas sugeridas por los entrevistados, para proteger la información electrónica de una organización

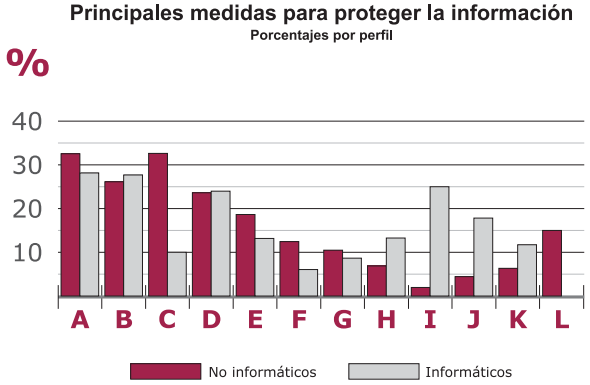
Pregunta: ¿Cuáles son las principales medidas que sugeriría para proteger la información electrónica de una organización?

La tabla de frecuencias y gráfica de respuestas a esta pregunta sobre las sugerencias para proteger la información electrónica, se presentan, respectivamente, en la Tabla 7 y en la Gráfica 5.

PRINCIPALES MEDIDAS PARA PROTEGER LA INFORMACIÓN ELECTRÓNICA

	FRECUENCIA (fx) Actividad / Puesto			PORCENTAJES De su categoría		PORCENTAJES Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Antivirus	273	102	375	32.5%	28.3%	22.8%	8.5%	31.3%
Capacitación adecuada	223	101	324	26.5%	28.1%	18.6%	8.4%	27.0%
Manejo adecuado de contraseñas	272	36	308	32.4%	10.0%	22.7%	3.0%	25.7%
Políticas / implementación de controles de acceso	201	87	288	23.9%	24.2%	16.8%	7.3%	24.0%
Respaldar información	160	48	208	19.0%	13.3%	13.3%	4.0%	17.3%
Instalaciones físicas adecuadas	106	21	127	12.6%	5.8%	8.8%	1.8%	10.6%
Políticas integrales y una cultura de seguridad en informática	87	31	118	10.4%	8.6%	7.3%	2.6%	9.8%
Apoyarse con empresas especializadas / outsourcing	59	47	106	7.0%	13.1%	4.9%	3.9%	8.8%
Firewalls / Proxy	16	90	106	1.9%	25.0%	1.3%	7.5%	8.8%
Monitoreo y control de sistemas	38	64	102	4.5%	17.8%	3.2%	5.3%	8.5%
Software seguro / actualizado	54	43	97	6.4%	11.9%	4.5%	3.6%	8.1%
Políticas Antipiratería	27	45	72	3.2%	12.5%	2.3%	3.8%	6.0%
Protección accesos inalámbricos	7	61	68	0.8%	16.9%	0.6%	5.1%	5.7%
Vigilancia y supervisión	25	26	51	3.0%	7.2%	2.1%	2.2%	4.3%
Uso de biométricos	6	40	46	0.7%	11.1%	0.5%	3.3%	3.8%
Mantenimiento adecuado de hardware	20	24	44	2.4%	6.7%	1.7%	2.0%	3.7%
Sistemas Operativos más seguros	5	29	34	0.6%	8.1%	0.4%	2.4%	2.8%
Reclutamiento y selección de personal adecuados	20	-	20	2.4%	-	1.7%	-	1.7%
Redundancia	0	16	16	-	4.4%	-	1.3%	1.3%
Implementación correcta de los sistemas	0	14	14	-	3.9%	-	1.2%	1.2%
Otros	113	62	175	13.5%	17.2%	9.4%	5.2%	14.6%
NS/NC	126	-	126	15.0%	-	10.5%	-	10.5%

TABLA 7



GRÁFICA 5

A Antivirus
B Capacitación adecuada
C Manejo adecuado de contraseñas
D Políticas / implementación de controles de acceso
E Respaldar información
F Instalaciones físicas adecuadas
G Políticas integrales y una cultura de seguridad en informática
H Apoyarse con empresas especializadas / Outsourcing
I Firewalls / Proxy
J Monitoreo y control de sistemas
K Software seguro / actualizado
L NS/NC
M Otros *

*** Otros.** *En el rubro de "Otros" se agruparon todas aquellas respuestas que en conjunto (entre las de los Informáticos y las de los No Informáticos), aún codificadas, no llegaban a una frecuencia importante que pudiera representarse adecuadamente en la gráfica. Dado que se trata de una pregunta abierta en la cual un solo entrevistado podía dar varias respuestas, el rubro de "Otros" resultó elevado (muchas respuestas con contenido muy diverso)*

y quitaba legibilidad a la gráfica, por lo cual no aparece incluido dentro de la misma. Las respuestas clasificadas como "Otros" de mayor relevancia, se desglosan a mayor profundidad en la tabla de frecuencias, como son Políticas antipiratería, Protección de accesos inalámbricos, etc.

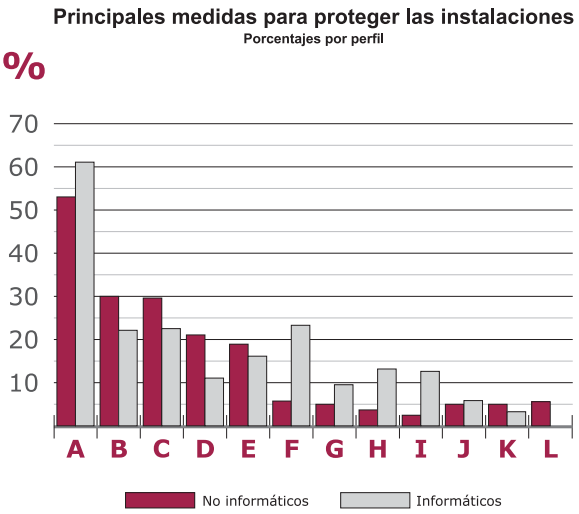
Las cuatro principales medidas para proteger la información, mencionadas por el grupo de Informáticos, son, por orden de importancia, Antivirus, Capacitación Adecuada, Firewalls / Proxys y Políticas e Implementación de Controles de Acceso, entre las que se mencionaron el establecimiento de privilegios, restricciones de acceso de personas a las instalaciones, turnos de trabajo bien definidos, acceso limitado a Internet para el personal, creación de planes de contingencia tipo DRP, etc. Entre otros aspectos que fueron mencionados, estuvieron la existencia de reglas claras por escrito, con sanciones bien determinadas y comunicadas, arcos de detección y lectores de tarjetas de identificación, gafetes visibles identificados por área, utilización de tecnología biométrica, etc.

Destaca también que un número importante de menciones, por parte del grupo de Informáticos, giró alrededor del Monitoreo de Sistemas, el apoyo de profesionales especializados y servicios de Outsourcing, así como el software seguro y actualizado. Mencionaron algunos de ellos, estar cansados de ser siempre los culpables de cualquier contingencia, cuando en las organizaciones no se tiene el presupuesto y la infraestructura para proteger la información adecuadamente (en aspectos como la adquisición de no-breaks, la contratación de personal capacitado y suficiente, etc.).

Para los No Informáticos, las soluciones percibidas fueron el uso de Antivirus y el Manejo Adecuado de Contraseñas (prácticamente en el mismo nivel), seguidas por una Capacitación Adecuada y Políticas e Implementación de Controles de Acceso. También destaca la mención del respaldo de información y el contar con instalaciones físicas adecuadas.

Principales medidas sugeridas por los entrevistados, para proteger las instalaciones donde se encuentran los equipos de cómputo y telecomunicaciones

Pregunta: ¿Cuáles son las principales medidas que sugeriría para proteger las instalaciones donde se encuentran los equipos de cómputo y telecomunicaciones de una organización?



GRÁFICA 6

A	Políticas / implementación de controles de acceso
B	Supervisión y vigilancia adecuada
C	Centro de cómputo cerrado / aislado
D	Sistemas de administración de energía
E	Instalaciones físicas adecuadas
F	Equipo contra incendios
G	Mantenimiento adecuado de instalaciones
H	Medidas de protección civil
I	Apoyarse con empresas especializadas / Outsourcing
J	Políticas integrales y una cultura de seguridad en informática
K	Reclutamiento y selección de personal adecuados
L	NS/NC - No Sabe / No Contestó

Ambos grupos, tanto Informáticos como No Informáticos, coinciden en que las principales medidas de protección de los sitios donde se encuentra la información y los equipos, están alrededor de Políticas y de la implementación de controles de acceso.

La supervisión y vigilancia adecuadas (integradas por una estructura organizacional con funciones y responsabilidades claramente delimitadas, personal de vigilancia y apoyo de tecnología, como cámaras de video, entre otros), es la segunda solución sugerida por los No Informáticos, apoyada por un número importante de Informáticos.

Queda claro también, en una proporción de menciones similar a la anterior, que los servidores, respaldos y sistemas de telecomunicaciones, deben mantenerse físicamente aislados.

Resulta interesante observar que en el grupo de Informáticos, está más arraigada la conciencia de contar con equipos contra incendio, de detección y detonación automática principalmente, como una medida de seguridad de las instalaciones, así como las tácticas de protección civil.

Un número importante de Informáticos, mencionó el Outsourcing como medida, argumentando que ven difícil que en sus organizaciones se llegue a tener la infraestructura necesaria para brindar la seguridad que requieren sus centros de cómputo.

JFS

PRINCIPALES MEDIDAS PARA PROTEGER LAS INSTALACIONES FISICAS DONDE SE ENCUENTRAN LOS EQUIPOS

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Políticas / implementación de controles de acceso	439	218	**657**	52.3%	60.6%	36.6%	18.2%	**54.8%**
Supervisión y vigilancia adecuadas	251	80	**331**	29.9%	22.2%	20.9%	6.7%	**27.6%**
Centro de cómputo cerrado / aislado	249	81	**330**	29.6%	22.5%	20.8%	6.8%	**27.5%**
Sistemas de administración de energía	181	40	**221**	21.5%	11.1%	15.1%	3.3%	**18.4%**
Instalaciones físicas adecuadas	159	59	**218**	18.9%	16.4%	13.3%	4.9%	**18.2%**
Equipo contra incendio	45	83	**128**	5.4%	23.1%	3.8%	6.9%	**10.7%**
Mantenimiento adecuado de instalaciones	42	35	**77**	5.0%	9.7%	3.5%	2.9%	**6.4%**
Medidas de protección civil	29	46	**75**	3.5%	12.8%	2.4%	3.8%	**6.3%**
Apoyarse con empresas especializadas / outsourcing	20	45	**65**	2.4%	12.5%	1.7%	3.8%	**5.4%**
Políticas integrales y una cultura de seguridad en informática	42	20	**62**	5.0%	5.6%	3.5%	1.7%	**5.2%**
Reclutamiento y selección de personal adecuados	41	11	**52**	4.9%	3.1%	3.4%	0.9%	**4.3%**
NS/NC	46	-	**46**	5.5%	-	3.8%	-	**3.8%**

TABLA 8

Percepción acerca de diversas marcas asociadas con Seguridad en Informática

Para conocer por un lado la identificación y recordación de marcas asociadas con Seguridad en Informática, así como la opinión que se tiene acerca de las mismas, se hicieron dos preguntas a los entrevistados:

Pregunta: Hablando concretamente de marcas de producto, tanto de hardware como de software, ¿Cuáles percibe que son buenas para enfrentar los problemas relacionados con Seguridad en Informática?

Pregunta: Hablando concretamente de marcas de producto, tanto de hardware como de software, ¿Cuáles percibe que tienen deficiencias para enfrentar los problemas relacionados con Seguridad en Informática?

Después de cada respuesta, se solicitó a los encuestados que explicaran más a fondo el porqué de su opinión al respecto. Para brindar una comprensión más sencilla de estas opiniones, la información se dividió en dos tablas, una con lo que opinaron los No Informáticos y otra con lo que opinaron los Informáticos, en las cuales se describen las respuestas codificadas de cada grupo, tanto las positivas (principales ventajas) como las negativas (principales deficiencias).

Nota importante: Los comentarios codificados en las columnas "Principales Fuerzas" y "Principales Deficiencias", no están ligadas al número de respuestas registradas en las columnas de menciones. Esto quiere decir que cualquier atributo, positivo o negativo, respecto de cualquier marca, fue respondido por una parte importante de quienes opinaron, mas no necesariamente por la totalidad. Por otro lado, tampoco se incluyen todos los atributos mencionados, sino únicamente aquéllos que tuvieron mayor frecuencia. De ahí que se denomine como "Principales".

En algunas respuestas respecto de diversas marcas, a pesar de que no existe ninguna mención contabilizada como marca buena o deficiente (frecuencia fx=0), se incluyeron comentarios en relación con la percepción de Principales Fuerzas o Principales Deficiencias. Esto se debe a que, a fin de enriquecer los resultados del estudio, se incluyeron comentarios hechos por los entrevistados, que no necesariamente tenían una relación directa con el carácter positivo o negativo de la pregunta. Por ejemplo, ante la pregunta ¿Cuáles marcas percibe como buenas para enfrentar los problemas relacionados con seguridad en informática?, hubo quien mencionó la marca y agregó alguna opinión adicional al respecto, en sentido opuesto: "X marca es buena, por tales razones. Sin embargo,..." o "Tal marca es buena, con tales cualidades, pero lástima que...".

Las respuestas clasificadas de ambos grupos, pueden consultarse en las respectivas Tabla 9 y Tabla 10.

Opinión de los NO INFORMÁTICOS respecto de las marcas que asocian con seguridad en informática

Marca	Menciones como marca buena (fx)	Menciones como marca deficiente(fx)	Principales Fuerzas	Principales Deficiencias
3Com	29	-	Eficaz	
Apple / Macintosh	28	-	Buena marca	
Cajas blancas	-	46	Bajo costo	Inestable
Cisco	40	-	Eficaz	
Computer Associates / Innoculate	29	-	Eficaz	
Dell	44	-	Buena marca	
Firefox	8	-		
HP	129	13	Buena marca. Buen soporte	Alto costo
IBM	40	23	Confiable	Poco soporte
Lanix	-	16		
Linux	17	-	Confiable	
LiveCall - Hauri	13	-	Confiable	
McAfee	78	45	Eficaz	Inestable. Poco soporte.
Microsoft	52	123	Marca líder	Inestable. Poco soporte. Alto costo.
Netscape	22	-	Poco vulnerable	
Oracle	18	6	Tecnología robusta	
Panda	9	5		
Rainbow	2	-		
Sony	21	35	Buena marca	Inestable. Alto costo.
Sun-Solaris	14	-	Confiable	
Symantec / Veritas	177	24	Marca líder. Buen Soporte. Eficaz.	Mal soporte.
Toshiba	15	-	Buena marca	
VeriSign	3	-		
Windows XP	-	10		Inestable
Otros	100	111		
NS/NC	266	482		

TABLA 9

Opinión de los INFORMÁTICOS respecto de las marcas que asocian con seguridad en informática

Marca	Menciones como marca buena (fx)	Menciones como marca deficiente(fx)	Principales Fuerzas	Principales Deficiencias
3Com	35	-	Confiable. Bajo costo.	
Apple / Macintosh	18	-	Poca existencia de virus	
Centrino	-	19		Muy vulnerable
Checkpoint	36	-	Tecnología robusta	Difícil de implementar
Cisco	109	-	Tecnología robusta.	
Computer Associates / Innoculate	16	-	Eficaz	
Dell	5	-		
EMC2	14	-	Tecnología robusta	
Firefox	41	-	Poco vulnerable	
HP	12	-	Confiable	
IBM	23	11	Confiable	Mal servicio
Java	20	-	Compatible. Fácil de implementar.	
Linux	101	6	Código abierto. Fácil de detectar ataques.	Poco soporte
LiveCall - Hauri	6	-		
McAfee	69	9	Tecnología robusta	Inestable
Microsoft	26	115	Buena marca	Inestable. Muy vulnerable
Microsoft XP SP2	14	39	Incluye Firewall	Inestable. Poco compatible.
Netscape	40	-	Poco vulnerable	
Oracle	49	19	Tecnología robusta (la base de datos)	Alto costo
Panda	17	5		
Rainbow	11	-	Eficaz	
Software libre (open	-	25		Poco soporte
Sonicwall	15	-	Tecnología robusta	
Sun-Solaris	76	-	Tecnología robusta	
Symantec / Veritas	133	21	Marca líder. Buen soporte.	Alto costo
Trend Micro	10	-		
VeriSign	24	-	Marca líder	
Otros	33	60		
NS/NC	38	44		

TABLA 10

CAMEXA

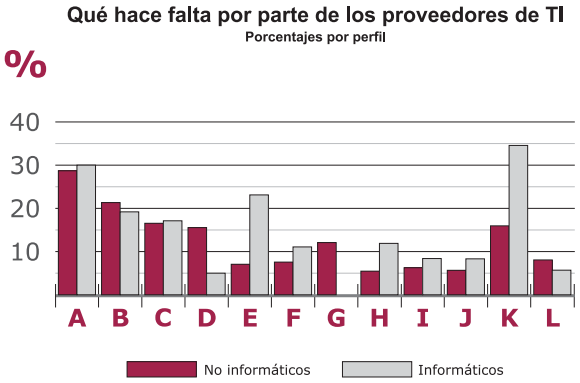
CANIETI

Computer Associates

En cuanto a Seguridad en Informática, qué hace falta por parte de los proveedores de TI.

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Información / más difusión	237	108	345	28.2%	30.0%	19.8%	9.0%	28.8%
Mejoras en el software / actualizaciones	177	70	247	21.1%	19.4%	14.8%	5.8%	20.6%
Mayor asesoría / consultoría	141	62	203	16.8%	17.2%	11.8%	5.2%	16.9%
Políticas razonables de precio	131	18	149	15.6%	5.0%	10.9%	1.5%	12.4%
Mejor integración de productos y soluciones	58	83	141	6.9%	23.1%	4.8%	6.9%	11.8%
Capacitación	61	41	102	7.3%	11.4%	5.1%	3.4%	8.5%
Facilidad de uso de hardware y software	100	-	100	11.9%	-	8.3%	-	8.3%
Mejores soluciones contra hackers	44	43	87	5.2%	11.9%	3.7%	3.6%	7.3%
Mejor soporte técnico	54	29	83	6.4%	8.1%	4.5%	2.4%	6.9%
Sistemas de identificación y control de usuarios	51	29	80	6.1%	8.1%	4.3%	2.4%	6.7%
Soluciones ad-hoc para cada empresa	12	44	56	1.4%	12.2%	1.0%	3.7%	4.7%
Información de soluciones para PyME	17	34	51	2.0%	9.4%	1.4%	2.8%	4.3%
Mayor capacidad técnica de los proveedores	20	10	30	2.4%	2.8%	1.7%	0.8%	2.5%
Más énfasis en el desarrollo de sitios seguros en Internet	11	12	23	1.3%	3.3%	0.9%	1.0%	1.9%
Mayor honestidad	-	12	12	-	3.3%	-	1.0%	1.0%
Otros	75	13	88	8.9%	3.6%	6.3%	1.1%	7.3%
NS/NC	66	19	85	7.9%	5.3%	5.5%	1.6%	7.1%

TABLA 11



GRÁFICA 7

A Información / más difusión
B Mejoras en el software / actualizaciones
C Mayor asesoría / Consultoría
D Políticas razonables de precio
E Mejor integración de productos y soluciones
F Capacitación
G Facilidad de uso de hardware y software
H Mejores soluciones contra "hackers"
I Mejor Soporte Técnico
J Sistemas de identificación y control de usuarios
K Otros
L NS/NC - No Sabe / No Contestó

Ambos grupos, en proporciones similares, coinciden en que siguen existiendo rezagos importantes en las áreas de información y difusión sobre temas relacionados con la Seguridad de la Información (28.2% de los No Informáticos y 30.0% de los Informáticos).

Para los Informáticos, la segunda opción que consideran hace falta por parte de los proveedores de TI, está en la mejor integración de productos y soluciones. En este sentido, se hizo referencia tanto al hecho de que no se ha tenido éxito en la creación de soluciones multiplataforma, que puedan interactuar de manera más sencilla y transparente, como a la convivencia de software de seguridad de distintos propósitos y marcas (firewalls, antivirus, anti spyware, etc.).

Tanto Informáticos como No Informáticos, consideran que el software en general puede mejorar sus esquemas de seguridad y que los procesos de actualización podrían optimizarse.

En tercer lugar para los No Informáticos y en cuarto para los Informáticos, se percibe la necesidad de mayor asesoría por parte de los fabricantes y de sus canales de distribución. Por un lado consideran que la tecnología

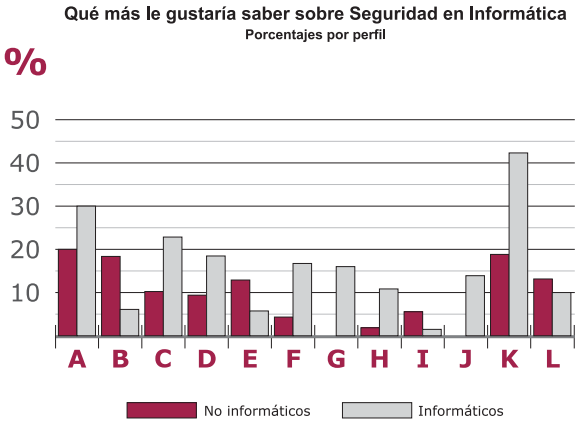
avanza más rápido que la capacidad de los proveedores para asimilar las nuevas cualidades de los productos. Por el otro, perciben que son pocas las empresas que toman en serio los servicios de consultoría. Unos, sólo ven por su interés de vender ciertas marcas; no hay objetividad e imparcialidad en sus asesorías. Otros, no se interesan por conocer las cualidades de los productos (por ejemplo, los mayoristas no se preocupan por configurar infraestructuras de capacitación a sus canales), o bien no se involucran a fondo con las necesidades de sus clientes.

Cabe destacar también, que el grupo de No Informáticos se presenta como más sensible a los precios de las soluciones de seguridad.

Qué más les gustaría conocer acerca de Seguridad en Informática

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Controles de acceso	169	108	277	20.1%	30.0%	14.1%	9.0%	23.1%
Más acerca de virus	150	22	172	17.9%	6.1%	12.5%	1.8%	14.3%
Más acerca de Hackers	86	82	168	10.2%	22.8%	7.2%	6.8%	14.0%
Seguridad en Internet	81	66	147	9.6%	18.3%	6.8%	5.5%	12.3%
Seguridad en Informática en general	107	20	127	12.7%	5.6%	8.9%	1.7%	10.6%
Seguridad en Comercio Electrónico	38	61	99	4.5%	16.9%	3.2%	5.1%	8.3%
Tecnología Inalámbrica	-	57	57	-	15.8%	-	4.8%	4.8%
Seguridad en telecomunicaciones	16	39	55	1.9%	10.8%	1.3%	3.3%	4.6%
Información de riesgos y soluciones para PyME	47	6	53	5.6%	1.7%	3.9%	0.5%	4.4%
Monitoreo y administración de redes	-	52	52	-	14.4%	-	4.3%	4.3%
Costo-Beneficio de los diferentes productos y servicios ofertados.	23	28	51	2.7%	7.8%	1.9%	2.3%	4.3%
Casos de éxito en la materia	31	18	49	3.7%	5.0%	2.6%	1.5%	4.1%
Difusión de los planes de Investigación y Desarrollo de las empresas de seguridad en informática	26	22	48	3.1%	6.1%	2.2%	1.8%	4.0%
Políticas y procedimientos / Mejores Prácticas	29	16	45	3.5%	4.4%	2.4%	1.3%	3.8%
Combate contra Spyware / Adware	2	23	25	0.2%	6.4%	0.2%	1.9%	2.1%
Más acerca de Phishing e ingeiería social	-	14	14	-	3.9%	-	1.2%	1.2%
Manejo de Identidad	-	8	8	-	2.2%	-	0.7%	0.7%
Otros	45	23	68	5.4%	6.4%	3.8%	1.9%	5.7%
NS/NC	109	36	145	13.0%	10.0%	9.1%	3.0%	12.1%

TABLA 12



GRÁFICA 8

A Controles de acceso
B Más acerca de virus
C Más acerca de *"hackers"*
D Seguridad en Internet
E Seguridad en informática en general
F Seguridad en Comercio Electrónico
G Tecnología inalámbrica
H Seguridad en telecomunicaciones
I Información de riesgos y soluciones para PyME
J Monitoreo y administración de redes
K Otros
L NS/NC - No Sabe / No Contestó

Las principales expectativas por conocer algo más relacionado con la Seguridad en Informática, para ambos grupos, corresponden básicamente al control de acceso de usuarios.

Para el grupo de los "No informáticos", las menciones más frecuentes en cuanto a control de acceso, en lo general se refirieron a:

- Cómo mantener la confidencialidad de su información
- Cómo restringir los accesos a su máquina
- Cómo configurar diferentes usuarios en un equipo
- Cómo bloquear el acceso a carpetas o archivos
- Cómo eliminar rastros de la actividad realizada

Para el grupo de los "Informáticos", las menciones más frecuentes en cuanto a control de acceso hacían referencia a:

- Herramientas de identidad
- Administración de puertos
- Tecnología biométrica
- Accesos remotos

Las siguientes prioridades de conocimiento para los Informáticos, fueron, en orden de importancia, más acerca de "hackers" y otros agresores externos, Seguridad en Internet, Seguridad en Comercio Electrónico, Tecnología Inalámbrica y Monitoreo de Redes.

Para los No Informáticos, aunque comparten inquietudes similares, sus prioridades cambian y giran alrededor de Virus y Seguridad en Informática en general, seguidas de información para prevenir los ataques de los "hackers" y Seguridad en Internet.

III. Estudio con expertos y proveedores líderes del mercado TI

Objetivos del estudio

1. Conocer la percepción que diversos expertos y líderes de opinión dentro de la industria, cuya actividad incide de manera directa o indirecta sobre la Seguridad en Informática, tienen respecto del grado de conocimientos y penetración de esta cultura entre las organizaciones de nuestro país.

JFS

2. Recabar la opinión de expertos y proveedores líderes de soluciones informáticas que operan en México, respecto del mercado actual de Seguridad en Informática, y compilar las diferentes visiones que tienen en cuanto a su desarrollo.

Metodología

Método de investigación

El estudio se realizó a través de cuestionario estructurado, el cual fue respondido tanto en entrevista personal y telefónica, como auto-administrado y enviado por correo electrónico.

Relación de entrevistados

Empresa	Nombre	Puesto
3Com	Ignacio Leñero	Director General
ALAPSI	Adrián Palma Castillo	Presidente
AMIPSI	Enrique Bustamante R.	Director General
AMITI	Javier Allard	Director General
Asiste	Moisés Polishuk	Director General
Avaya	José Gómez Obregón	Director General
CANIETI	Rogelio Garza	Director General
Cibercorp	Gerardo Hernández	Director General
Computer Associates	Rogelio Montekio	Gerente de Desarrollo de Negocios
DSS de México	Jesús Saucedo	Director General
Fundación Ealy Ortiz, A.C.	Enrique Bustamante Martínez	Director General
Grupo Vilsa	Luis Vidales	Director General
Insys	Antonio Quiñones Raúl Rodríguez	Vicepresidente Director de Desarrollo e Investigación
Intel	Jorge Gómez Figueroa	Gerente de Desarrollo de Negocios, Sector Financiero
ITESM	Francisco Camargo	Director de Informática
Kio Networks	José Fonseca	Director de Outsourcing
Microsoft	Felipe Lemaitre Carabias	Gerente de Seguridad Informática
Opentec	Carl Rianhard	Presidente
Oracle de México	Leopoldo Granados	Arquitecto de Soluciones
Sun Microsystems de México	Alejandro Salum Paulo Kalapis	Director de Mercadotecnia Gerente de la Práctica de Software
Symantec de México	Gabriel Alvarado	Sr. Regional Director México, Centro América, Caribe & Chile

Resultados

Situación de la Seguridad en Informática en México, frente a otros países del mundo

Se recopilaron opiniones en distintos sentidos. Hubo quienes ven un panorama negativo que requiere acciones urgentes, otros que opinan que la situación de México es la adecuada y unos más que hicieron notar algunos rubros en los que tenemos ventaja como país y otros en los que hay que esforzarse para mejorar.

De manera general, en materia de Seguridad en Informática se considera a México por debajo de los niveles de los países desarrollados. A nivel de América Latina, se considera que se encuentra al mismo nivel que los demás países e incluso en un nivel ligeramente superior al de la mayoría.

Existe la percepción de que a nivel de grandes empresas y corporativos, el nivel de conciencia respecto de la seguridad de la información es suficientemente alto, equiparable al de los países con mayor desarrollo tecnológico. Desde su posición, México observa las tendencias de la tecnología y las prácticas de punta, aprendiendo al mismo tiempo de la experiencia de quienes las implementan de manera inmediata, con lo que se da la oportunidad de seleccionar lo mejor de cada una de ellas.

Entre los principales aspectos de rezago, se mencionaron:

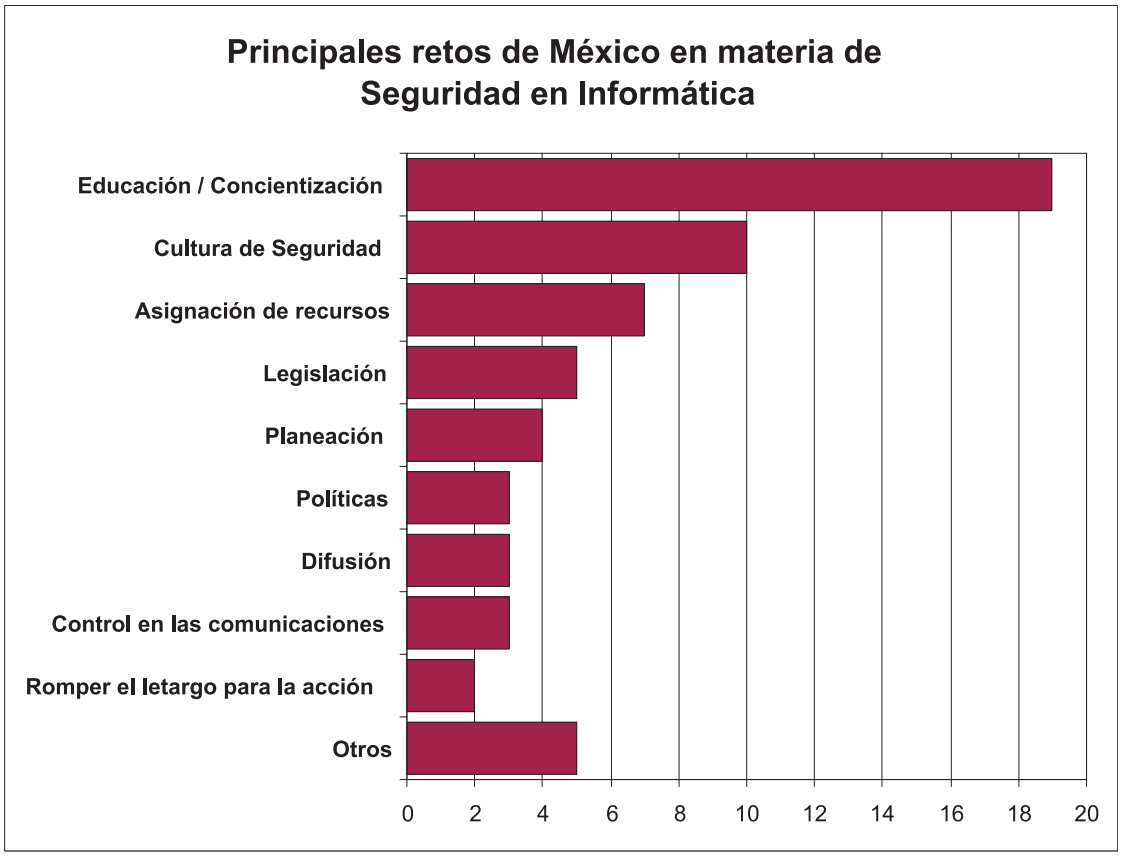
- Falta de cultura de seguridad, en general, así como poco conocimiento en la materia.
- Poca conciencia a nivel directivo, principalmente en empresas medianas y chicas, quienes suelen relegar la inversión en Seguridad de la Información, anteponiendo otras prioridades que no necesariamente tienen que ver con la continuidad del negocio.
- Hace falta un mayor esfuerzo en promover el desarrollo tecnológico en el país. Tenemos en el mercado los últimos adelantos en cuanto a seguridad en informática, pero en el país este tipo de tecnología no se desarrolla.

Principales OBSERVACIONES
"México esta haciendo esfuerzos importantes por hacer más seguras las redes, sin embargo, no existe una cultura de seguridad enfocada de manera integral".
"Carecemos de estándares Nacionales que no proveen un marco de referencia, así como de un marco jurídico que dé fuerza legal a las iniciativas de seguridad".
"Se cuida la compra de equipo de cómputo, pero no se mira a la 'Seguridad de la Información' con suficiente énfasis, principalmente cuando se habla de infraestructura para redes, acceso a contenidos seguros, bases de datos seguras y a procesos de negocios".
"México se registra como uno de los países con infraestructuras más afectadas por código malicioso, así como el cuarto país generador de ataques a la infraestructura de Internet en la región".
"En el sector empresarial aún se percibe a la Seguridad Informática como un aspecto técnico operativo que no ocupa la agenda estratégica de la corporación".

Principales retos de México como país, en materia de Seguridad en Informática

Las respuestas codificadas de todos los entrevistados (quienes dieron, en la mayoría de los casos, más de una opinión cada uno), giraron alrededor de nueve rubros principalmente, como puede observarse en la Gráfica 9.

JFS



GRÁFICA 9

Los expertos coinciden en que uno de los principales retos está en la educación y concientización, abarcando a todos los niveles de las organizaciones, tanto estratégicos como tácticos y operativos. Consideran que una mayor conciencia al respecto, podría ayudar a convertir las cuestiones de seguridad en una prioridad a nivel empresarial y de las instituciones, lo cual permitiría planear mejor los presupuestos destinados a este rubro. También es necesario extender esta educación y colocar la tecnología de seguridad al alcance de toda la sociedad, en tanto que el uso de la tecnología en sí, está cada vez más generalizado; hay muchas más personas conectadas a Internet y todas ellas deben compartir una "responsabilidad informática", protegiendo sus equipos y, en consecuencia, la red.

Aparte de escalar la conciencia de la problemática a todos los niveles de de la organización, la cultura de seguridad tiene que ver con el establecimiento de reglas de seguridad que se incrementen y estandaricen, a nivel general de todo el país.

En materia de legislación, se percibe que no existen aún leyes "robustas" que permitan actuar adecuadamente ante cualquier evento de seguridad. El reto consiste en llegar a consolidar esas leyes, de tal forma que se puedan combatir los delitos cibernéticos y castigarlos de manera efectiva.

Hablando de planeación, un reto importante es la implantación de un adecuado equilibrio entre los tres elementos que componen todo sistema, incluyendo un sistema de seguridad informática, los cuales son las personas, los procesos y la tecnología. Óptimamente, pudiendo ser administrado en ambientes heterogéneos, con un balance adecuado entre seguridad y disponibilidad.

Por otro lado, dentro de un ambiente institucional o de empresa, es necesario desarrollar políticas internas que permitan que la seguridad no sea algo definido por cada sector o grupo de usuarios, sino a nivel de toda la organización.

Principales OBSERVACIONES
"En cuanto a soluciones de seguridad, es necesario que los usuarios conozcan qué se usa, cómo se usa y qué problemáticas resuelve".
"Para enfrentar el futuro, se necesita desarrollar gente más capacitada en materia de seguridad, gente capaz de comprender mejor los riesgos".
"De manera paralela, también se requiere fomentar una cultura de la legalidad".
"Hay que tener conciencia de que la seguridad se compone de personas, procedimientos y tecnología, y que si se considera cada uno de estos rubros por separado, la seguridad no es completa".
"Hace falta mostrar a las empresas el valor que tienen las inversiones en seguridad, como aportación al negocio, no sólo en cuanto a la cuestión económica de la inversión, sino también en cuanto tiempo, recursos humanos, etc."
"Es necesario adoptar una forma más ordenada y estructurada de enfrentar los retos de seguridad informática, ya que, aunque muchas organizaciones están tomando mejores prácticas y estándares como guías para la mejor implantación de la seguridad informática, otras organizaciones todavía están concentradas en resolver 'bomberazos'".
"A nivel dirección general debe llegar la importancia de la seguridad informática, no únicamente como un elemento de mitigación de riesgos, sino como un elemento que brinda ventajas competitivas, diferenciadores de mercado e incluso mejoras en los procesos de las organizaciones".
"Otro reto es pasar de una cultura reactiva y correctiva a una cultura proactiva y preventiva en materia de seguridad informática. México tiene mucho por hacer y el problema es la lentitud con la que actuamos. Sabemos lo que se tiene que hacer, pero algunos países tienen prisa y otros no. Hacemos cosas, pero no con urgencia. Corea, Vietnam, China, ellos sí tienen urgencia y es notoria la diferencia. Evidentemente, esto se refleja en la competitividad del país".

JFS

Principales retos de las organizaciones usuarias, en materia de Seguridad en Informática

De acuerdo a la opinión de los expertos entrevistados, los principales retos a enfrentar por las organizaciones usuarias en materia de Seguridad en Informática, tienen que ver, en primera instancia, con la educación, difusión y fomento de una conciencia alrededor del tema. También están identificados retos importantes en las áreas de Planeación, Presupuesto y Políticas Internas.

Los directivos deben comprender bien el fenómeno de la seguridad (si no lo ven, no lo creen) y al mismo tiempo hacerlo extensivo al resto de los empleados. En este sentido, el reto, además de capacitar al personal, es necesario responsabilizarlo e involucrarlo a través de mensajes repetitivos (campañas internas), ejemplos y una actitud corporativa en donde la seguridad esté integrada.

Los responsables de la implementación de mecanismos de seguridad dentro de la empresa, deben buscar soluciones consistentes y de largo plazo. Deben adoptar una forma más ordenada y estructurada de enfrentar los retos de seguridad informática, dando prioridad urgente a la creación y configuración de redes seguras, ya que todas las demás aplicaciones dependen de esto, de una infraestructura sólida y segura. .

Paralelamente con la actualización permanente de los sistemas, es necesario crear y comunicar políticas claras en torno a la seguridad de la información. Estas políticas deberían estar alineadas con el nivel de seguridad que específicamente requiere la organización y contemplar estándares, guías, procedimientos y definición de responsabilidades.

La mayoría de los entrevistados percibe que se subestiman los presupuestos asignados a esta área. Se debe trabajar en crear una mayor conciencia acerca del valor de la información y vislumbrar a la seguridad como una necesidad e invertir en ella en la proporción adecuada.

Se considera que las organizaciones, en general, deben ser más proactivas. Deben dejar la pasividad y realmente tomar acciones al respecto; tomar conciencia del problema y atender de forma preventiva y no sólo correctiva las vulnerabilidades.

Se habló también acerca de la profesionalización de proveedores y compradores e incluso hubo quien lo mencionó como "ataque a la corrupción" entre ambos.

Principales observaciones
"Se debe adoptar la seguridad como el conjunto de tecnología, procesos y personas, y no sólo como una solución antivirus y un firewall".
Entre otros retos de importancia, se mencionaron: "Dar mayor énfasis al cuidado y manejo de identidades". "Conjugar los elementos técnicos y acciones necesarias, a nivel interno". "Mantener sus infraestructuras tecnológicas actualizadas".

Principales retos de los proveedores de hardware, en materia de Seguridad en Informática

La mayoría de los entrevistados perciben que los proveedores (fabricantes y distribuidores) aún no incorporan el concepto de seguridad a las estrategias de sus productos y que siguen viendo las soluciones como partes aisladas, cuando debería ya de existir una conciencia de que la seguridad es parte integral en la operación de cualquier equipo. Estas empresas podrían, o bien integrar controles y dispositivos de seguridad a nivel de hardware y/o proveer alternativas integrales de seguridad junto con sus productos, preferentemente empleando estándares abiertos con el fin de facilitar la integración con el resto de la cadena de soluciones informáticas.

Otros retos a sortear por los proveedores de hardware están relacionados con el desarrollo tecnológico. Se considera que se deberían incluir mecanismos de seguridad más robustos en los productos, basados en las necesidades actuales y futuras de las organizaciones, en lo que se refiere a políticas de seguridad. Asimismo, desarrollar equipos que permitan la implantación de redes inteligentes, con mejor encripción, que además detecten comportamientos anormales de los usuarios y así poder reducir el riesgo.

También se dieron varias menciones en cuanto a que entre los principales retos, aparte de los que se acaban de describir, están los relacionados con:

- Educación / Capacitación a los usuarios

  Se refirieron tanto a la parte de capacitación, como a la difusión de los elementos de seguridad que se implementan con los sistemas, guías, mejores prácticas, etc.

- Precio

  Se habló de hacer los equipos y las soluciones de seguridad más accesibles para los usuarios, a través de mejores precios y esquemas financieros.

Principales observaciones
"Se debe entender la relación que existe entre soluciones de hardware, soluciones de software y seguridad, en donde la seguridad debe ser el primer círculo del esquema".
Entre otros retos de importancia, se mencionaron: "Generar soluciones de hardware que, además de auto administrables, sean actualizables de manera sencilla". "Buscar soluciones de seguridad que sean menos pesadas y no requieran tanto hardware adicional". "Crear centros de soporte tipo automóviles, para configurar e-tuning en los equipos". "Crear soluciones celulares y modulares, que funcionen entre sí". "Mejorar el servicio posventa". "Entender que el problema de la seguridad no se resuelve con sólo productos de Hardware; éstos nada más son un elemento de la solución".

JFS

Principales retos de los proveedores de software, en materia de Seguridad en Informática

La mayoría de las opiniones de los expertos, tratan acerca de que los principales retos de los proveedores de software, están en dos rubros principalmente: el propio desarrollo y tecnología incorporada en los programas aplicativos y sistemas operativos, así como la integración de mecanismos de seguridad dentro de los mismos.

Con respecto al desarrollo de software, se considera que deben fabricarse productos con niveles de vulnerabilidad cada vez más bajos, con autoprotecciones o formas de trabajo protegidas de antemano contra ataques o reproducciones, dando mayor énfasis en la encripción de los datos y soluciones relacionadas con las comunicaciones.

Otro reto en este mismo sentido, es buscar soluciones de seguridad que sean menos pesadas y no requieran tantos recursos de hardware.

En cuanto a la integración de la seguridad en sus productos, los entrevistados coinciden en que los desarrolladores de software deben configurar soluciones que ya incluyan la seguridad y no se dediquen a vender aplicaciones separadas. De hecho, el concepto de seguridad debería regir el desarrollo desde su conceptualización y durante todo el proceso.

Otro reto importante, es el de facilitar al usuario todo lo relacionado con seguridad. Por un lado, se trata de que el software ya incorpore la seguridad y que su uso y actualización sea cada vez más transparente y requiera menos la participación del usuario. Que el proceso de instalación de parches y actualizaciones sea más intuitivo y que su publicación se dé con mayor oportunidad.

A diferencia de la encuesta realizada en 2004, muy pocos hablaron acerca de la responsabilidad de educar al usuario o de estrategias de precio.

Principales observaciones

"El mayor reto al que se enfrenta un fabricante de software, es la complejidad del desarrollo de un sistema aplicativo u operativo, pues al tener una gran cantidad de código generado por equipos de varios ingenieros, los errores de programación facilitan que se incremente el impacto y cantidad de vulnerabilidades ubicadas en los mismos. Los proveedores, por tanto, deberían considerar colocar dentro de sus procesos de control de calidad mecanismos de certificación que permitan detectar problemas de seguridad, sin afectar la calidad aplicativa de los códigos programados".

Algunos de los retos específicos que fueron mencionados, son:
"Invertir recursos en investigación y desarrollo, con enfoque hacia la seguridad. Son el sector que más debe cuidar esto".
"Que los desarrolladores mexicanos integren mayores aspectos de seguridad, para tener la capacidad de competir a nivel internacional".
"Trabajar en simplificar y disminuir el esfuerzo de las empresas en mantener su infraestructura segura".
"Proveer soluciones informáticas viables de acuerdo a las necesidades del cliente, visto de manera individual desde la perspectiva de seguridad, sin considerar que una sola alternativa 'se acopla' a todas las empresas".
"Manejar y desarrollar esquemas de licenciamiento mucho más flexibles, con lo cual se permite a los usuarios poder acceder a las soluciones que, además de rentables, permitan la implantación de programas de seguridad informática, de acuerdo a las condiciones de cada organización".
"Combate a la piratería".
"Buscar una mayor integración de sus soluciones, no sólo entre sus propios productos, también con otros proveedores. Lo anterior normalmente se logra implantando estándares abiertos en sus productos y soluciones".

Principales retos de los integradores de soluciones, en materia de Seguridad en Informática

Son múltiples los retos mencionados por los expertos, que deben enfrentar los integradores. Los principales pueden clasificarse en los siguientes rubros generales:

- Incluir el aspecto de seguridad en todas sus propuestas tecnológicas.
- Brindar una verdadera asesoría, entendiendo las necesidades del cliente y optimizando sus presupuestos.
- Tener una mayor especialización en cuanto a soluciones tecnológicas y definirse mejor dentro de mercados verticales.
- Hacer mucho más énfasis en la capacitación de su personal, respecto de las innovaciones y soluciones tecnológicas que manejan.
- Promover más la estandarización y buscar la escalabilidad eficiente a futuro.
- Educar más y dar una mejor orientación a sus clientes.

Principales observaciones
"Integrar nuevas políticas o servicios de seguridad de manera transparente, que minimicen el impacto sobre los sistemas actuales y/o la operación del usuario".
"Convertirse en aliados tecnológicos tanto de los usuarios como de los proveedores, considerando la seguridad como un factor clave en la integración de soluciones".
"Seguir una metodología que permita desarrollar estrategias de mayor alcance, y que consideren al problema de seguridad como un todo, no como situaciones aisladas".
"Contar con los recursos necesarios para capacitar a su propio personal, en todo lo relacionado con las nuevas tecnologías, las cuales cambian y se renuevan a ritmos sumamente acelerados".
"Guiar a las empresas en soluciones adecuadas y de manera responsable, esto quiere decir, ni vender más de lo que se requiera ni vender tecnología solamente".
"Crear soluciones integradas y completas, orientadas al negocio de cada uno de sus clientes, buscando reducir los riesgos a un nivel aceptable".
"Seguir un marco de referencia basado en algún estándar o mejor práctica, para permitir entregar a los clientes un modelo basado en experiencia y con capacidad de manejar modelos de madurez, los cuales permiten implantar una solución de manera gradual".
"Buscar que las soluciones que propongan a sus clientes sean rentables con el fin de poder justificar de mejor manera una inversión acorde con cada organización".
"Avisar de los retos de seguridad a sus clientes y acercarles fuentes de información para que estén seguros".
"Mantener las soluciones de plataformas listas para crecer conforme lo vaya requiriendo el usuario".
"Manejo adecuado de gente y sistemas en conjunto, ya que son los que tienen una mayor responsabilidad en las implementaciones".
"Tener mejores alianzas y creatividad en soluciones de seguridad".
"Adecuar la operación con la colocación de los elementos necesarios para proporcionar una infraestructura flexible y resistente, que ayude incluso en el cumplimiento o adherencia a normatividades y estándares de Tecnologías de Información".
Entre otros retos de importancia, se mencionaron: "Certificaciones para los temas de seguridad que desean resolver". "Regirse bajo estándares de seguridad bien definidos". "Mantener las soluciones de plataformas estables". "Conocer cómo se debe integrar la seguridad, al combinar plataformas, evitando huecos".

Principales retos de las Instituciones Educativas mexicanas, en materia de Seguridad en Informática

A grandes rasgos, la mayoría de los retos mencionados por los entrevistados, están relacionados con la responsabilidad de las instituciones educativas por crear una cultura a nivel sociedad, difundir valores y conceptos de seguridad entre sus alumnos de todas las carreras, capacitar técnicamente a los alumnos de las carreras relacionadas con tecnología de la información y promover más la investigación sobre el tema a nivel interno, con enfoque hacia el desarrollo y transferencia de tecnología.

Otros comentarios hicieron referencia al mantenimiento y actualización de la infraestructura de cómputo y telecomunicaciones de las mismas instituciones, entre otras razones para garantizar a sus usuarios (maestros, alumnos y áreas administrativas), la seguridad en el manejo de su información.

JFS

Principales observaciones
"Incorporar prácticas de seguridad modernas y que contemplen la tecnología, procesos y personas, en sus carreras de infraestructura de cómputo y de desarrollo".
"Las carreras relacionadas a informática debiesen de colocar en su curricula, materias relacionadas con la seguridad, desde la programación hasta la infraestructura, buscando el mantenimiento de la confidencialidad, integridad y disponibilidad de la información".
"El desarrollo de recurso humano calificado en esta especialidad. Es patético llegar con gerentes que no saben".
"Integrar a sus planes de estudio no sólo los diferentes elementos teóricos de un sistema de seguridad informática, sino basar dicho conocimiento en los estándares y mejores prácticas que se emplean en el mercado en la actualidad y aquéllos que están siendo desarrollados para su implantación futura".
"Crear programas que permitan entender e interactuar con políticas de seguridad relacionadas al impacto de un ecosistema determinado (corporativos, educativos, etc.)".
"Educar a los usuarios en el uso de la información que se obtiene a través de la red y para usarla de manera segura".
"Integrar planes de generación de conciencia en lo referente a la seguridad informática, no únicamente en los planes de carreras relacionadas con la informática, sino en los planes de todas las carreras. Mejorará el nivel de conciencia de los usuarios en general, con lo que las implantaciones de estos esquemas serán mucho más fáciles".
"Dar énfasis en la educación sobre manejo de riesgos".
"Difundir y promover los temas de valores, ética, responsabilidad y el desarrollo de una cultura de seguridad de información, para que asimile cualquier usuario que esté conectado a Internet".
"Crear conciencia y educar a los alumnos no sólo técnicamente, sino en cuanto a los valores que conlleva la seguridad. De las escuelas, sale un gran número de *'hackers'* ".
"Fomentar una cultura de la legalidad y virtudes de la misma, con especial énfasis en la seguridad y valor de la información en una empresa, más allá de sólo sus implicaciones económicas en caso de riesgo".

Principales retos de los Medios de Comunicación, en materia de Seguridad en Informática

Los principales retos de los medios, están en función de su labor informativa. Se habló de su responsabilidad como agentes educadores y de fomento a la cultura, tanto a nivel de usuarios individuales como organizacionales.

En cuanto a la labor de difusión de contenido, se visualizaron diferentes vertientes en las que deberían poner énfasis los medios. Entre ellas:

- Difusión del tema de seguridad de la información, en general.
- Difusión de soluciones, incluyendo productos, evaluaciones, etc.
- Difusión de ejemplos y casos de éxito o de fracaso.
- Difusión más allá de los medios especializados, para llegar no sólo a los tecnólogos y los informáticos, sino a toda la sociedad, a través de un lenguaje accesible para todos.

Otro de los retos más importantes que fueron mencionados por varios de los entrevistados, es que para cumplir bien su función informativa, los medios deben documentarse bien. De otra manera no pueden ser un proveedor de información confiable.

Algunas otras opiniones se refirieron a la infraestructura de comunicación electrónica de los medios (sus sitios de comunicación "on line" con el público), los cuales deben cumplir con requerimientos específicos de seguridad para ,entre otras cosas, limitar la piratería de contenidos y dar certidumbre a sus usuarios.

Principales observaciones
"Enaltecer las bondades de la seguridad informática a nivel prevención, ejemplificando con las 'mejores prácticas' que han sido adoptadas por los grupos líderes que mantienen la vanguardia al respecto".
"Comunicar de modo balanceado las amenazas y las soluciones posibles a éstas, tanto de manera correctiva como preactiva".
"Mejorar la difusión de la seguridad informática como parte integral de cualquier operación realizada por medios electrónicos".
"Difundir la importancia que tiene la seguridad de la información y enfatizar que no sólo los grandes *'hackers'* pueden robar información confidencial, sino que existen muchas otras maneras conocidas como ingeniería social".

JFS

Principales retos del Gobierno de México, en materia de Seguridad en Informática

La mayoría de los expertos coincide en que hace falta una normatividad clara y efectiva. No existen leyes que permitan sancionar los delitos cibernéticos. El reto es crear, mantener y legislar sobre las políticas y reglas de seguridad, con el fin de hacer que el marco regulatorio para el uso de las mismas, permita el desarrollo de la seguridad de manera más fácil y, en caso de romper esquemas de seguridad regulados, defina sanciones que garanticen el cumplimiento de las leyes y políticas. Para lograrlo de la mejor manera, el Gobierno debería trabajar de manera conjunta con la misma industria.

Educar y promover una cultura de seguridad entre los trabajadores del mismo gobierno y hacia la sociedad en general, es otro de los retos mencionados.

Otros comentarios que tienen que ver con la infraestructura de las instituciones, permiten vislumbrar algunos retos de carácter presupuestal y otros relacionados con el combate a la corrupción, para que las propias instituciones lleven a cabo proyectos serios e impulsar un verdadero Gobierno Digital que pueda ofrecer mecanismos y servicios seguros, obteniendo al mismo tiempo la confianza de la ciudadanía.

La definición de estándares al interior del Gobierno, por su lado, jugará un papel fundamental en todo este proyecto de infraestructura y servicios al ciudadano. Se comentó que existen demasiadas iniciativas dispersas. "Algunos Municipios, por ejemplo, están haciendo sus propios proyectos sin considerar que no es necesario reinventar el hilo negro. Cuando existen miles de municipios, el gobierno podría establecer un estándar en materia de seguridad que haga que sea más fácil la implementación a lo largo del país. Lo mismo se podría decir de gobiernos estatales".

Principales observaciones
"Se debe buscar la creación de una conciencia informática en todos los niveles de la organización, estableciéndose sobre todo la normatividad en la materia, acorde a las tendencias mundiales de los países más tecnificados".
"Generar y liberar una adecuada legislación que regule y sancione las faltas o fallas en la confidencialidad, integridad y disponibilidad, que dé certidumbre a las organizaciones".
"Debería modificar los criterios de su proceso de compra. En una licitación, no se compra lo mejor, se compra lo barato. Y lo barato cuesta caro, es la historia que se sigue repitiendo en México. La Seguridad es algo que cuesta, pero luego tiene muchos beneficios a largo plazo; una licitación no considera esto en absoluto".
Entre otros retos, se mencionaron: "Señalar y condenar las actividades de piratería en nuestro país".

Aportaciones relacionadas con Seguridad en Informática, hechas por las empresas entrevistadas

3Com
Ignacio Leñero
Director General

"Desarrollo de la manera de obtener una estructura de seguridad para después montar hardware y aplicaciones sobre ella, y cómo hacerlo de manera segura, tanto interna como externa, desarrollando vacunas preventivas y no correctivas, con conceptos como cuarentenas parciales".

ALAPSI
Adrián Palma Castillo
Presidente

"La ALAPSI es la única asociación a nivel Latinoamérica que está totalmente relacionada con la seguridad informática, donde su misión es la difusión del conocimiento en seguridad informática y el integrador de todos los profesionales dedicados a la seguridad informática. Sus principales objetivos son :

"Promover la capacitación y adiestramiento en seguridad informática.
"Promover la cultura de seguridad informática a todos los niveles en las organizaciones y en la sociedad en general.
"Proponer políticas, normas y legislación en la materia.
"Ser la instancia de consulta de los gobiernos y organismos nacionales e internacionales.
"Difundir el código de ética de la Asociación.
"Proponer a la ley en vigor, los elementos necesarios para la preparación, calificación y acreditación de peritos en materia de seguridad informática, de acuerdo a las normas y estándares internacionales.
"Ser el organismo supervisor de la calidad del profesional en seguridad informática, en el campo y a nivel de certificaciones internacionales".

AMIPSI
Enrique Bustamante R.
Director General

"Creación de alianzas con las empresas y grupos más representativos de nuestro país, en torno al desarrollo, antipiratería y cadenas virtuosas y productivas de las tecnologías de información nacionales, tales como BSA, CONACYT, AMCIS, CANIETI, AMITI, amén de las autoridades respectivas como la Secretaría de Economía, Función Pública, E-Mexico, PFP, Profeco y Condusef, en pro del desarrollo nacional de nuestra industria".

AMITI
Javier Allard
Director General

"Difusión de información a los socios y trabajo en el Congreso, para la generación de iniciativas de Ley en combate a delitos cibernéticos".

Asiste
Moisés Polishuk
Director General

"Consultoría enfocada a las necesidades de cadenas productivas en un enfoque holístico".

Avaya
José Gómez Obregón
Director General

"Avaya, como líder en el área de Telefonía IP, ha demostrado un fuerte compromiso en el desarrollo de tecnología para la protección y confidencialidad de las telecomunicaciones. Una de las contribuciones es el desarrollo de una solución basada en H.235 (Seguridad y Encripción para H.323 y H.245), la cual se ha denominado Avaya Encryption Algorithm AEA2, lo que facilitó que nuestra empresa fuera de las primeras en adoptar el estándar AES como reemplazo de DES para proteger comunicaciones de Telefonía IP. A través de la plataforma

Communication Manager, Avaya ofrece una solución de IP Telephony segura, end-to-end, utilizando plataformas robustas integrando soluciones de encripción, así como algoritmos de autenticación.

"Las soluciones de Telefonía IP de Avaya incluyen encripción a todos los niveles, protegiendo de esta manera tanto la operación de la solución de Telefonía IP, como la comunicación que se lleva a cabo en ésta".

JFS

CANIETI

Rogelio Garza
Director General

"Como un organismo empresarial que agrupa a los principales actores involucrados, CANIETI constantemente organiza conferencias, cursos, talleres que fomentan el uso de la seguridad. Asimismo, se trabaja de manera estrecha con las autoridades, con el fin de promover un marco jurídico adecuado que propicie mejores prácticas de seguridad en informática".

Cibercorp

Gerardo Hernández
Director General

"Aun cuando ofrecemos soluciones puntuales y productos, buscamos dar a nuestros clientes una visión más amplia de solución, donde no sólo se instalen o incorporen elementos nuevos de control o protección, sino que se optimice lo hecho hasta ahora.

"También promovemos la ecuación hacia el cliente, para que busque proveedores que le permitan tener un aproximación sistemática a la solución".

Computer Associates

Rogelio Montekio
Gerente de Desarrollo de Negocios

"Computer Associates ofrece al mercado una práctica de seguridad que busca integrar diferentes soluciones, enfocadas en tres principales objetivos:

1) Administración de Amenazas: Dentro de esta solución contamos con los diferentes componentes necesarios para proteger y ayudar a un sistema a mitigar sus riesgos, enfocándonos particularmente en aquellas amenazas que son externas al mismo, tales como virus, spyware, hackers, código malicioso, etc.

2) Administración de Identidad y Control de Acceso. Complementando lo anterior, contamos con una solución que comprende la administración de la identidad y accesos de los usuarios, respondiendo a preguntas como ¿Quién eres?, ¿Qué puedes hacer? y ¿Qué se hizo dentro del sistema?. Se puede tener un control tan granular como se desee, que va desde aprovisionamiento (altas, bajas y cambios) de los usuarios con base en roles y funciones, hasta controlar quién, desde qué equipo y empleando qué programa, tiene un determinado nivel de acceso a nuestros equipos.

3) Administración de Información de Seguridad. Complementamos una visión global al integrar un sistema de centralización, correlación y filtrado de eventos, que no sólo nos permitirá determinar lo que está ocurriendo en nuestro ambiente, sino también podremos llevar esta información y presentarla en un portal a manera de "dashboard" o "Balance Score Card" de seguridad, el cual nos ayudará a medir impacto a negocio y presentar la información en tiempo prácticamente real, así como matizarla de acuerdo a quién solicite la información. Todo lo anterior integrando los productos de Computer Associates y de otros fabricantes de sistemas.

"La solución de CA para la protección de la información incluye la aplicación de respaldo BrightStor® ARCserve® Backup v11.1 y 10 copias de eTrust™ antivirus, junto con uno, dos o tres contratos de mantenimiento; de esta manera ofrecemos a las empresas una solución integral y completa que los ayudará a administrar de manera efectiva sus necesidades de defensa y protección para su información.

"Aunado a lo anterior, dentro de CA se cuenta con *consultores entrenados y certificados en las mejores prácticas, estándares y regulaciones, con el objetivo de poder apoyar a nuestros clientes y socios en implantaciones de ITIL / ISO 15000, BS7799 / ISO17799, CobIT, Cumplimiento con la Ley Sarbanes-Oxley, por mencionar algunos".*

DSS de México

Jesús Saucedo
Director General

"Simplemente, tenemos políticas claras y utilizamos la infraestructura y herramientas que consideramos necesarias para minimizar los riesgos".

Fundación Ealy Ortiz, A.C.

Enrique Bustamante Martínez
Director General

"En lo que corresponde a nuestro campo de acción, los estándares y parámetros que utilizamos son los que de alguna forma se utilizan como los óptimos para una empresa de este género y dimensión".

Grupo Vilsa

Luis Vidales
Director General

"Participación con organismos internacionales de seguridad y, específicamente, con la IAFCI (International Association of Financial Crimes Investigation).

"Vilsa invierte en capital humano, en tecnología de punta, intercambio internacional con nuevas tecnologías, seguridad y soluciones".

Insys

Antonio Quiñones • Vicepresidente
Raúl Rodríguez • Director de Desarrollo e Investigación

"Insys tiene *11 años en el nicho de la seguridad informática y ha evolucionado hacia una seguridad integral (Seguridad es protección de los activos). Para ello, desarrolla diferentes herramientas, con el propósito de integrar la solución segura como un todo:*

- *Soluciones basadas en tecnología, con gran orientación al servicio.*
- *Software totalmente mexicano, para Identity Management, User Provisioning y Administración, Autenticación, Autorización y Auditoría.*

En Insys damos mucho énfasis en la formación y certificación de industria, en el personal que trabaja con nosotros.

La prioridad número uno en Insys, es sacar al cliente de cualquier problema.

Intel México

Jorge Gómez Figueroa
Gerente de Desarrollo de Negocios, Sector Financiero

"En Intel hemos desarrollado varias iniciativas que *permiten que el desarrollo de políticas de seguridad sean más fáciles de administrar o desarrollar, así como de fácil integración a los sistemas actuales. Por ejemplo, XD (Executed Disable Bit), sin llegar a ser un Antivirus total, es una herramienta que detecta comportamientos "irregulares" en el manejo de memoria RAM, aislando el segmento corrupto; este comportamiento es típico en varios ataques de virus (Blaster). Otro elemento clave es iAMT (Intel Architecture Management Technology), la cual complementa la mayoría de los sistemas de administración de hardware, al almacenar los datos del equipo en una parte de la plataforma Intel".*

JFS

ITESM

Francisco Camargo
Director de Informática

"Formación de Recursos Humanos calificados:

- *Diplomado en Seguridad Informática* http://actualizacion.itesm.mx/proevent/jsp/publico/pddetalleprog.jsp?id=SEGUINFORCEM1_00705CEM_03

- *Especialización en Seguridad Informática en las carreras de Tecnologías de Información, en particular el Ingeniero en Tecnologías Computacionales.*
- *Especialización en Seguridad Informática en la Maestría en Ciencias Computacionales.*
- *Tesis doctorales en Seguridad Informática en el Doctorado en Ciencias Computacionales.*

Fomentar la Cultura de Seguridad en **http://www.cem.itesm.mx/di/seguridad/index.html**, *entre:*

- *Alumnos.*
- *Padres de Familia.*
- *Egresados.*
- *Profesores y Personal* Administrativo".

KIO Networks

José Fonseca
Director de Outsourcing

"En lo que respecta a la Seguridad de la Información, KIO tiene como premisas fundamentales que una solución integral de seguridad está compuesta por Gente, Procesos y Herramientas. Tomando en cuenta todos estos elementos, ha creado un complejo de centros de cómputo de última generación con estándares internacionales en seguridad y continuidad con 99.999% de disponibilidad, únicos en México y Latinoamérica. KIO ha realizado enormes inversiones en infraestructura de construcción de edificaciones seguras para centros de datos y espacios de oficina para recuperación y continuidad de negocios. Aunado a ello, KIO ha desarrollado una enorme base de capital humano especializado en servicios de administración, operación y soporte de tecnología de información y seguridad.

"Con la adopción de estándares y prácticas mundiales de servicios de tecnología, KIO es una corporación con altos niveles de automatización de sus procesos, para lo cual ha realizado millonarias inversiones en herramientas de monitoreo, diagnóstico, operación, soporte y mantenimiento, lo cual le ha ganado el reconocimiento y distinción con el Premio Nacional de Tecnología 2004.

"En el aspecto de la gente como hemos mencionado, KIO cuenta con personal con la experiencia profesional necesaria, certificada en las diferentes tecnologías de seguridad implementadas en el Centro de Datos, que garantizan la correcta administración de la Seguridad en la Información de todos nuestros clientes.

"En lo referente a la Administración de la Seguridad de la Información, KIO basa sus Procesos en Metodologías líderes en el manejo y la administración de seguridad de la información, como ITIL y ISO17799/BS7799:2002, las cuales garantizan la integridad y la seguridad de la información de nuestros clientes, a través del servicio Security & Networks Operations Centres.

"En la parte de herramientas KIO cuenta con la infraestructura necesaria para poder albergar gran cantidad de datos y, sobretodo, garantizar la confidencialidad, integridad y disponibilidad de la información de sus clientes; para lo cual se utilizan productos de fabricantes líderes en el mercado de Seguridad, los cuales, al complementarse, ayudan a ofrecer soluciones de seguridad integrales con componentes cada día más sofisticados y especializados.

"Los servicios de KIO Networks abarcan un amplio portafolio en el que nuestros clientes se benefician, gracias a un enfoque de servicios integrados bajo demanda, con los más altos estándares de seguridad, continuidad y disponibilidad"

Microsoft México

Felipe Lemaitre Carabias
Gerente de Seguridad Informática

"Para Microsoft la seguridad es la más grande prioridad y hemos estado invirtiendo fuertemente en este tema por los últimos tres años. Estas inversiones ya están rindiendo importantes frutos.

"Las inversiones han sido diversas, por ejemplo, este año han ascendido a 3 mil millones de dólares en investigación y desarrollo directamente relacionado con seguridad, se han liberado versiones más seguras de nuestro software como Windows 2003 y IIS6, se han reforzado otros productos como Windows XP con el Service Pack 2, se han desarrollado productos gratuitos para que las empresas se aseguren como SUS, WSUS, MBSA y otros. Se han desarrollado mejores prácticas y guías que permiten a las empresas y a los usuarios conocer e implementar tecnología, configuraciones, mejores prácticas, políticas, etc. Se ha trabajo con la industria en desarrollar leyes y estándares, así como con el gobierno en perseguir a los criminales informáticos.

"En México también hemos trabajo mucho al respecto, por ejemplo, junto con el Tec de Monterrey y otras reconocidas instituciones, hemos entrenado profundamente a más de 9,500 expertos informáticos en seguridad, hemos invertido también mas de $700,000 dólares en entrenar a miles de profesionales en seguridad y en desarrollo de código seguro. Hemos trabajado con ofertas proactivas con nuestros clientes y socios, enviado miles de kits de seguridad y cientos de assesments de seguridad, así como también hemos iniciado distintas campañas para informar a la población en general de los peligros y de las soluciones.

"Microsoft continuará comprometido con la seguridad y durante este año continuará liderando los esfuerzos por asegurar a las personas y a las empresas".

Opentec

Carl Rianhard
Presidente

"Opentec es asesor de varias soluciones como CRM, KM o Knowledge Management, y redes.

"Creemos que Opentec aporta muchísimo haciendo énfasis en el alcance de los proyectos considerando el elemento de seguridad. Por ejemplo, un proyecto de CRM que trata con una base de datos de clientes, tiene que ser segura al 100%, o sea, impenetrable!! Lo mismo con un proyecto de KM, nosotros apoyamos a nuestros clientes con material confidencial, con sus propios planes estratégicos, etc. Estos contenidos se tienen que proteger.

"Con respecto a infraestructura básica de un cliente que sea PYME, es muy importante que su red incluya todo, servidores, clientes, software, seguridad y todo integrado con procesos. Las PYMEs pierden mucho tiempo haciendo y rehaciendo. La baja en costos de computadoras y redes ahora permite a una PYME tener una infraestructura de clase mundial, como debe ser".

Oracle de México

Leopoldo Granados
Arquitecto de Soluciones

"Oracle está contribuyendo con la generación de soluciones que cubren las 4 A's, que son Autentificación, Autorización, Auditoría y Administración, en todas las capas de las aplicaciones, es decir, desde la interfaz del usuario final hasta donde se guarda la información. Oracle contribuye al hacer saber a los usuarios que la seguridad va más allá de los antivirus, firewalls y detectores de intrusos, también es necesario tener seguridad en donde se guarda la información".

JFS

Sun Microsystems de México

Alejandro Salud • Director de Mercadotecnia
Paulo Kalapis • Gerente de la Práctica de Software

"Educar y evangelizar.
Innovar en tecnología de seguridad en informática.
Desarrollo de estándares tecnológicos.
Contribución al software libre.
Ser pioneros en temas de administración de identidades.
Ofrecer al mercado sistemas operativos seguros".

Symantec de México

Gabriel Alvarado
Sr. Regional Director México, Centro América, Caribe & Chile

"*Symantec es la compañía líder en Seguridad Informática en el mundo y, por tanto, tiene la responsabilidad de guiar y crear nuevas tecnologías y procesos que permitan una simplificación de las tareas de seguridad a empresas, instituciones y usuarios finales.*

"Symantec sabe que la información es el motor de las empresas, por lo que es necesario que se pueda garantizar la seguridad y disponibilidad en todo momento en toda la empresa. Éste es el motivo por el que para Symantec la administración de la información debe ofrecer, de manera simultánea, una seguridad y una administración de primera clase para los recursos de red. El resultado es lo que nosotros llamamos Information Integrity. Se trata de un enfoque revolucionario para la administración de la información, creado para permitir que las empresas sigan funcionando y creciendo pase lo que pase.

"Este enfoque logra una interacción equilibrada entre mantener la información con el nivel de seguridad más elevado posible, al tiempo que se garantiza que la información sea fácilmente accesible para los usuarios y se pueda aprovechar al máximo su valor.

"Symantec combina tecnologías de seguridad, sistemas y almacenamiento líderes del mercado, con una oferta de servicios completa y exclusiva, para poder proporcionar la integridad de la información. Nuestro enfoque equilibrado, el cual se basa en tres factores muy importantes, permite optimizar el valor de la información.

"Primero, Symantec ayuda a comprender todo lo que se necesita saber acerca del entorno de información: el estado del hardware, software, datos y otros activos de red; las amenazas de seguridad procedentes de todo el mundo; problemas de cumplimiento clave en un ámbito interno y externo; y mucho más. Todo ello es un reflejo de los sólidos conocimientos adquiridos por el equipo de analistas con mayor experiencia del sector.

"En segundo lugar, Symantec ayuda a emprender las acciones necesarias para reforzar el entorno de información, de modo que pueda aprovechar al máximo las nuevas oportunidades que surjan en las compañías. Los sistemas vitales están actualizados, según los requisitos de cumplimiento, y se pueden restaurar. Los dispositivos, las aplicaciones y las redes, están protegidos frente a amenazas antes de que éstas se produzcan. Además, las nuevas tecnologías y procesos, desde dispositivos inalámbricos hasta sistemas de comercio electrónico, pueden integrarse con suma facilidad para poder ampliar las ventajas competitivas de cada empresa.

"Por último, Symantec ayuda a controlar los recursos informáticos para evitar interrupciones, reducir el tiempo de inactividad al máximo y ampliar las posibilidades. Desde la instalación hasta la corrección mediante revisiones, nuestro objetivo es poder garantizar la seguridad no sólo de la información, sino de todos los sistemas, de modo que las empresas puedan seguir funcionando y creciendo pase lo que pase".

IV. Conclusiones de la investigación

Panorama general

Los resultados de este estudio permiten observar y comparar contra el estudio realizado en 2004, la percepción que se tiene acerca de la Seguridad en Informática en las ciudades más importantes de México, desde las diferentes perspectivas que en conjunto nos acercan a la visión general del país en un momento dado. Este estudio permite conocer el momento que está viviendo la seguridad en informática en la percecpión de usuarios y expertos en la materia.

El estudio 2005 muestra que México sigue estando rezagado en lo referente a seguridad en informática, con prácticamente las mismas carencias y deficiencias en difusión, capacitación y fomento a la cultura de seguridad en informática, tanto a nivel organizacional como individual. Existe una clara percpción de que hace falta conciencia en los niveles directivos de las organizaciones, ya que en materia presupuestaria el punto de la seguridad no tiene la prioridad que requiere.

Al igual que en el 2004, la preocupación acerca de virus sigue encabezando la lista de amenazas. Asimismo, destaca el hecho de que, por primera vez, los encuestados están considerando los accesos inalámbricos como conceptos de riesgo, al tiempo que figuran términos como manejo de identidad, phishing y spyware/adware.

No es de extrañar, en consecuencia, que entre las medidas para proteger la información se ubique en primer lugar el antivirus, seguido por el que se lleve a cabo una mayor capacitación, en tercer lugar el manejo adecuado de contraseñas y en cuarto lugar la necesidad de implementación de políticas y controles de acceso más efectivos.

Un pequeño paso en la dirección correcta, es que aumentó el número de personas que quieren conocer más acerca de políticas y procedimientos de seguridad en informática, con respecto al 2004, aunque sigue siendo una proporción muy pequeña de la muestra total.

Un concepto que en general tuvo menor importancia para los respondentes, respecto del estudio de 2004, fue el software original como una cuestión relacionada con seguridad.

En la presente edición del estudio aparecen por primera vez conceptos como la preocupación por los accesos inalámbricos, la conectividad y el software deficiente, así como el phishing, el spyware y el adware, así como la educación para enfrentar a las Ingeniería Social, los cuales en el 2004 no se habían contemplado, o eran en proporciones tan pequeñas que quedaron clasificados bajo el rubro de "otros."

Coincidencias y diferencias entre el usuario "Informático" y el "No Informático"

Las diferencias entre "Informáticos" (directores, gerentes y jefes de sistemas, encargados de la adquisición e instalación de equipos y software de las empresas, etc.) y "No Informáticos" (ejecutivos de las áreas de administración, producción, ventas, mercadotecnia, operaciones, jurídica, etc.), en varios rubros, fueron similares a las que se detectaron en 2004. Es notorio que existen diferencias de percepción entre los dos grupos, sobre todo en lo que respecta a las medidas que deben tomarse para enfrentar problemas de seguridad. Por otra parte, las coincidencias en otros rubros fueron mayores que en 2004, lo cual puede indicar que la información acerca del tema de seguridad en TI no está siendo limitada únicamente a grupos que se dedican específicamente a la informática. De ser así, puede considerarse un aspecto positivo para el establecimiento de una cultura general de seguridad en informática.

Coincidencias

- Al igual que en el 2004 los virus representan la amenaza de mayor riesgo para ambos grupos, los cuales, además, continúan mostrando preocupación por "hackers".

JFS

- Es indudable que tanto "Informáticos" como "No Informáticos", consideran que hace falta mayor difusión e información por parte de los proveedores.
- Al igual que en 2004, los dos grupos perciben el "desconocimiento" como uno de los mayores riesgos contra la seguridad.
- Los dos grupos consideran de mucha importancia la integridad y confiabilidad de la información.
- Tanto Informáticos como No Informáticos, consideran que el software en general puede mejorar sus esquemas de seguridad y que los procesos de actualización podrían optimizarse
- Ambos grupos perciben que hace falta una mayor asesoría por parte de fabricantes y distribuidores.

Diferencias

A continuación se presentan las diferencias más sobresalientes entre la percepción de los usuarios "Informáticos" (directores, gerentes y jefes de sistemas, encargados de la adquisición e instalación de equipos y software de las empresas, etc.) y los "No Informáticos" (ejecutivos de las áreas de administración, producción, ventas, mercadotecnia, operaciones, jurídica, etc.):

Usuarios informáticos

- Perciben, en mayor proporción que los No Informáticos, el software deficiente, como un problema de seguridad.
- Para el grupo de los Informáticos, Seguridad en Informática tiene más que ver con la integridad y la confiabilidad de la información, que con la protección contra Virus.
- Al igual que en 2004, este grupo tiene mayor conciencia acerca de los daños que podrían ocasionar los agresores internos.
- Un rubro en el que ha crecido de manera importante el interés, comparativamente con el 2004, es el de manejo de identidad.
- Muestran un mayor interés en el Monitoreo de Sistemas.
- Muestran un mayor interés en el apoyo por especialistas mediante outsourcing.

Usuarios "No Informáticos"

- Se preocupan más por soluciones como antivirus y manejo de contraseñas.
- Consideran que la capacitación adecuada y las políticas e implementaciones específicas de controles de acceso, son soluciones importantes.
- No hicieron menciones sobre "disponibilidad de la información" como un concepto que les preocupe.
- Este grupo mostró un mayor interés en conocer más acerca de virus, así como sobre seguridad en informática en general..

Principales demandas por parte de los usuarios

Usuarios "No Informáticos"

En el grupo de los usuarios "No Informáticos", las principales demandas que manifestaron hacia los proveedores de tecnología, fueron:

- Información / más difusión
- Mejoras en el software / actualizaciones
- Mayor asesoría / consultoría
- Políticas razonables de precio
- Facilidad de uso de hardware y software
- Capacitación

Es importante notar que estas seis categorías, si bien cambian en sus porcentajes, siguen exactamente el mismo orden del 2004, lo cual quiere decir que la percepción de

los No Informáticos no ha cambiado en el sentido de lo que esperan de los proveedores de tecnología.

A los No Informáticos les interesa principalmente conocer más acerca de:

- Control de acceso de usuarios, hardware y software
- Más acerca de virus
- Seguridad en Informática en general
- Más acerca de "hackers"
- Seguridad en Internet
- Información de riesgos y soluciones para PyME

Aunque esta lista no es exactamente igual, en orden, que en el 2004, es muy similar, lo cual indica que los No Informáticos buscan prácticamente la misma información que hace un año; este hecho podría indicar que no han obtenido esta información o que no ha sido suficiente.

Usuarios Informáticos

Para los usuarios "Informáticos", lo que hace falta por parte de los proveedores de TI, fue, principalmente:

- Información / más difusión (en primer lugar, igual que en 2004)
- Mejor integración de productos y soluciones
- Mejoras en el software / actualizaciones
- Mayor asesoría / consultoría
- Soluciones ad-hoc para cada empresa
- Mejores soluciones contra "hackers"

Aunque con un número muy pequeño de respondentes, es interesante recalcar que aparece por primera vez en este estudio, y en este grupo, la exigencia a los proveedores de tener mayor honestidad.

En cuanto a las necesidades más importantes de conocimiento acerca de Seguridad en Informática, este grupo expresó que le interesaban principalmente los siguientes temas:

- Control de acceso de usuarios, hardware y software
- Más acerca de "hackers"
- Seguridad en Internet
- Seguridad en Comercio Electrónico
- Tecnología Inalámbrica
- Monitoreo y administración de redes
- Seguridad en telecomunicaciones

Aquí aparecen dos temas muy específicos que no tenían este nivel de importancia en 2004: Seguridad en Comercio Electrónico y Tecnología Inalámbrica. Es evidente que los informáticos están viendo el desarrollo acelerado de estas tecnologías y que están conscientes de los riesgos de seguridad que pueden implicar, pero que no están obteniendo suficiente información confiable al respecto.

Principales retos de las entidades organizadas de México

En materia de retos, México enfrenta muchos. Según muestra el estudio, algunos de ellos son: promover la educación y el desarrollo de una mayor conciencia de seguridad a todos los niveles; combatir el letargo histórico para realizar las acciones (y pasar a una cultura proactiva y preventiva, en vez de reactiva y correctiva); contar con una legislación expedita; crear estándares a nivel nacional; trabajar en una difusión mayor y más objetiva; crear e implementar políticas claras y bien diseñadas; ofrecer productos integrales que contemplen a la seguridad como un elemento implícito, y contar con una mayor capacitación y especialización por parte de los participantes de este nicho en general (proveedores de tecnología, consultores e integradores).

A continuación se presentan los principales retos que deben enfrentar las organizaciones en México, de acuerdo a la opinión de los expertos y proveedores del gremio:

Entidad	Principales retos
Organizaciones usuarias	• Educación, difusión y fomento de una conciencia alrededor del tema. • Promoción de una mayor conciencia entre los niveles directivos, haciéndola extensiva a los empleados. • Búsqueda de soluciones consistentes y de largo plazo. • Creación y comunicación de políticas claras en torno a la seguridad de la información. • Asignación correcta de presupuestos.
Proveedores de hardware	• Integrar controles y dispositivos de seguridad a nivel de hardware y/o proveer alternativas integrales de seguridad junto con sus productos. • Incluir mecanismos de seguridad más robustos en los productos. • Proporcionar educación / capacitación a los usuarios. • Hacer los equipos y las soluciones de seguridad más accesibles para los usuarios, a través de mejores precios y esquemas financieros.
Proveedores de software	• Fabricar productos con niveles de vulnerabilidad cada vez más bajos. • Enfatizar la encripción de datos y las soluciones relacionadas con las comunicaciones. • Buscar soluciones de seguridad que sean menos pesadas y no requieran tantos recursos de hardware. • Configurar soluciones que ya incluyan la seguridad. • Facilitar al usuario todo lo relacionado con seguridad (mejorar actualizaciones y el proceso de obtenerlas).
Integradores de soluciones	• Incluir el aspecto de seguridad en todas sus propuestas tecnológicas. • Brindar una verdadera asesoría. • Tener una mayor especialización en cuanto a soluciones tecnológicas. • Hacer mucho más énfasis en la capacitación de su personal. • Promover más la estandarización. • Educar más y dar una mejor orientación a sus clientes.
Instituciones educativas	• Crear una cultura a nivel sociedad. • Difundir valores y conceptos de seguridad entre sus alumnos de todas las carreras. • Capacitar técnicamente a los alumnos de las carreras relacionadas con tecnología de la información. • Promover más la investigación sobre el tema a nivel interno.
Medios de comunicación	• Fomentar la cultura de seguridad en informática. • Difusión de soluciones. • Difusión de ejemplos y casos de éxito o de fracaso. • Difusión más allá de los medios especializados, para llegar no sólo a los tecnólogos y los informáticos, sino a toda la sociedad, a través de un lenguaje accesible para todos.
Gobierno	• Crear una normatividad clara y efectiva. • Crear leyes que permitan sancionar los delitos cibernéticos. • Trabajar de manera conjunta con la industria. • Educar y promover una cultura de seguridad entre los trabajadores del mismo gobierno y hacia la sociedad en general.

Áreas de oportunidad para la industria TI

1. Aún más que en el 2004, es clara la ventaja competitiva que tendrán aquellos proveedores de servicios o productos que proporcionen verdadera asesoría a sus clientes, en materia de seguridad en informática. Si los proveedores de soluciones facilitan información de diversas fuentes a las empresas, la lealtad de sus clientes podría verse incrementada, ya que si bien en un inicio esta estrategia se percibiría como un valor agregado, pronto se convertirá en un requisito indispensable al momento de seleccionar un proveedor.

2. Las empresas que ofrezcan productos y servicios que no sólo sean altamente seguros, sino que convivan con otros productos o servicios, sin provocar puntos de falla en seguridad, también tendrán enormes ventajas sobre su competencia.

3. Todo esfuerzo de Difusión y Capacitación será de beneficio para usuarios, y no deben dejarse únicamente a las instituciones educativas. Ideas creativas de cómo ayudar a los usuarios a conocer más, de maneras ágiles e interesantes, provocarán no sólo una mayor cultura de seguridad en informática en el país, sino un mercado más maduro, beneficiando a toda la industria en general.

4. Se ve, aún más claro que en el estudio del 2004, la ventaja que tendrán aquellas empresas que se alíen con otras para presentar soluciones completas al cliente, desde el dimensionamiento y la integración del proyecto, hasta la capacitación final al cliente, considerando a la seguridad como un elemento indispensable en cada uno de los pasos que se lleven a cabo, en cada producto y servicio que se incorpore al proyecto.

5. Una cercana colaboración con los organismos gubernamentales, las instituciones educativas y los medios masivos de comunicación, lograrán que la seguridad en informática se desmitifique y se vuelva parte de la vida cotidiana de los usuarios. A medida que esta participación se incremente, el país conseguirá una ventaja competitiva frente a otros que tienen mayor rezago en esta área, lo cual representa beneficios tangibles cuando se trata de inversionistas o socios comerciales.

Se reitera, finalmente, lo que se expresó en el Estudio de Percepción de Seguridad México 2004: Éstas son sólo algunas de las áreas de oportunidad de negocio que podrían desprenderse de los resultados de este estudio, y, en su caso, de su comparación con los resultados de hace un año. Cada lector, cada empresario, podrá tener, a través de la visión particular de su mercado y de su negocio, una gama de múltiples opciones para incrementar su participación en este esfuerzo por colocar a México en un alto nivel en materia de Seguridad en Informática.

V. Artículos sobre Seguridad en Informática

¿Por qué las organizaciones deben tener una Arquitectura de Seguridad de la información?

Por Adrián Palma
Presidente de la ALAPSI

JFS

Las organizaciones requieren hoy día garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información que manejan y procesan para brindar una operación segura y confiable a sus clientes y socios de negocio, así como la protección de sus activos tecnológicos. Pero ¿cómo se puede lograr esto? ¿Por dónde empezar? ¿Qué se necesita? La respuesta es una solución basada en una Arquitectura de Seguridad de la Información, la cual permitirá identificar los elementos y los componentes necesarios para definir, normar, implantar, monitorear y auditar los requerimientos de seguridad, con una visión de negocios apoyada en 3 factores críticos de éxito: recursos humanos, procesos de negocio y tecnología. Nótese la diferencia entre una arquitectura de seguridad de la información y una arquitectura de infraestructura de seguridad, donde ésta es diseñada con elementos tecnológicos exclusivamente y no con elementos que involucren a toda la organización.

En las organizaciones todo cambia con el tiempo: las personas, la tecnología, la forma de hacer negocio, los procesos, los volúmenes de información, los riesgos etc., por lo tanto las necesidades y requerimientos de seguridad también cambian. Esta situación hace extremadamente complejo el determinar el nivel de seguridad requerido para tratar de mitigar los nuevos riesgos, por lo que es fundamental contar con una arquitectura de seguridad cuyo objetivo principal sea el tener una base en la que los nuevos riesgos generados por cualquier tipo de cambio se incluyan en la arquitectura de seguridad y estén alineados bajo este marco, de forma que este proceso sea lo más transparente y sencillo para la organización.

Algunas de las etapas que se deben considerar en una arquitectura, son:

-Análisis de Vulnerabilidades y Evaluación de Controles
-Corrección de Vulnerabilidades
-Desarrollo de Políticas, Estándares, Guías, Procedimientos y Baselines
-Creación de la Función Informática
-Análisis y Evaluación de Riesgos
-Estrategia de Seguridad
-Programa de Concientización
-Adquisición, Desarrollo e Instalación y Puesta a Punto de herramientas
-Monitoreo, Auditoría y Cómputo Forense.

Ver figura 1. Ejemplo de Road Map

Las instituciones y organizaciones, al contar con una Arquitectura de Seguridad de la Información diseñada a su medida y basada en sus propios riesgos tecnológicos que impactan directamente a sus procesos de negocio o funcionales, le permitirá conocer el difícil, complejo y misterioso punto de equilibrio, entre el riesgo, el costo y la seguridad que necesita ser implantada, sin que estas medidas afecten la capacidad de operación y de servicio de la organización, además de las ventajas competitivas que nos brinda la tecnología.

Figura 1. Road Map

El tener una arquitectura de seguridad también garantiza que se tendrán todos los elementos necesarios para una adecuada administración de riesgos tecnológicos (Tolerar, Transferir, Mitigar o en algunos casos Evitar) y se podrá ser preciso en la identificación e implementación de los controles y mecanismos de seguridad que realmente requiere la organización y así evitar inversiones cuantiosas e innecesarias.

Las organizaciones que tengan la convicción real y la visión, lograrán un liderazgo en su ramo como pioneros en la definición e implantación de una Arquitectura de Seguridad de la información y contarán con estándares y lineamientos de seguridad que les permitan responder de manera preventiva y proactiva ante cualquier intento de ataque, evento, incidente o fraude, que ponga en peligro la operación, el servicio o la información sensitiva y crítica de la organización. Y en caso de que este tipo de intentos llegasen a materializarse, podrán estar seguros de que no impactarán de manera significativa; recordemos que no hay ningún mecanismo 100% seguro y que en algún momento las organizaciones siempre se enfrentaran con un incidente de seguridad. La diferencia versará en que ese incidente no afectará la capacidad de operación, servicio y, en algunos casos, la supervivencia de las organizaciones.

Como resultado de lo anterior, cualquier organización que siga este modelo será capaz de operar de forma preventiva y no reactiva, asegurando la disminución de pérdidas ocasionadas por la materialización de los riesgos tecnológicos, a su vez se estará preparado para recibir y aprobar cualquier tipo de auditoría o revisión en materia de seguridad de la información, así como obtener cualquier tipo de certificación internacional. Finalmente, lo más importante, la Alta Dirección tendrá la tranquilidad de que la organización o institución se encontrará operando de manera segura y confiable.

¿Sueño o realidad? La verdad es que el diseño y desarrollo de arquitecturas de seguridad de la información es toda una realidad en México; existen organizaciones que han llevado a cabo este tipo de proyectos y ¿el resultado?..... ha sido todo un sueño. ■

Identity & Access Management

Por Jorge Plascencia
Gerente de Desarrollo de Negocios Seguridad de Computer Associates

JFS

Al día de hoy las organizaciones enfrentan grandes retos y situaciones sin precedentes; consideremos la convergencia de información en los sistemas electrónicos que podemos encontrar en una organización de cualquier tamaño. Sin importar si somos un gran corporativo o una empresa en crecimiento, todos tenemos información vital para nuestra operación y supervivencia.

Cada día es más común escuchar noticias sobre el robo de información confidencial o vital para una empresa y, lamentablemente, este evento coloca a la organización en una posición de la cual no siempre es posible sobrevivir.

Así también la necesidad de mejorar nuestros procesos operativos, incrementar nuestra eficiencia y reducir nuestros costos, son actividades que siguen teniendo relevancia diaria en la toma de decisiones, tanto tecnológicas como empresariales. Consideremos los procesos de soporte técnico o mesas de ayuda a usuarios, que si bien son parte de una mejor práctica, como ITIL (Information Technology Infrastructure Library), pueden ser un cuello de botella, ya que cada vez que uno de nuestros clientes (usuarios) olvidan su contraseña, bloquean su cuenta o desean algún tipo de servicio relacionado a su contraseña y/o identidad, tienen que contactar a nuestra mesa de ayuda. Esto genera costos y falta de productividad que afecta a toda la organización.

Otro factor a considerar dentro de la organización es el cumplimiento de estándares y mejores prácticas. Si bien la ley Sarbanes Oxley ha causado mucho revuelo entre las empresas y organizaciones en general, cabe mencionar que existen muchas otras regulaciones y mejores prácticas que algunas organizaciones están adoptando. Consideremos el estándar de seguridad BS7799, el cual es el estándar más reconocido en seguridad a nivel mundial. Este estándar comprende varios dominios de la seguridad conteniendo un número significativo de requerimientos de control, lo que lo hace uno de los principales estándares de seguridad para las organizaciones al día de hoy.

El cumplir con un determinado estándar no es una tarea trivial, aun para las organizaciones más determinadas. Consideremos por ejemplo una práctica que es considerada por varios estándares, entre ellos la Ley Sarbanes Oxley, el BS7799, el ISO17799, HIPPA, entre otros; nos referimos a la Segregación de Funciones, la cual, de manera general, indica que una misma persona no puede ser juez y parte en una misma función o tarea. Por ejemplo, un administrador de una aplicación no puede ser el auditor de su trabajo. El reto que esto trae a las organizaciones es interesante, ya que los sistemas distribuidos como UNIX, LINUX o Windows, están diseñados bajo esta premisa y tienen "SUPER USUARIOS", los cuales no pueden ser controlados o restringidos en sus funciones y capacidades dentro del sistema, lo cual viola de manera directa la segregación de funciones.

Por lo anterior, Computer Associates ha liberado una "Suite" de productos orientados a apoyar a las organizaciones en un adecuado control de Identidad y Acceso. Esta "suite" de productos permite a las organizaciones:

- Automatizar el aprovisionamiento de usuarios, es decir, automatizar el proceso de creación, modificación y eliminación de usuarios dentro de nuestros sistemas y aplicaciones, con base en roles y funciones de negocio.

- Controlar el acceso a información crítica o vital para la organización, incluyendo la capacidad de controlar no sólo el tipo de acceso y quién tiene acceso a la información, sino incluso tener la posibilidad de determinar con qué programa o aplicación se accede a un dato en el sistema. Así también permite a las organizaciones definir políticas y reglas de acceso de negocio y llevarlas a la práctica de una manera más fácil y sencilla.

Con lo anterior las organizaciones pueden hablar de seguridad pro-activa. Ya no será necesario esperar a que se presente un ataque para identificarlo y tomar

acciones; con esta herramienta es perfectamente posible el determinar una regla de acceso a datos y sistemas, la cual se mantendrá, incluso en los casos de ataques de "hackers" que hayan logrado tener acceso a una cuenta de un SUPER USUARIO.

Otra gran capacidad que tendrán las organizaciones al emplear la suite de "Identity & Access Management" de Computer Associates, es el uso de una herramienta de Single Sign-On, la cual nos permitirá integrar un solo usuario y contraseña o bien el uso de tecnología biométrica, si es necesario, ante el usuario; y en realidad mantener usuarios y contraseñas más robustos y complicados ante nuestras aplicaciones y sistemas. Con esto se simplifica la vida de nuestros clientes (usuarios), y se robustece nuestra seguridad.

Así pues, Computer Associates pone a disposición del mercado mexicano esta suite de control de acceso e identidad, la cual puede ayudar a cualquier organización a bajar costos, incrementar productividad y mejorar sus sistemas de seguridad, incluso al grado de lograr el cumplimiento de estándares, regulaciones y mejores prácticas. ■

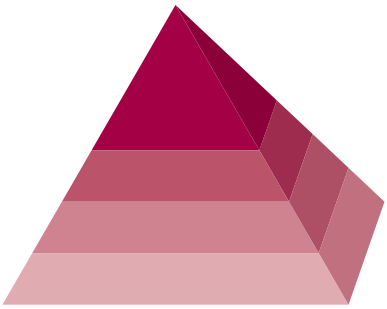
Seguridad integral de la información

Por José Fonseca
Director de Outsourcing de KIO Networks

JFS

Cuando se trata del cuidado de la seguridad, confidencialidad, disponibilidad e integridad de nuestra información, tanto en forma individual como institucional, siempre tratamos de balancear entre algunos dilemas: qué tanto nos protegemos, cuánto nos impacta el no protegernos adecuadamente, cuánto nos cuesta protegernos, cómo nos mantenemos actualizados permanentemente y qué tan completos son nuestros mecanismos que permitan preservar la seguridad, disponibilidad y confidencialidad de nuestra información.

Un buen comienzo para resolver tales dilemas, es el clasificar los activos de información por su nivel de criticidad para aplicar distintas medidas, grados de protección y niveles de gasto, acordes con el valor de lo que se desea proteger:



En un siguiente nivel de análisis podemos identificar las diversas clases de riesgo a las que estamos sometidos y las probabilidades y frecuencia de que un evento nos ocurra:

Intrusiones. Aunque no existe una clasificación única de problemas posibles y acciones de solución, es posible utilizar alguna de las más comunes:

Problemas: Daños, Incidentes, Amenazas y riesgos.

Soluciones de defensa: Prevención, Detección, Reacción y Adaptación, contra cada uno de los problemas.

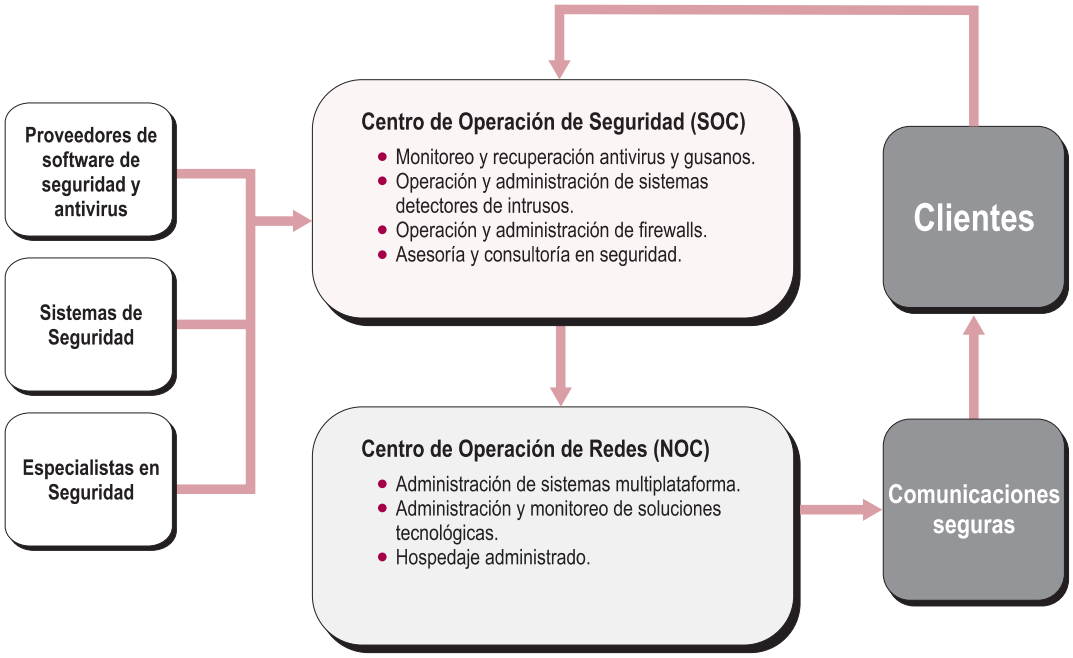
Como resultado podemos formar una matriz de combinaciones sobre problemas y soluciones de defensa y criticidades, para conocer nuestro mapa de vulnerabilidades y de ahí generar las acciones de respuesta que pueden ser de diversos tipos, entre preventivas y correctivas:

- Detección y Prevención de Intrusos
- Protección de Vulnerabilidades
- Respuesta Acelerada a Incidentes Detectados
- Filtrado de Contenidos
- Prevención y Corrección Anti-Virus
- Negación de Servicio
- Autenticación de Usuarios
- Administración y Recuperación de Claves de Acceso
- Recuperación de Datos

Resolver el dilema de la seguridad puede resultar un problema complejo, de múltiples variables y diversas categorías, cuya resolución puede requerir de varios componentes integrados que trabajen orquestadamente para lograr resolverlo de manera total.

Por otro lado es importante mencionar que siempre es mejor, más barato y con menor riesgo e impacto a una institución, el prevenir que resolver un tema de seguridad. Por lo anterior, es importante que la solución de seguridad ponga mucho más énfasis en la detección de eventos por medio de alertas y acciones de prevención preactivas. Para lograr esto, los diversos componentes y herramientas de seguridad pueden sofisticarse a tal grado en que los eventos se correlacionan en relaciones complejas para anticipar de forma cada vez más inteligente a una posible falla.

También es necesario incorporar una infraestructura segura para albergar las herramientas y componentes de seguridad mismos. Los modelos más avanzados contemplan la existencia de centros de operación de seguridad SOC y centros de operación de redes NOC, los cuales se abastecen permanentemente con información de los eventos e incidentes de seguridad que están siendo detectados en el sistema y con los nuevos componentes, elementos tecnológicos y procesos que van apareciendo por parte de proveedores y especialistas, para robustecer la seguridad en forma continua:



Finalmente expresaremos que los sistemas de seguridad deben observar algunas características que es preciso destacar:

1. Monitoreo específico y especializado por cada dispositivo
2. Detección y análisis de eventos
3. Respuesta preventiva a alertamientos detectados
4. Existencia de herramientas multi-dispositivo
5. Capacidades de análisis en profundidad y respuesta en tiempo real
6. Capacidad de minería de datos, inteligencia y correlación de eventos

Los sistemas de seguridad lógica han llegado a ser tan complejos y requerir enormes necesidades de inversión, que en muchos casos es conveniente adquirir servicios tercerizados de seguridad para que un solo centro de seguridad integral administrada, pueda atender a múltiples clientes y lograr una máxima eficiencia y economías de escala en esta vital actividad. ■

El robo de identidad puede ser un problema de seguridad nacional

Por Luis Raúl Vidales Sánchez
CEO de Grupo Vilsa

JFS

Los delincuentes de nuestro tiempo ya no son una caricatura. No son los chicos malos con antifaz y cachiporra escondidos en una casucha. El crimen organizado tiene a su disposición tecnología, información, redes internacionales y, peor aún, cómplices por doquier.

Hoy día, sus objetivos van más allá del dinero en efectivo, las carteras o los autos. Ahora roban identidades: clonan tarjetas, hurtan información, vulneran a las instituciones. En ciertos casos pueden ser incluso la puerta de entrada, o más aún, al financiamiento del terrorismo.

Eso es lo peor de este tipo de delitos: además de las pérdidas de cientos de millones de pesos que provocan a nuestros bancos y empresas, ponen en riesgo nuestra integridad como nación. Estamos hablando de la seguridad nacional.

No es una exageración. Lamentablemente, los ejemplos ahí están, como lo que según los medios de información ocurrió con aquella empresa denominada Choice Point, la cual, según éstos, literalmente entregó la base de datos de nuestros electores a gente de otra nación.

Por eso la información financiera, las bases de datos de una institución privada o de gobierno y los sistemas de identidad, no deben ser puestos en manos de inexpertos, arribistas o mercenarios disfrazados de empresarios o funcionarios.

El mal uso de estos datos impacta en la pérdida del patrimonio económico del trabajador más humilde o en situaciones de seguridad nacional, como la capacidad del Gobierno para operar sus programas de salud o asistencia pública.

Todas las identificaciones emitidas por una entidad del Gobierno, como licencias de conducir, tarjetas de seguro social, tarjetas de programas sociales, permisos para portar armas y credenciales para identificación, deben forzosamente garantizar una alta seguridad, durabilidad y cumplir con su función de manera expedita.

Grupo Vilsa ofrece la más alta tecnología y seguridad para cualquier tipo de programa Institucional, elementos de seguridad que arrancan desde el proceso de fabricación y personalización de cualquier tipo de identificación.

Nuestras soluciones pueden incluir, en una tarjeta, diversos elementos como: Fotografía a todo color, Firmas Digitalizadas, Huella digital, Códigos de Barra Bidimensionales, Laminado de larga duración Duragard Holográfico, Codificación en la Banda Magnética y Tarjetas Inteligentes de Contacto o sin contacto y Kinegramas ®.

Todos estos elementos permiten crear documentos altamente seguros, garantizando la credibilidad, privacidad de la información y, por supuesto, calidad en el servicio. Todos nuestros sistemas cuentan con una plataforma abierta, lo cual los convierte en una herramienta adaptable a las necesidades de cada proyecto, integrando diversas plataformas y manteniéndolos a la vanguardia tecnológica.

Grupo Vilsa sabe de esto. Después de 23 años de atender las necesidades más importantes en la materia, tanto en el terreno privado como gubernamental, nos dan la autoridad moral para afrontar cualquier reto. Sea cual sea su magnitud y dimensión.

No es casualidad que **Grupo Vilsa** haya participado en diversos eventos de carácter internacional, entre los que destacan las principales reuniones cumbres celebradas en México en el último lustro.

Basta revisar algunos ejemplos: la XI Conferencia de Esposas de Jefes de Estado y de Gobierno de las Américas celebrada en la Ciudad de México y la X Reunión de los líderes de la Asia-Pacific Economic Cooperation (APEC) en Los Cabos, en 2002; la Convención de las Naciones Unidas contra la Corrupción, en Mérida y la V Cumbre de la Organización Mundial de Comercio (OMC) en Cancún, en 2003. La Cumbre Extraordinaria de las Américas en Monterrey y la Tercera Cumbre América Latina y El Caribe -Unión Europea (ALCUE) desarrollada en Guadalajara en 2004.

Grupo Vilsa se ocupó de garantizar la seguridad en los accesos y en el manejo de los datos de los participantes, utilizando para ello tecnología de vanguardia, que en muchos casos, ha sido desarrollada en nuestro propio país y cuyas aplicaciones están disponibles para nuestros clientes.

Quizá por eso las distintas instituciones bancarias de nuestro país confían en **Grupo Vilsa**. Igual ocurre con las grandes firmas comerciales y con no pocos programas gubernamentales federales y estatales que demandan confiabilidad, seguridad y eficiencia. E igual confían pequeños y medianos usuarios que basan su éxito en los sistemas que ofrecemos. Ésa es la diferencia que ofrecen a sus clientes: la garantía de seguridad en el manejo de sistemas de identidad.

En el mejor de los sentidos, somos su mejor arma para enfrentar al crimen organizado.

Participamos activamente en Grupos de Combate a Ilícitos, con el apoyo de Organizaciones Internacionales como IAFCI (International Association of Financial Crimes Investigators), de la cual formamos parte.

Para derrotarlos, las autoridades y la iniciativa privada necesitan aliados de capacidad y honestidad comprobada y, evidentemente, equipados con recursos tecnológicos de vanguardia. Ese aliado es Grupo Vilsa. No importa si hablamos de la seguridad de su patrimonio o de la seguridad nacional. Permítanos ayudarle. Para eso estamos y estamos listos. ■

Tips para instalar una red inalámbrica

Sumario de un artículo producido por IT@Intel, proporcionado por Oscar Badillo
***Business Marketing Manager*, Mexico and Nothern Cone, Intel**

JFS

Tratándose de la operación de una red, nunca se puede estar suficientemente seguro. La organización de Intel invierte miles de horas cada año para redefinir sus procesos y políticas de uso, instalando las últimas tecnologías y administrando el ambiente de la red. Con la migración hacia una red inalámbrica, la necesidad por la dedicación crece aún más. A continuación hay algunas cosas que los gerentes de IT deben tener en cuenta cuando trabajen con una red inalámbrica:

- **Busque y asigne a los expertos**: La seguridad es una disciplina muy específica que requiere un conocimiento profundo y mucha experiencia. Considere la creación de una disciplina de IT dedicada únicamente a asuntos de seguridad; así, todos los esfuerzos se pueden acceder con una revisión amplia.

- **Pruebas, pruebas, pruebas**: Las compañías deben considerar que sus implementaciones de seguridad de redes y políticas de uso sean revisadas y probadas por consultores externos. Si no se tiene un experto dentro de la organización, ésta podría ser la medida más efectiva para encontrar defectos que pudieran invitar a una intromisión.

- **Respete el ambiente inalámbrico**: Por definición, las redes inalámbricas se enfrentan a altos niveles de amenaza de intrusión no autorizada, cualquiera con una antena puede potencialmente tomar parte del tráfico de la red, potencialmente desde muchos kilómetros de distancia. Sus políticas de seguridad e instalaciones deben tomar en consideración esta amenaza.

- **Busque la manera de estandarizar**: Uno de los atractivos de WEP, es que ofrece un común denominador para proteger redes 802.11b, no importando el fabricante de los dispositivos. VPN aún es un poco complicado, pero las compañías pueden suavizar la transición al estandarizar en un simple proveedor cuando esto sea posible. El incremento de seguridad de un VPN probablemente justifica su costo en las organizaciones grandes.

- **No sea descuidado**: Encriptación no hace mucho para proteger la información si los "hackers" pueden determinar sus llaves; de la misma manera, VPN no será exitosa si los atacantes pueden tener acceso a los clientes con acceso a la red, tales como las PCs de casa de un empleado, y usarlas para entrar a la red. Refuerce sus instalaciones con una amplia educación y entrenamiento a los empleados en relación al uso y manejo de passwords y PCs

- **Sea capaz de terminar con el acceso**: Asegúrese de que el proceso para terminar con el acceso de una cuenta pueda ser revocado rápidamente cuando esto sea necesario. ¿Qué pasaría si, debido a un proceso de IT con defectos, un empleado resentido y hostil con acceso a información sensible o sistemas críticos pudiera conservar su acceso a la red después de haber sido despedido? Esté listo para responder. ■

Comentarios al estudio de Percepción sobre Seguridad Informática en México, 2005.

Por el Dr. Roberto Gómez Cárdenas
Instituto Tecnológico y de Estudios Superiores de Monterrey

El estudio de percepción llevado a cabo por Joint Future Systems S.C., nos muestra que para la gente de sistemas la seguridad informática representa integridad y confiabilidad de la información, mientras que para los no informáticos el concepto está relacionado con virus y control de acceso. Los virus siguen representando el principal temor de los usuarios con respecto a seguridad informática, los medios han tenido mucho que ver con esto, ya que es de lo que más informan. Cada vez que un nuevo gusano aparece en Internet, los medios de comunicación se encargan de darlo a conocer. No sucede lo mismo con otro tipo de ataques o amenazas, que muchas veces son confundidas con virus. Por otro lado, empezamos a ver que la gente de sistemas tiene más conciencia de lo que involucra la seguridad informática.

Las amenazas más fuertes para la gente no relacionada con sistemas son los virus, como consecuencia de lo comentado anteriormente. Otro factor que influye en que la gente considere a los virus como su principal amenaza, es el daño directo que este tipo de amenazas provoca en los usuarios. Ataques más elaborados van dirigidos a servidores de instituciones a cargo de gente de sistemas y no a usuarios comunes y corrientes, por lo que el usuario no se ve afectado de forma directa por este tipo de ataques. Lo anterior refuerza el hecho de que la gente de sistemas esté igual de preocupada por virus y por agresores internos. Después de todo, los usuarios no tienen que preocuparse por otros usuarios ajenos a su computadora personal. Podemos apreciar que el término de "hacker" hace su aparición como un elemento de ataque y no inteligencia, mucho se ha dicho que es en realidad un "hacker", pero la imagen de éstos sigue siendo mala.

El hecho de que la encuesta arroje que entre las principales medidas para proteger la información electrónica están las políticas y el manejo adecuado de contraseñas, habla de que ya se cuenta con una conciencia de la importancia de estos dos aspectos. Muchas son las compañías que no cuentan con una política de seguridad y varias de las que cuentan con ella, no la respetan. Es importante que el usuario esté conciente de que debe respetar una política y del cuidado que debe tener con sus contraseñas.

Sorprende que en cuestión de marcas aparezca HP, que es más vista como una proveedora de equipo que de soluciones de seguridad informática. Por otro lado que una marca antivirus aparezca como la segunda buena marca para enfrentar problemas de seguridad, no es más que una consecuencia de lo mencionado arriba. Vale la pena señalar que Linux aparece como algo seguro y muy por arriba de otros sistemas operativos comerciales. Asimismo, Linux sólo es considerado por las personas relacionadas con sistemas.

A pesar de los esfuerzos de Microsoft por mejorar su imagen como sistema operativo seguro, la mayor parte de la gente la sigue viendo como un software inseguro.

La gente está preocupada por falta de información y difusión sobre seguridad informática. Dada la pregunta, parece que esperan que esta información provenga del proveedor. ¿No sería mejor que el usuario, relacionado con sistemas o no, buscara la información por si mismo? ¿Cuánta gente de sistemas está inscrita en un grupo de interés relacionado con seguridad informática? ¿Cuántos usuarios se preocupan por recibir noticias relacionadas con seguridad informática y no esperar que éstas les lleguen de parte de un proveedor o de amigos, siendo victimas de "hoaxes"? Considero que es un buen punto a tomar en cuenta; es bueno que la gente esté conciente de que le hace falta información, pero sería mejor que esté dispuesta a buscarla. Uno de los factores que puede influir en esto, es la falta de información en español.

Por último, el control de acceso es considerado la principal medida para proteger las instalaciones. Sería interesante saber qué entiende la gente por control de acceso. Una de las desventajas del control de acceso a cualquier instalación es la molestia que provoca a los usuarios el seguir este tipo de reglas, el registro de la persona, de sus pertenencias, etc. Existe tecnología que puede ayudar a lo anterior, pero ¿hasta qué punto está dispuesta una persona a proporcionar su huella digital para poder entrar a un sitio de trabajo?

Según el estudio, el principal temor con respecto a seguridad informática, son los virus, la gente espera más información de sus proveedores y Microsoft debe redoblar esfuerzos para cambiar su imagen de software inseguro. ■

Seguridad y Comunicación

Por el Lic. Enrique Bustamante Martínez
Director General de la Fundación Ealy Ortiz A.C.
EL UNIVERSAL, México

La tendencia actual indica que la información será el vehículo de intercambio en los distintos mercados globales del presente siglo, tendencia que la sociedad mundial está adoptando de diversas formas. La moneda de intercambio para las nuevas generaciones es la información. "Information must be free" proclaman, y por eso la distribuyen libremente.

JFS

Los objetivos iniciales del Internet fueron académicos, de manejo de información especializada y de investigación, hoy en día éstos se han visto opacados por una ola enorme de nuevos servicios y una gran demanda por mejores tecnologías para el procesamiento de información presentada a través de datos, video y sonido, en donde los estándares son medidos en millones de bits de información por segundo y en resoluciones de hasta millones de pixeles, todo con el fin de satisfacer las necesidades de los "nuevos mercados" de entretenimiento, negocios y telecomunicaciones.

De lo anterior es evidente que el tema de seguridad informática se convierta en uno de los temas centrales de análisis y preocupación, no sólo en los medios de comunicación, sino en todas las empresas en el mundo.

Al menos en México, aunque ya es posible comprar toda clase de mercancías, incluyendo comida, pagar impuestos, adeudos o hasta trabajar a distancia empleando Internet, aun no se ha llegado a los extremos de generar individuos totalmente ajenos a su realidad e imbuidos en una realidad virtual, informática y sin contacto social, como ha sucedido en algunos puntos de la geografía mundial, pero en esa dirección se mueven algunos sectores, en especial los más jóvenes.

Sin una manera efectiva de regular la colocación de nueva información y de verificar la veracidad de sus contenidos, numerosos sitios contienen información mal estructurada, distorsionada o incluso falsa y muchos más, la "obtienen" de otros sitios sin autorización de sus autores, o de la empresa que la genera. El tema de seguridad informática en las empresas ha llegado a ser motivo de investigaciones dentro de marcos legales del más profundo rigor.

Desde la invención de la imprenta por Gutenberg en el siglo XVI y la revolución industrial del siglo XVIII, ningún otro avance tecnológico había impactado en tan grande escala a la sociedad como el Internet.

Recientemente el Instituto Tecnológico de Massachussets (MIT por sus siglas en inglés), hizo públicos los resultados de una extensa encuesta en donde se planteó a los interrogados que indicaran cuál o cuáles consideraban eran los principales desarrollos tecnológicos que habían cambiado el mundo.

Internet ocupó el primer sitio, por encima de teléfonos celulares, computadoras portátiles, memorias portátiles, el DVD, la biotecnología o la medicina genómica. En muchos sentidos, puede decirse que Internet ha creado un antes y un después, de la misma manera que ocurrió hace muchas décadas con la invención y popularización de la televisión o del teléfono o de la radio. Con ello, los estudiosos y promotores del tema de seguridad, intentan un desarrollo en paralelo.

Tal vez no sea exagerado considerar que la brecha cultural es más parecida a la surgida con la invención de la imprenta que a cualquier otra. Pero en este caso, la enorme cantidad de información disponible y la velocidad con que se puede acceder a ésta, han hecho a esta revolución tecnológica más acelerada y con un impacto más profundo.

Internet puede convertirse en la principal fuerza unificadora jamás vista en el mundo, al hacer que el conocimiento, base de todo progreso, quede al alcance de todos, ahora será necesario unificar a este crecimiento, una cultura de la seguridad informática, que hasta hoy, ha demostrado un retraso frente al acelerado crecimiento de las nuevas tecnologías dentro de la llamada sociedad de la información, pero que es considerada fundamental en el desarrollo de un futuro cercano de un mundo cada vez más interrelacionado. ■

Soluciones de Gestión de Identidad

Por Alejandro Salud Cerdeño
Director de Mercadotecnia
Sun Microsystems de México

La gestión efectiva de las identidades de usuario y su acceso a recursos empresariales, se ha convertido en un requisito crítico para competir en el entorno empresarial actual.

Las organizaciones están aumentando el número de clientes, empleados, socios y proveedores, que tienen acceso a recursos críticos de información, pero al mismo tiempo deben proteger sus datos sensibles.

Este reto ha abierto a las empresas hacia nuevas formas de hacer negocios, garantizando simultáneamente que sus activos de información sigan siendo seguros.

Por eso hoy en día existen diferentes soluciones de gestión de identidad que racionalizan y simplifican el proceso de las identidades de usuario en todas las variedades de infraestructuras de computación y entornos de aplicaciones. Acaban con costosos enfoques manuales para crear, mantener y eliminar datos de identidad, permitiendo a las organizaciones aumentar la accesibilidad, preservando una estricta seguridad. Además, para ayudar a garantizar el cumplimiento de los requisitos regulatorios que existen hoy en día, las soluciones de gestión de identidad pueden ofrecer un control centralizado, una visibilidad completa de los privilegios de acceso y una ejecución consistente de las políticas de gestión de identidad.

La solución de gestión de identidades de Sun ofrece capacidades de gestión de identidad de punto a punto superiores. Incluye todas las funciones y servicios básicos que necesitan las empresas para utilizar, compartir y gestionar, la información de las identidades. ■

"Phishing" y "Pharming"

Por Juan Francisco Serrano
Director General de Joint Future Systems

JFS

Dos actividades ilícitas que han ido creciendo, son las conocidas a nivel mundial como "phishing" y "pharming"

Existe debate sobre el origen de los términos. Algunas personas creen que es simplemente lo mismo que "fishing" o pesca en inglés, remplazando la "f" por "ph" como moda de los usuarios de Internet, mientras que otros expertos opinan que es una combinación de "fishing" y PH, significando Personal History. Lo mismo ocurre con pharming, que viene del término "farming" o cosechar en inglés.

Independientemente del origen del término, ambas actividades están enfocadas al robo de información confidencial ("pescando" para ver quien cae en la trampa o "cosechando" al crear áreas para la obtención de datos) a través de Internet (principalmente de aspectos financieros, como serían: claves de acceso, números de tarjetas de crédito, cuentas bancarias, números de claves confidenciales de acceso a cajeros automáticos, etc.)

El "**phishing**" se basa en el engaño directo al usuario. A través de un correo electrónico, se le solicita hacer click en una liga, dentro de ese correo electrónico, la cual supuestamente lo llevará a una institución financiera . Por la facilidad de enviar correos electrónicos, la idea de los atacantes o defraudadores, es mandar millones de correos con esta solicitud. Si bien muchos de los receptores del correo no tendrán ninguna relación con la institución financiera que se menciona en el correo, existe una alta probabilidad de llegar a usuarios reales con cuentas en esa institución, principalmente si se trata de una empresa grande con una base extensa de cuentahabientes en un país o en el mundo entero. Una vez que el usuario ha dado clic sobre la liga, accede a una página falsa, la cual suele ser una copia casi perfecta del sitio verdadero.

Al usuario se le pide que ingrese su nombre de usuario y contraseña, datos que son capturados en ese momento por los agresores. Es frecuente que adicionalmente se le pidan al usuario una serie de datos financieros adicionales, con la excusa de estar actualizando información. Si el usuario cae en esta trampa, le está entregando a desconocidos, instantáneamente, información con la cual pueden cometerse múltiples fraudes en contra del mismo usuario.

Generalmente los correos electrónicos pretenden intimidar al usuario para que actúe inmediatamente, con argumentos como: "Si no ingresa a esta página y actualiza su información, su cuenta será congelada". Es importante notar que los correos electrónicos de este tipo son cada vez más sofisticados e inteligentes, y no siempre son tan burdos como el ejemplo mencionado anteriormente. Correos más sofisticados incluyen ofertas para participar en sorteos o rifas, avisos de que la información del usuario ha sido comprometida porque alguien ha hecho mal uso de ella (por lo cual se le solicita revise las transacciones y cambie su información financiera, obviamente en el sitio fraudulento) y múltiples otras maneras de lograr que el usuario teclee su información dentro de la página falsa.

"**Pharming**" es una técnica mucho más compleja y peligrosa. De manera sumamente simplificada, consiste en manipular con software las direcciones que utiliza una máquina para llevar un usuario a una página determinada. Toda dirección en Internet consiste en una serie de números, como por ejemplo 100.100.100.100. Este número es conocido como dirección IP, el cual, por la poca memorabilidad que ofrece su estructura, se asocia a un nombre alfanumérico de más fácil identificación y recordación para los usuarios (como www.jfs.com.mx , por ejemplo), por un servidor destinado específicamente para ello, al cual se le conoce como un "Domain Name Server" DNS o Servidor de Nombres de Dominio. Se utilizan estos servidores de DNS a diferentes niveles, desde máquinas individuales hasta servidores mundiales, pasando por redes locales y proveedores de acceso a Internet. Esta estructura jerárquica es necesaria para poder manejar las millones de millones de búsquedas que se hacen de DNS a nivel mundial cada minuto.

A través de "pharming", un agresor manipula estos servidores, en cualquiera de sus niveles, para que al

teclear una dirección, el usuario sea llevado a una página falsa. Evidentemente, cuanto más alto es el nivel jerárquico del servidor (por ejemplo un servidor mundial), más difícil va a ser concretar el ataque; además, la gran cantidad de usuarios que se verían afectados, permitiría a los prestadores del servicio identificar, con cierta facilidad, que se trata de una actividad anormal y posiblemente fraudulenta. El nivel más peligroso es el de proveedores de Internet, porque puede sólo ser atacado uno de sus servidores, lo cual asegura al agresor un número interesante de personas que van a su página falsa, pero no lo suficientemente grande como para que sea rápidamente detectado el problema. Es posible, inclusive, que la liga que aparece en un buscador haya sido "secuestrada" y envíe al usuario a una página falsa.

Los "pharmers" muchas veces sólo requieren una página de entrada falsa, de donde toman el nombre de usuario y la clave que tecleó el usuario, y luego lo mandan a la página real, (utilizando esa misma clave y nombre de usuario), lo cual hace difícil la detección de que algo haya sucedido, puesto que el usuario percibirá que todo el tiempo ha estado navegando dentro de un sitio real, no dándose cuenta de que sus datos han sido robados.

¿Qué se puede hacer?

Hay varias recomendaciones para que los usuarios se protejan contra este tipo de agresores:

Contra "Phishing":

1. En general, las instituciones financieras nunca solicitan datos de sus cliente por correo electrónico. Desconfíe de cualquier correo de este tipo y contacte a su institución financiera por teléfono.
2. Nunca le dé click a una liga dentro de un correo. Si quiere ir a un sitio, teclee la dirección directamente en su navegador.
3. Reporte el evento: Averigüe si la institución tiene una dirección de correo específica para enviarles este tipo de correos y utilice la función de reenviar (forward) de su programa de correo para enviarles el correo sospechoso, de manera que ellos puedan tomar cartas en el asunto. IMPORTANTE: No intente copiar el correo o guardarlo en su disco, simplemente reenvíelo a donde le indique su institución financiera y bórrelo inmediatamente después.
4. Evite hacer click encima del cuerpo de texto del correo, sobre todo si el puntero del mouse se visualiza como una manita o flecha, en lugar del cursor normal en forma de I. Esto indica que se trata de una imagen con una liga, y no de texto en su formato natural.
5. Si ya entró a una página y algo le parece sospechoso, o se da cuenta de que está usted en un sitio falso, inmediatamente contacte al sitio original y cambie toda la información que pueda haber sido comprometida.
6. No dé información que solicite un sitio, si no es coherente. (Por ejemplo, para qué podría un sitio pedirle el NIP de cajero automático).
7. No haga caso de amenazas del tipo de que "su cuenta será suspendida si usted no da click aquí" .
8. Cambie sus claves frecuentemente, dependiendo del uso que les dé. Mientras más frecuentemente las use, más frecuentemente debe cambiarlas. Se sugiere que una persona que usa su clave para acceder a su banco diariamente, por ejemplo, cambie su clave una vez por semana.
9. Reporte el correo sospechoso a su proveedor de Internet.
10. No utilice las mismas claves para todas sus cuentas de correo y de acceso a páginas. Se recomienda tener una diferente para cada sitio en donde se maneja información confidencial. Puede usarse una clave tipo "comodín" para todos los registros a página que no tienen mayor importancia.

Contra "Pharming":

1. Utilice proveedores de Internet confiables. Desconfíe de ofertas de empresas poco conocidas, con precios muy bajos, no necesariamente porque estas empresas sean poco éticas, sino porque sus bajos costos pueden indicar una falta de inversión en seguridad.
2. Evite utilizar máquinas en lugares públicos como cafés Internet, Hot Spots y hoteles, para acceder a sitios en donde se manejen datos confidenciales para usted.
3. Lleve usted un registro completo de todas las transacciones y consultas que haga en los sitios en donde puede manejar información confidencial. Reporte al sitio inmediatamente cualquier actividad que no haya sido hecha por usted.
4. Utilice software original y manténgalo actualizado. Si es de código abierto, obtenga programas que le informen de cualquier cambio que sufra dicho código.
5. Comuníquese con su proveedor de acceso a Internet o administrador de red e infórmele de su preocupación por el tema de "pharming". Exprese claramente su expectativa de que ambos lleven a cabo todas las medidas necesarias para proteger sus servidores de dominio, de cualquier tipo de ataque.
6. Cambie sus claves frecuentemente, al igual que en el caso de protección en contra de "phishing".
7. Instale programas que protejan a su computadora en este nivel básico.
8. Reporte cualquier anomalía que detecte, a su administrador de red, proveedor de Internet y a sus compañeros de trabajo. Si es un usuario de Internet en casa, pida a su proveedor de acceso que verifique la validez de un sitio.

Además de estas acciones preventivas contra ambos tipos de amenaza, se recomienda trabajar con empresas financieras (nacionales e internacionales) conocedoras de tecnología, que estén dispuestas a apoyar a sus clientes en caso de cualquier problema, así como trabajar con ellos para buscar soluciones. Si estas empresas ofrecen alguna garantía al cliente por escrito, sería un motivo importante para seleccionarlos sobre otras alternativas.

Si bien estos consejos no abarcan todas las posibilidades de ataque, pueden reducir significativamente los riesgos de cualquier usuario, tanto corporativo como individual. Aún así, la responsabilidad de toda área de sistemas y de cualquier usuario de Internet, es mantenerse actualizado sobre el tema en forma permanente, para conocer las nuevas formas de ataque que vayan surgiendo y saber enfrentarlas. Como bien es sabido, cada vez que se encuentran soluciones, ya sean tecnológicas o de cualquier otro tipo, ante las amenazas creadas por personas malintencionadas, los mismos agresores tenderán a crear nuevas formas de ataque y a incrementar el grado de sofisticación de las mismas. Es una guerra sin fin, en donde tendrá más probabilidades de sobrevivir quien esté más informado y cuente con las herramientas adecuadas en el momento preciso. ■