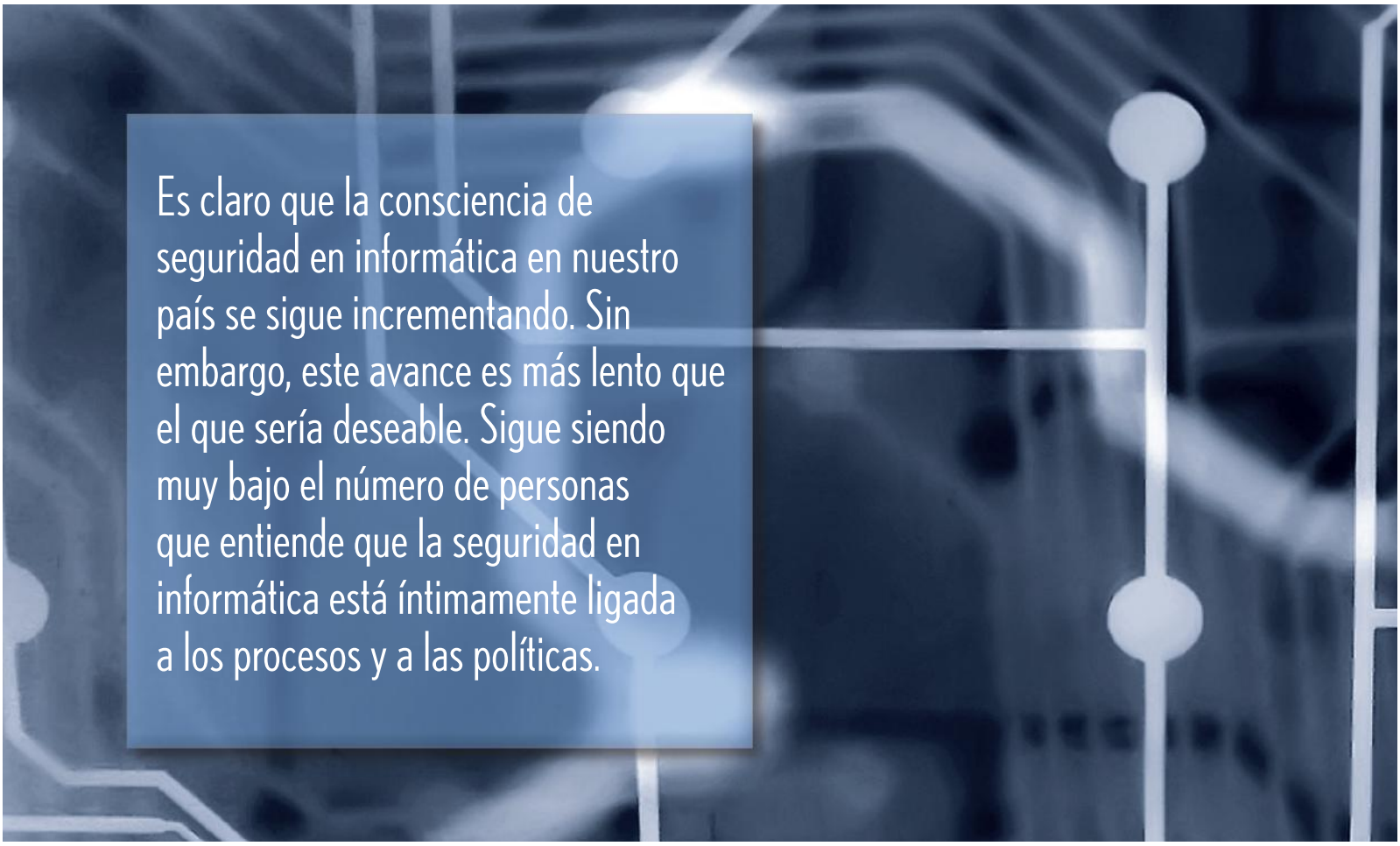
Se agradece la ayuda de la Fundación Ealy Ortiz , A.C.

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.

Foto portada: Doug Olson / Fotolia.com



Tradicionalmente, el concepto de Seguridad en Informática se ha asociado con ámbitos tecnológicos altamente sofisticados, fuera del alcance y comprensión del hombre común. Para las personas definidas como **No-Informáticos**, es decir, aquéllas que por el rol que desempeñan en la organización para la cual trabajan, no tienen bajo su responsabilidad las decisiones de implementación tecnológica, la Seguridad en Informática suele ser, o al menos había solido ser, un tema álgido y misterioso, materia de las discusiones entre los gurúes del "Olimpo", sobre el cual sólo los pertenecientes al círculo místico podían opinar. Sin embargo, la seguridad en informática se ha vuelto parte de la vida cotidiana de todos los usuarios de equipo de cómputo, tanto en el ámbito profesional como en el personal.

Quienes han estado a cargo de un área de tecnología o al menos han desempeñado las adquisiciones e instalación de los equipos de cómputo de su empresa, saben que la seguridad de la información no es únicamente responsabilidad suya. Este grupo, denominado en este estudio como los **Informáticos**, está consciente de que su papel es fundamental para promover ambientes seguros dentro de su organización, pero sabe que conseguirlo no depende cien por ciento de lo que él haga ni del alcance de sus decisiones. El involucramiento de toda la organización es indispensable, empezando por el conocimiento y las buenas prácticas de los usuarios, soportado por las áreas de decisión en diversos ámbitos, como son la Dirección General, Finanzas y Recursos Humanos, principalmente.

Para analizar los cambios en la percepción que de un año a otro se van dando alrededor de la Seguridad en Informática en México, **Joint Future Systems**, por cuarto año consecutivo, ha encabezado el **Estudio de Percepción sobre Seguridad en Informática México 2008**, con el apoyo de empresas patrocinadoras, todas ellas líderes en nuestro país en la creación de una cultura de seguridad.

A pesar de que se han visto algunos avances en el transcurso de los últimos años, esta conciencia no ha permeado adecuadamente, al menos en México. Los Informáticos sienten que no tienen los apoyos suficientes dentro de su organización, que les ayuden

a cerrar el candado de una estrategia integral de seguridad de la información. Y no siempre es una cuestión relacionada con disponibilidad de presupuesto; casi el 38% de los integrantes de este grupo percibe que la Seguridad en Informática es poco importante o nada importante, dentro de su empresa.

Del lado de los usuarios en general, se observa un mayor conocimiento de los riesgos y amenazas que atentan contra los sistemas informáticos y que pueden repercutir en sus propios intereses. Muestran una mayor preocupación alrededor del comercio electrónico y de las transacciones financieras en línea, de los alcances cada vez más extensos de la difusión pornográfica y están más familiarizados con la terminología de Seguridad, como *Phishing, Spyware,* Suplantación o Robo de Identidad, etc. Sin embargo, esta conciencia está más internalizada en los usuarios, por las consecuencias que puede tener el uso de la tecnología y las comunicaciones en su ámbito personal o familiar, y no tanto como parte de una cultura empresarial que promueva la Seguridad en Informática. Para ellos puede ser mucho más importante la confidencialidad de su correo electrónico personal, que la integridad de las bases de datos de su empresa o la continuidad del negocio para el cual trabajan.

Este estudio proporciona información recopilada de dos fuentes complementarias, lo que permite contemplar dos perspectivas, tanto la del usuario común, divididos, como se mencionó anteriormente en informáticos y no informáticos, y un grupo de expertos. 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 y colaboradores especiales, 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 18 expertos en temas relacionados con seguridad en informática.
C) 4 artículos de interés, relacionados con seguridad en informática.

CONTENIDO

III. ESTUDIO CON EXPERTOS Y PROVEEDORES LÍDERES DEL MERCADO TI 25

V. ARTÍCULOS SOBRE SEGURIDAD EN INFORMÁTICA 36

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. Conocer cuáles normas y regulaciones relacionadas con seguridad en informática están presentes en la mente de los usuarios en general.
6 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.
7. Crear un entorno que impulse el crecimiento del mercado de productos y servicios de seguridad, así como la correcta implementación de soluciones especializadas.
8. 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, asociaciones 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.

Metodología

Método de investigación

Se utilizó la encuesta como método de investigación, aplicando un cuestionario estructurado como instrumento de medición. La recopilación principal de información se llevó a cabo a través de encuestas personales y por correo electrónico.

Posteriormente, se realizaron encuestas telefónicas, que permitieron cubrir la cuota del 30% de entrevistados de la categoría "Informáticos".

Características de la muestra

Perfil de los entrevistados

Característica principal	Directivos y niveles medios de diferentes áreas organizacionales, de instituciones y empresas de todos tamaños.
Edad:	Indistinta
Sexo:	Indistinto
Cobertura geográfica:	Múltiple, dentro de la República Mexicana
N.S.E.	Indistinto

Tamaño de la muestra

Total informáticos	311
Total No Informáticos	726
Total entrevistados	*1,037*

Codificación de respuestas

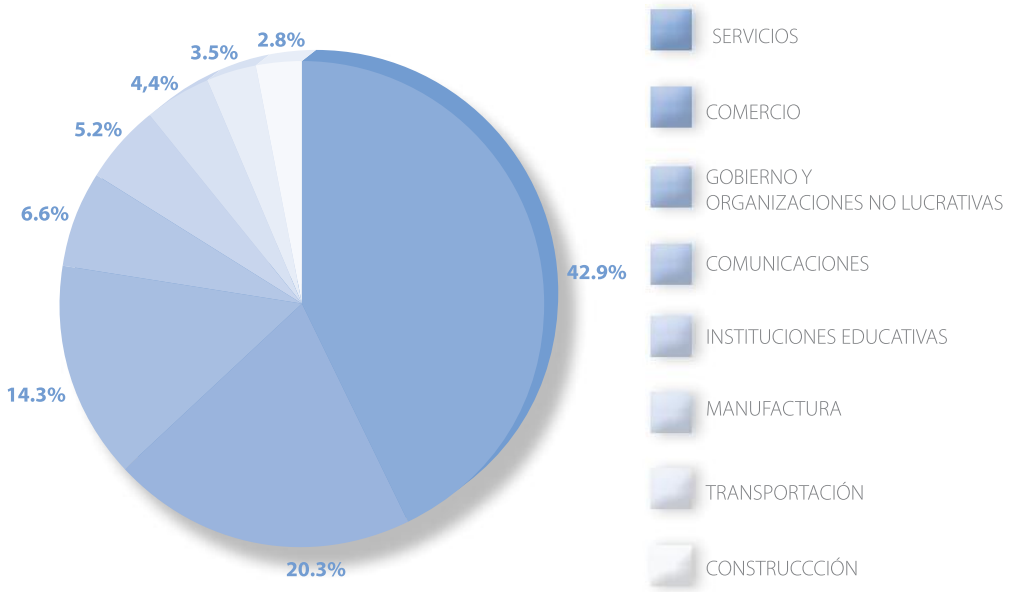
La mayoría de las preguntas solicitaban responder con una selección determinada de respuestas de opción múltiple (las 5 respuestas, principalmente, que resultaran más significativas para el entrevistado, de entre una extensa lista). Para las preguntas que por sus características requerían respuestas abiertas y espontáneas, todas éstas 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

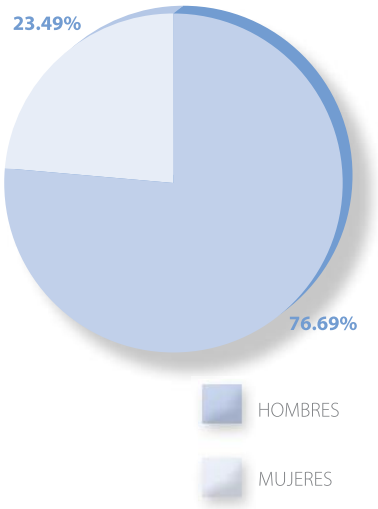
Composición de la muestra

La composición de la muestra se clasifica bajo tres criterios – por sector, por sexo y por puesto o área de trabajo.

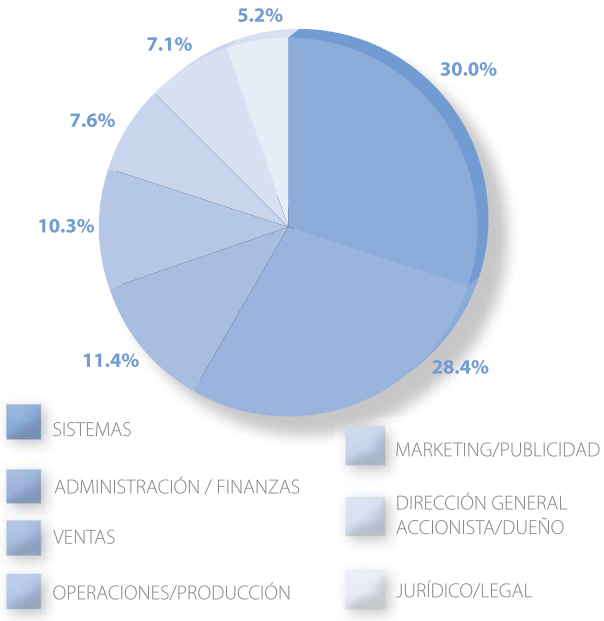
GRÁFICA 1. COMPOSICIÓN DE LA MUESTRA POR SECTOR



GRÁFICA 2. COMPOSICIÓN DE LA MUESTRA POR SEXO



GRÁFICA 3. COMPOSICIÓN DE LA MUESTRA POR PUESTO/ÁREA



¿Qué se entiende por "Seguridad en Informática"?

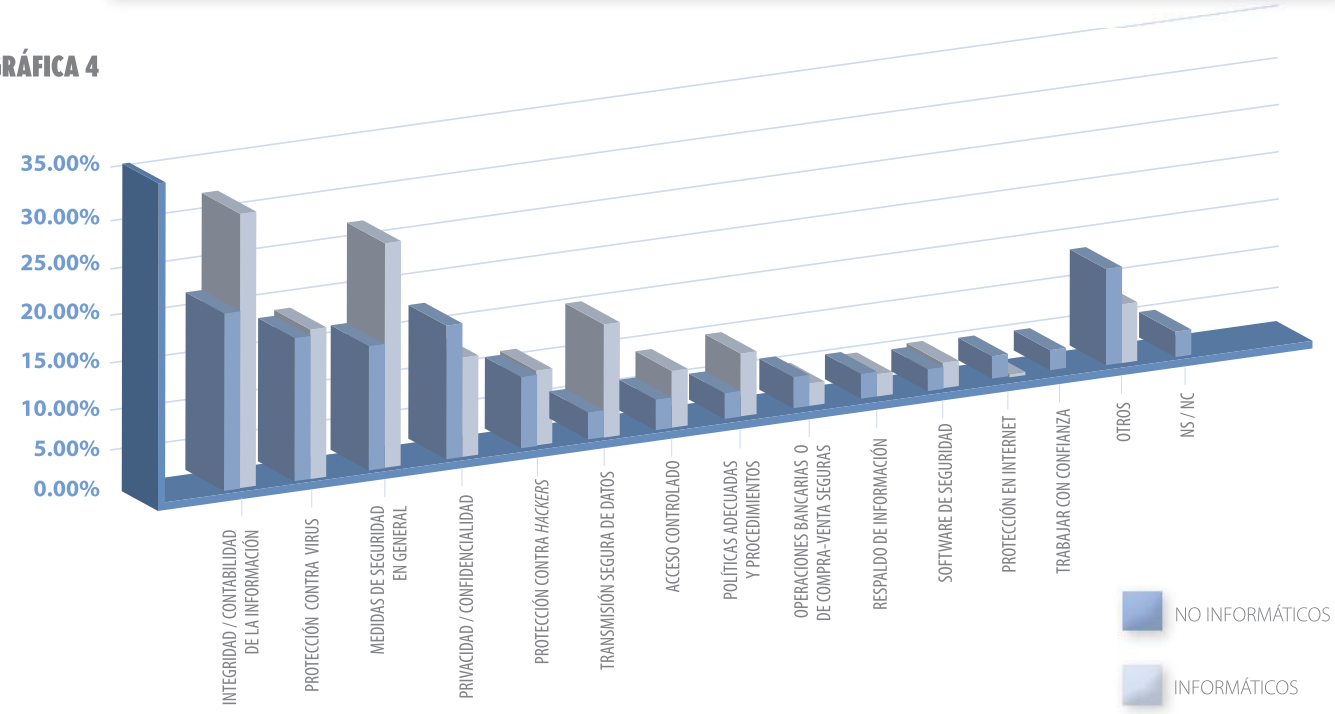
Pregunta: Hablando del término "Seguridad en Informática", ¿Qué entiende usted por este concepto? ¿Para usted qué significa?

Se registraron todas las respuestas emitidas por los entrevistados, quienes por lo regular mencionaron más de una opción (1.29 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codificadas, puede apreciarse en la Tabla 1 y la Gráfica 4.

TABLA 1

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Integridad / Confiabilidad de la información	145	98	243	19,97%	31,51%	13,98%	9,45%	23,43%
Protección contra Virus	133	60	193	18,32%	19,29%	12,83%	5,79%	18,61%
Medidas de seguridad en general	106	82	188	14,60%	26,37%	10,22%	7,91%	18,13%
Privacidad / confidencialidad	114	36	150	15,70%	11,58%	10,99%	3,47%	14,46%
Protección contra Hackers	69	30	99	9,50%	9,65%	6,65%	2,89%	9,55%
Transmisión segura de datos	23	41	64	3,17%	13,18%	2,22%	3,95%	6,17%
Acceso controlado	30	23	53	4,13%	7,40%	2,89%	2,22%	5,11%
Políticas adecuadas / procedimientos / uso responsable	26	24	50	3,58%	7,72%	2,51%	2,31%	4,82%
Operaciones bancarias o de compra-venta seguras	34	11	45	4,68%	3,54%	3,28%	1,06%	4,34%
Respaldo de información	26	9	35	3,58%	2,89%	2,51%	0,87%	3,38%
Software de seguridad	21	11	32	2,89%	3,54%	2,03%	1,06%	3,09%
Protección en Internet	24	2	26	3,31%	0,64%	2,31%	0,19%	2,51%
Trabajar con confianza	19	-	19	2,62%	0,00%	1,83%	0,00%	1,83%
Otros	91	24	115	12,53%	7,72%	8,78%	2,31%	11,09%
NS/NC	28	-	28	3,86%	0,00%	2,70%	0,00%	2,70%
	889	**451**	**1.340**					

GRÁFICA 4



Integridad y Confiabilidad de la Información, es el rubro más relacionado con el concepto Seguridad en Informática por ambos grupos de entrevistados. Este hecho destaca en forma particular frente al estudio realizado en 2007, en tanto que este concepto ocupó el año pasado la quinta posición en frecuencia de las menciones sumadas de ambos grupos. Es notorio que este concepto ha ganado una posición más alta en la mente de los No-Informáticos respecto el año pasado, si bien sigue siendo significativamente más identificado por el grupo de Informáticos.

Integridad y Confiabilidad de la Información, es el rubro más relacionado con el concepto Seguridad en Informática por ambos grupos de entrevistados.

Resulta evidente que la Transmisión Segura de Datos es mucho más tomada en cuenta por el grupo de Informáticos.

Asimismo resulta evidente que la Transmisión Segura de Datos es mucho más tomada en cuenta por el grupo de Informáticos que por el de No-Informáticos, así como conceptos como el Acceso Controlado, las Políticas y Procedimientos adecuados. Cabe mencionar, sin embargo, que el número de menciones alrededor de ambos conceptos fue bastante bajo.

En contraparte, se muestra cómo la Privacidad y Confidencialidad de la Información tiene una mayor identificación como aspecto de Seguridad en Informática entre los No-Informáticos.

La protección contra virus sigue teniendo un lugar importante en la percepción de ambos grupos de entrevistados, como parte integrante de la Seguridad de la Información.

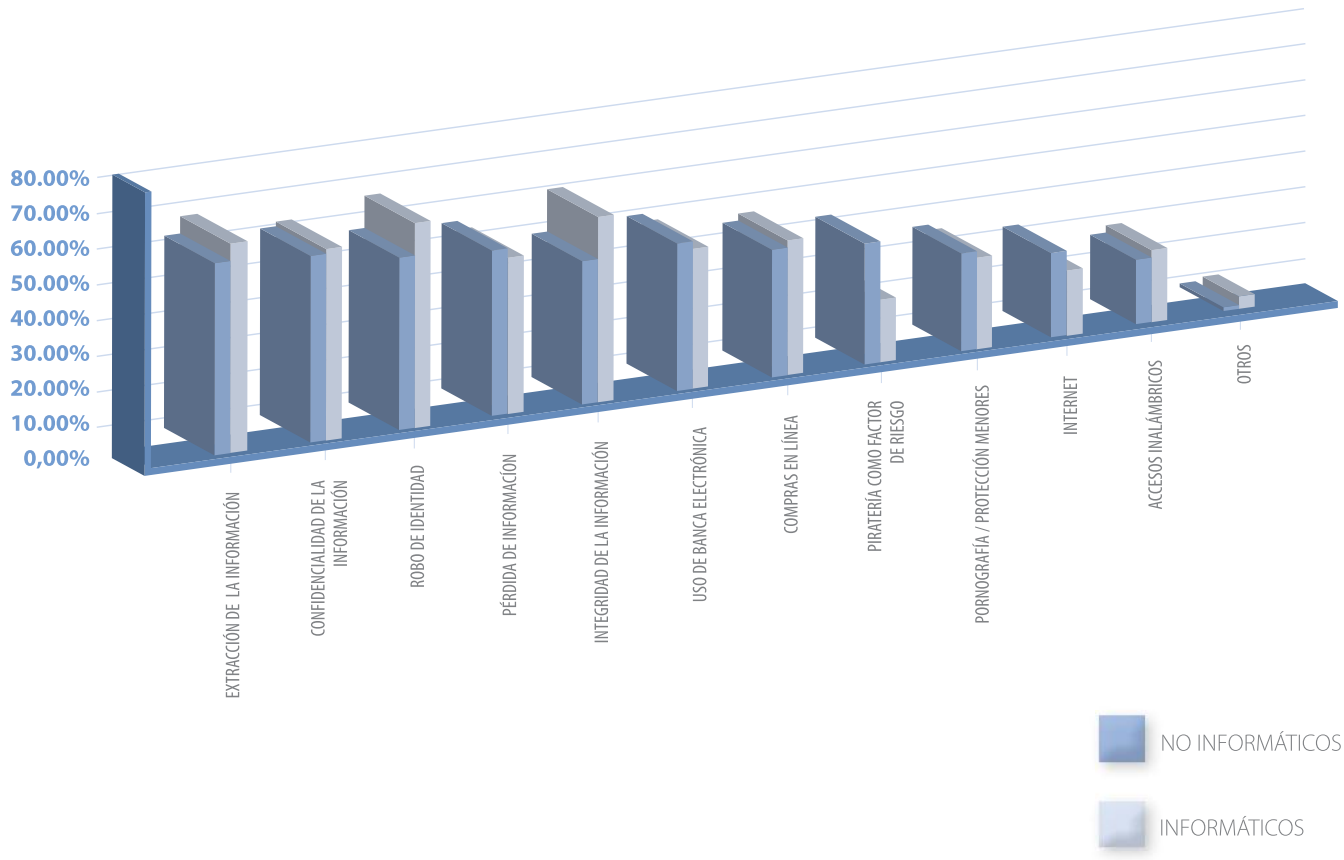
Principales preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido.

Pregunta: De la siguiente lista, por favor dígame las 5 opciones que representen sus principales preocupaciones en relación con la seguridad de los equipos de cómputo y de su contenido.

TABLA 2

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Extracción de información	453	211	664	62,40%	67,85%	43,68%	20,35%	64,03%
Confidencialidad de la Información	439	193	632	60,47%	62,06%	42,33%	18,61%	60,95%
Robo de identidad	403	208	611	55,51%	66,88%	38,86%	20,06%	58,92%
Pérdida de información	392	150	542	53,99%	48,23%	37,80%	14,46%	52,27%
Integridad de la información	337	183	520	46,42%	58,84%	32,50%	17,65%	50,14%
Uso de banca electrónica	346	140	486	47,66%	45,02%	33,37%	13,50%	46,87%
Compras en línea	312	140	452	42,98%	45,02%	30,09%	13,50%	43,59%
Piratería como factor de riesgo	297	64	361	40,91%	20,58%	28,64%	6,17%	34,81%
Pornografía / Protección menores	244	93	337	33,61%	29,90%	23,53%	8,97%	32,50%
Internet	216	65	281	29,75%	20,90%	20,83%	6,27%	27,10%
Accesos inalámbricos	184	86	270	25,34%	27,65%	17,74%	8,29%	26,04%
Otros	7	22	29	0,96%	7,07%	0,68%	2,12%	2,80%
	3.630	**1.555**	**5.185**					

GRÁFICA 5



Resulta significativo este año cómo la Extracción de Información es considerada como la principal preocupación, cuando en el estudio 2007 habían resaltado otros conceptos como el de Pérdida de Información, Invasión a la Privacidad y el uso de Banca Electrónica (principalmente en el grupo de los No-Informáticos).

Robo de Identidad e Integridad de la Información, es una preocupación percibida un poco más por los Informáticos que por los No-Informáticos, si bien este segundo grupo también está consciente de su importancia.

Si bien los conceptos de Piratería como Factor de Riesgo e Internet en sí mismo, no forman parte de sus principales preocupaciones, es evidente que ambas preocupaciones tienen más peso entre el grupo de No-Informáticos que en el de Informáticos.

Robo de Identidad e Integridad de la Información, es una preocupación percibida un poco más por los Informáticos que por los No-Informáticos, si bien éste segundo grupo también está consciente de su importancia.

Amenazas de mayor riesgo para la Seguridad de la Información

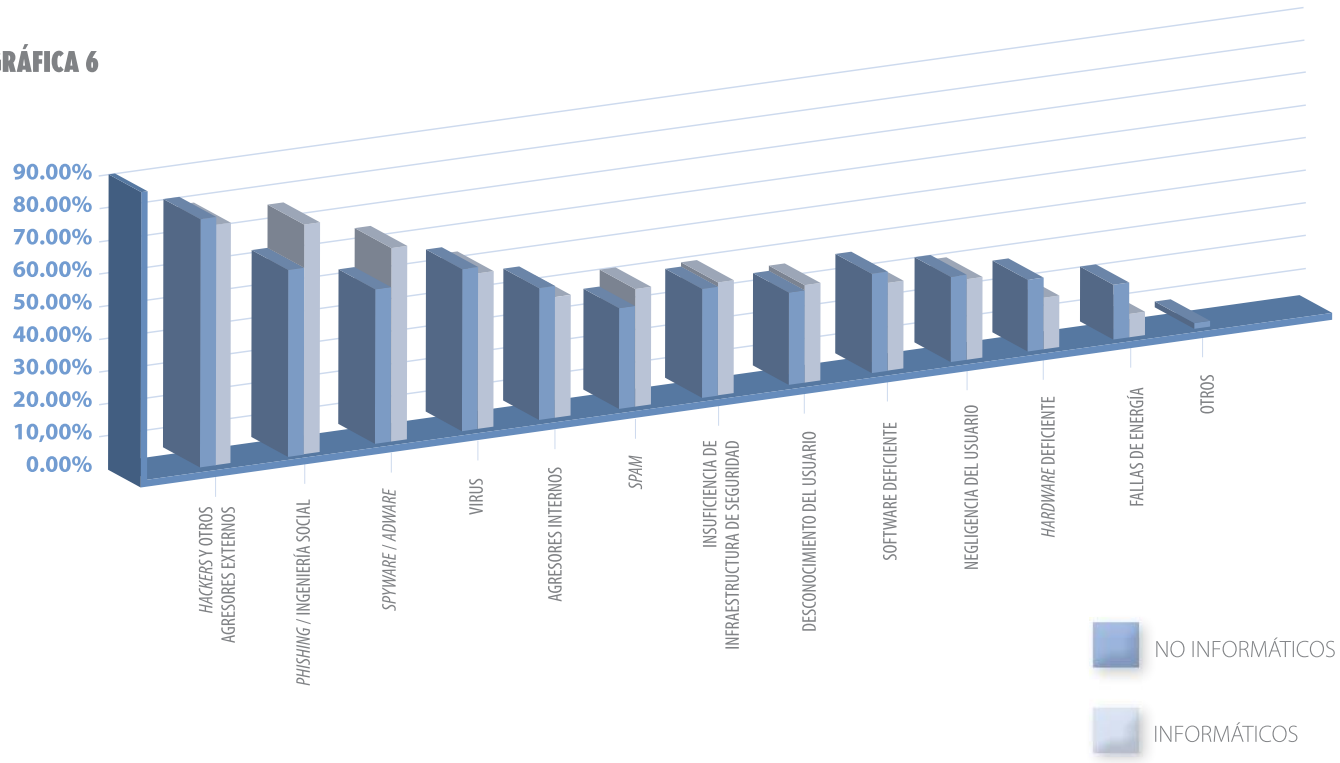
Pregunta: De la siguiente lista, por favor dígame las que considere son las 5 amenazas de mayor riesgo para la seguridad de la información.

La tabla de frecuencias y gráfica de respuestas a esta pregunta, se presentan, respectivamente, en la Tabla 3 y en la Gráfica 6.

TABLA 3

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Hackers y otros agresores externos	579	239	818	79,75%	76,85%	55,83%	23,05%	78,88%
Phishing / Ingeniería social	442	233	675	60,88%	74,92%	42,62%	22,47%	65,09%
Spyware / Adware	364	197	561	50,14%	63,34%	35,10%	19,00%	54,10%
Virus	378	161	539	52,07%	51,77%	36,45%	15,53%	51,98%
Agresores internos	328	128	456	45,18%	41,16%	31,63%	12,34%	43,97%
Spam	253	125	378	34,85%	40,19%	24,40%	12,05%	36,45%
Insuficiencia de infraestructura de seguridad	252	112	364	34,71%	36,01%	24,30%	10,80%	35,10%
Desconocimiento del usuario	228	102	330	31,40%	32,80%	21,99%	9,84%	31,82%
Software deficiente	240	89	329	33,06%	28,62%	23,14%	8,58%	31,73%
Negligencia del usuario	210	83	293	28,93%	26,69%	20,25%	8,00%	28,25%
Hardware deficiente	186	56	242	25,62%	18,01%	17,94%	5,40%	23,34%
Fallas de energía	158	30	188	21,76%	9,65%	15,24%	2,89%	18,13%
Otros	12	-	12	1,65%	0,00%	1,16%	0,00%	1,16%
	3.630	**1.555**	**5.185**					

GRÁFICA 6



Otro aspecto que resulta muy notorio, respecto de los estudios anteriores, es que los Virus como amenaza ya no son considerados el mayor riesgo para la Seguridad de la Información. En las investigaciones pasadas, este concepto había ocupado la primera posición en la percepción de ambos grupos de entrevistados y actualmente ocupa la cuarta entre todas las menciones.

Al parecer, tanto Informáticos como No-Informáticos, están más conscientes de que los ataques cada vez más están tendiendo a generar algún beneficio para quien lo lleva a cabo, en lugar de causar un daño por el daño mismo de manera aleatoria. De ahí que las amenazas consideradas de mayor riesgo sean aquéllas en donde existe una persona detrás, con la intención de obtener una ganancia, principalmente económica, como consecuencia del ataque. Así, las amenazas consideradas de mayor riesgo son los *Hackers* y otros agresores externos, el *Phishing* y la Ingeniería Social.

Tanto Informáticos como No-Informáticos, están más conscientes de que los ataques cada vez más están tendiendo a generar algún beneficio para quien lo lleva a cabo, en lugar de causar un daño.

Una mayor proporción del grupo de los Informáticos, respecto de los No-Informáticos, considera al *Phishing* / Ingeniería Social y al *Spyware / Adware,* como amenazas de riesgo.

Normas y regulaciones de seguridad que conoce

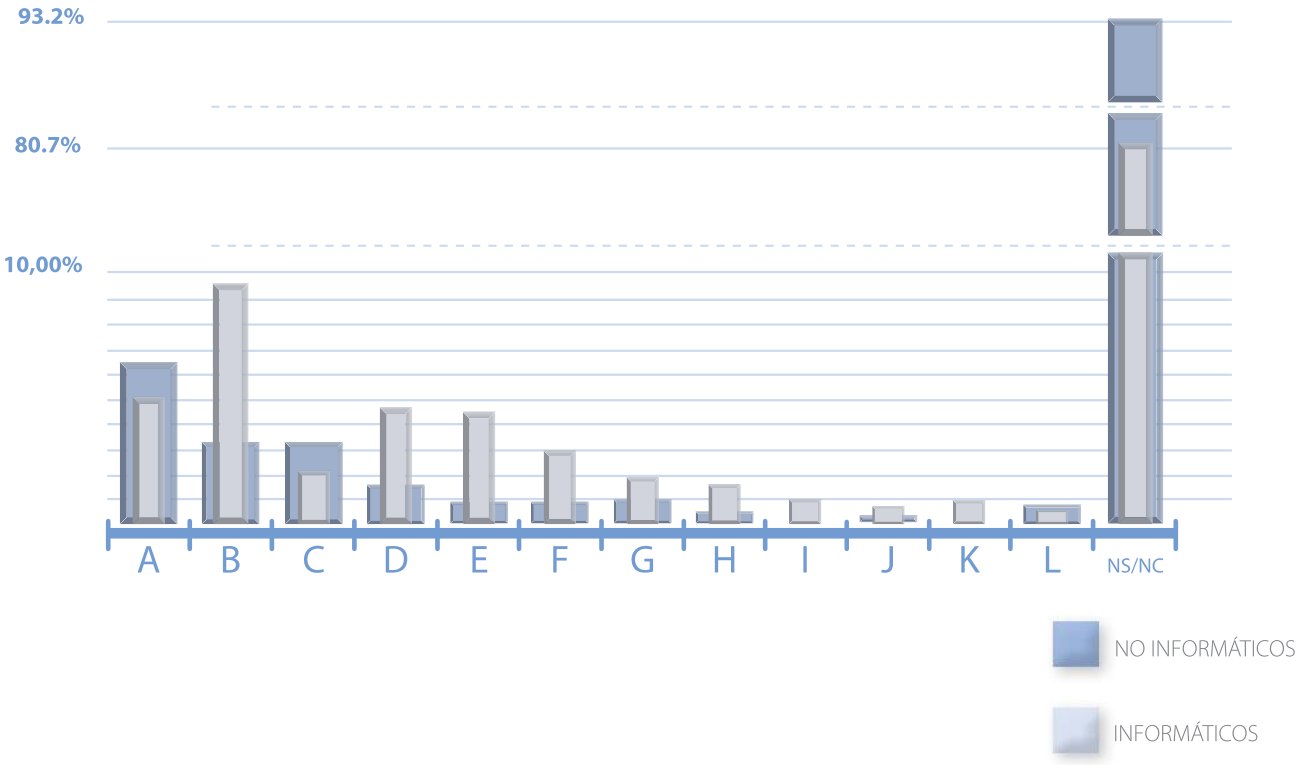
Pregunta: ¿Cuáles estándares, normas o regulaciones conoce, que mejoren la seguridad en informática?

La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 4 y en la Gráfica 7.

TABLA 4

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No nformáticos	Informáticos	No Informáticos	Informáticos	TOTAL
ISO 9000/9001	45	15	60	6,20%	4,82%	4,34%	1,45%	5,79%
Sarbanes-Oxley	21	30	51	2,89%	9,65%	2,03%	2,89%	4,92%
ISO/IEC	21	6	27	2,89%	1,93%	2,03%	0,58%	2,60%
ITIL	11	14	25	1,52%	4,50%	1,06%	1,35%	2,41%
ISO 27001	5	13	18	0,69%	4,18%	0,48%	1,25%	1,74%
ISO 17799	5	8	13	0,69%	2,57%	0,48%	0,77%	1,25%
COBIT	5	5	10	0,69%	1,61%	0,48%	0,48%	0,96%
BS 270001	2	4	6	0,28%	1,29%	0,19%	0,39%	0,58%
IEEE	-	2	2	0,00%	0,64%	0,00%	0,19%	0,19%
SISA	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
SSL	-	2	2	0,00%	0,64%	0,00%	0,19%	0,19%
Otros	3	1	4	0,41%	0,32%	0,29%	0,10%	0,39%
NS/NC	677	251	928	93,25%	80,71%	65,28%	24,20%	89,49%
	796	**352**	**1.148**					

GRÁFICA 7



A	ISO 9000/9001
B	Sarbanes-Oxley
C	ISO/IEC
D	ITIL
E	ISO 27001
F	ISO 17799
G	COBIT
H	BS 270001
I	IEEE
J	SISA
K	SSL
L	Otros
NS/NC	No sabe / No contestó

Respecto del estudio realizado el año pasado, se redujo significativamente la proporción de Informáticos que mostró tener un conocimiento sobre normas y regulaciones, habiendo disminuido de un 31.7% a un 19.29, mientras que la proporción de No-Informáticos aumentó de 1.70% a 6.75%

Como se puede observar, existe un alto grado de desconocimiento acerca de estándares, normas y regulaciones relacionadas con seguridad en informática. Prácticamente el 90 por ciento (89.49%) de todos los entrevistados (compuesto por un 93.25% de los No-Informáticos y un 80.71% de los Informáticos), mencionó no conocer nada al respecto. Del 10.5% que mencionó alguna, una gran parte de las menciones hicieron referencia a estándares o regulaciones que no están directamente relacionadas con seguridad (como fueron ISO 9000, ISO 9001, etc.).

Resulta notorio que en este estudio, respecto del estudio realizado el año pasado, se redujo significativamente la proporción de Informáticos que mostró tener un conocimiento al respecto, habiendo disminuido de un 31.7% a un 19.29%, mientras que la proporción de No-Informáticos aumentó de 1.70% a 6.75%

¿Qué hace falta por parte de los proveedores de TI?

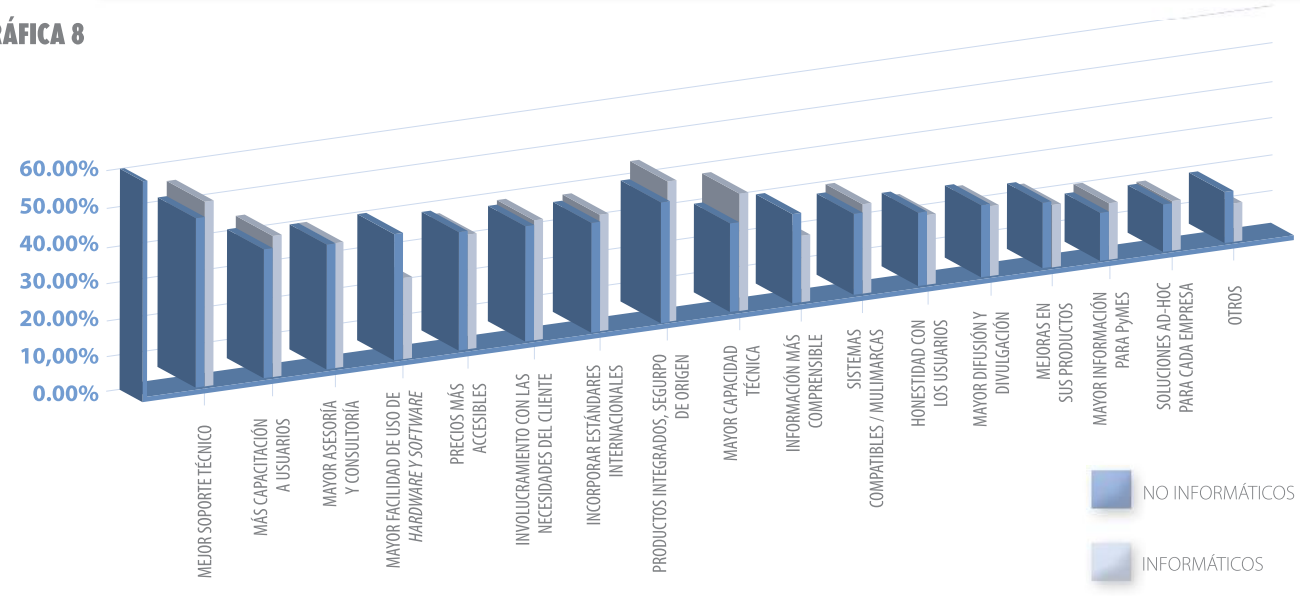
Pregunta: ¿Qué cree usted que deberían mejorar los proveedores de tecnología? Escoja 5 de las siguientes opciones, las que considere más importantes.

La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 5 y en la Gráfica 8.

TABLA 5

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Mejor soporte técnico	354	166	520	48,76%	53,38%	34,14%	16,01%	50,14%
Más capacitación a usuarios	291	134	425	40,08%	43,09%	28,06%	12,92%	40,98%
Mayor asesoría / consultoría	277	119	396	38,15%	38,26%	26,71%	11,48%	38,19%
Mayor facilidad de uso de *hardware y software*	282	70	352	38,84%	22,51%	27,19%	6,75%	33,94%
Precios más accesibles	263	108	371	36,23%	34,73%	25,36%	10,41%	35,78%
Involucramiento con las necesidades del cliente	254	114	368	34,99%	36,66%	24,49%	10,99%	35,49%
Incorporar estándares internacionales	228	111	339	31,40%	35,69%	21,99%	10,70%	32,69%
Productos integrados, seguros de origen	228	131	359	31,40%	42,12%	21,99%	12,63%	34,62%
Mayor capacidad técnica	207	111	318	28,51%	35,69%	19,96%	10,70%	30,67%
Información más comprensible	204	52	256	28,10%	16,72%	19,67%	5,01%	24,69%
Sistemas compatibles / mulimarcas	182	87	269	25,07%	27,97%	17,55%	8,39%	25,94%
Honestidad con los usuarios	170	70	240	23,42%	22,51%	16,39%	6,75%	23,14%
Mayor difusión / divulgación	167	70	237	23,00%	22,51%	16,10%	6,75%	22,85%
Mejoras en sus productos	159	61	220	21,90%	19,61%	15,33%	5,88%	21,22%
Mayor información para PyMES	120	58	178	16,53%	18,65%	11,57%	5,59%	17,16%
Soluciones ad-hoc para cada empresa	119	52	171	16,39%	16,72%	11,48%	5,01%	16,49%
Otros	125	41	166	17,22%	13,18%	12,05%	3,95%	16,01%
	3.630	**1.555**	**5.185**					

GRÁFICA 8



La capacitación a usuarios y un mayor nivel de asesoría, vuelven a ser de los factores más demandados a los proveedores de Tecnología de la Información, por parte de los entrevistados. Perciben que continúa habiendo huecos en este sentido, lo cual bien podría representar una oportunidad o área blanca tanto para fabricantes como para proveedores de servicios relacionados con tecnología y seguridad informática.

Destaca también el hecho de que para el usuario No-Informático, comparado con el Informático, la información que en general les llega sobre el tema, no les resulta tan comprensible como quisieran.

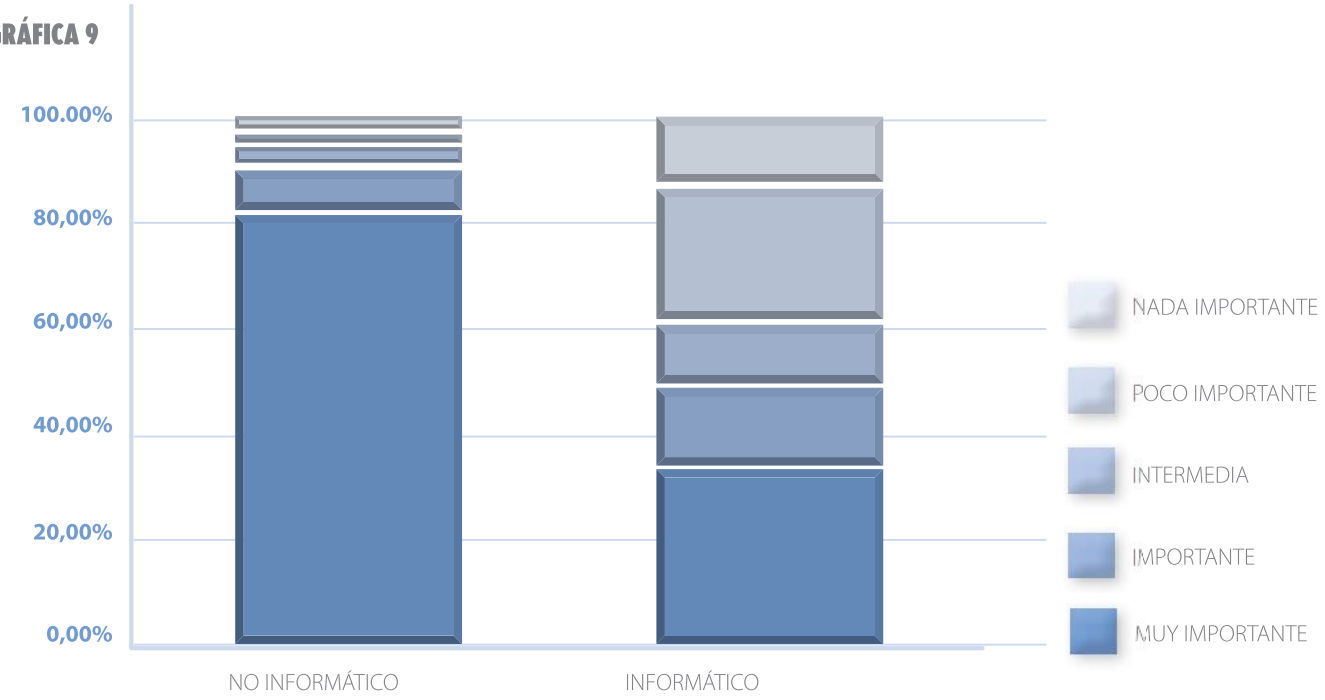
La capacitación a usuarios y un mayor nivel de asesoría, vuelven a ser de los factores más demandados a los proveedores de Tecnología de la Información, por parte de los entrevistados.

Importancia de la Seguridad en Informática en las empresas

Pregunta: ¿Qué tan importante cree usted que es la Seguridad en Informática para los directivos de la empresa en donde trabaja?

La representación de las respuestas a esta pregunta se presenta en la Gráfica 9.

GRÁFICA 9



Sólo el 34.73% de los Informáticos mencionaron que es muy importante.

Es muy marcada la diferencia de percepción entre ambos grupos de entrevistados, como puede observarse en la gráfica. Para la gran mayoría de los No-Informáticos (82.9%), las organizaciones donde trabajan consideran muy importante la Seguridad en Informática. Sin embargo, prácticamente la mitad de los Informáticos (50.16%) perciben que este concepto es importante en alguna medida para la Dirección de su empresa (sólo el 34.73% de los Informáticos mencionaron que es muy importante y un 15.43% percibe que la lo consideran importante). Perciben que el tema es poco importante o nada importante, 37.9% de este grupo.

Para la gran mayoría de los No-Informáticos (82.9%), las organizaciones donde trabajan consideran muy importante la Seguridad en Informática.

Aspectos a tomar en cuenta en la compra de tecnología

La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 6 y en la Gráfica 10.

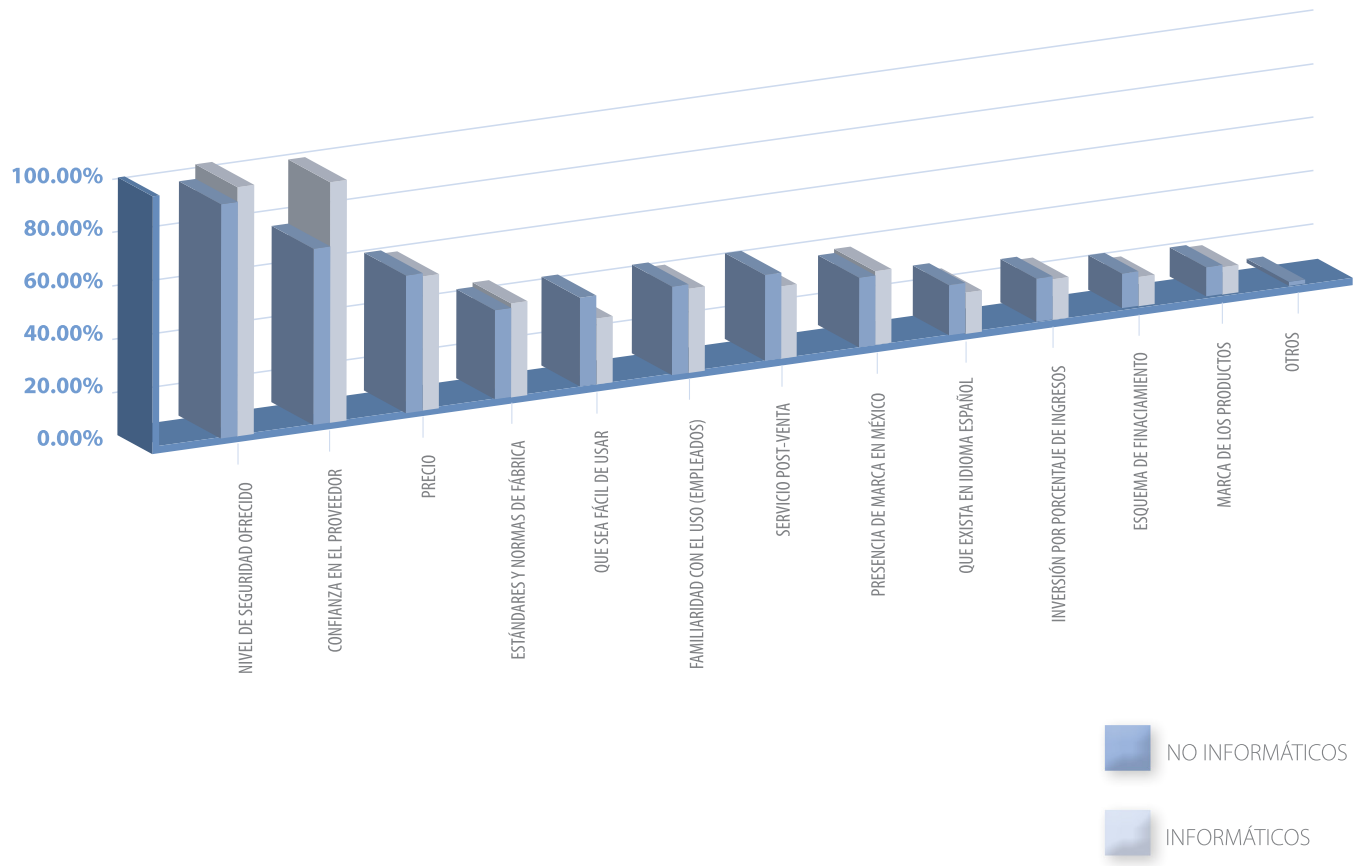
TABLA 6

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Nivel de seguridad ofrecido	672	306	978	92,56%	98,39%	64,80%	29,51%	94,31%
Confianza en el proveedor	512	300	812	70,52%	96,46%	49,37%	28,93%	78,30%
Precio	403	169	572	55,51%	54,34%	38,86%	16,30%	55,16%
Estándares y normas de fabricación / integración	312	139	451	42,98%	44,69%	30,09%	13,40%	43,49%
Que sea fácil de usar	308	98	406	42,42%	31,51%	29,70%	9,45%	39,15%
Familiaridad con el uso (empleados)	281	114	395	38,71%	36,66%	27,10%	10,99%	38,09%
Servicio post-venta	272	99	371	37,47%	31,83%	26,23%	9,55%	35,78%
Presencia de marca en México	213	95	308	29,34%	30,55%	20,54%	9,16%	29,70%
Que exista en idioma español	199	56	255	27,41%	18,01%	19,19%	5,40%	24,59%
Inversión por porcentaje de ingresos	180	72	252	24,79%	23,15%	17,36%	6,94%	24,30%
Esquema de financiamiento	155	59	214	21,35%	18,97%	14,95%	5,69%	20,64%
Marca de los productos	116	48	164	15,98%	15,43%	11,19%	4,63%	15,81%
Otros	7	-	7	0,96%	0,00%	0,68%	0,00%	0,68%
	3.630	**1.555**	**5.185**					

Los Informáticos son más susceptibles a considerar la confianza en el proveedor, que los No-Informáticos. Los usuarios No-Informáticos, empero, tienden a fijarse más que los Informáticos en aspectos como el que las soluciones sean fáciles de usar, el servicio posventa y el que estén disponibles en idioma español.

Es de resaltar, que el factor "precio" ocupa el tercer lugar en las prioridades de ambos grupos de entrevistados.

GRÁFICA 10



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: *¿Qué marcas de productos relacionados con Seguridad en Informática (tanto de hardware como de software) considera* ***buenas****?*

Pregunta*: ¿Qué marcas de productos relacionados con Seguridad en Informática (tanto de hardware como de software) considera* ***malas****?*

Las respuestas clasificadas a ambas preguntas, pueden consultarse en las respectivas Tabla 7 y Tabla 8.

TABLA 7

Marcas percibidas como BUENAS para enfrentar problemas relacionados con Seguridad en Informática

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Muestra =	**726**	**311**	**1.037**	**xni/726**	**xi/311**	**xni/1037**	**xi/1037**	
Norton/Symantec	224	110	334	30,85%	35,37%	21,60%	10,61%	32,21%
McAfee	104	83	187	14,33%	26,69%	10,03%	8,00%	18,03%
HP	84	46	130	11,57%	14,79%	8,10%	4,44%	12,54%
Panda	81	25	106	11,16%	8,04%	7,81%	2,41%	10,22%
Kaspersky	34	63	97	4,68%	20,26%	3,28%	6,08%	9,35%
Dell	79	13	92	10,88%	4,18%	7,62%	1,25%	8,87%
Cisco	17	42	59	2,34%	13,50%	1,64%	4,05%	5,69%
Compaq	40	12	52	5,51%	3,86%	3,86%	1,16%	5,01%
Apple / Macintosh	35	15	50	4,82%	4,82%	3,38%	1,45%	4,82%
Ninguno	31	19	50	4,27%	6,11%	2,99%	1,83%	4,82%
IBM	30	16	46	4,13%	5,14%	2,89%	1,54%	4,44%
Microsoft	28	11	39	3,86%	3,54%	2,70%	1,06%	3,76%
Verisign	8	24	32	1,10%	7,72%	0,77%	2,31%	3,09%
AVG	13	18	31	1,79%	5,79%	1,25%	1,74%	2,99%
Hauri	13	18	31	1,79%	5,79%	1,25%	1,74%	2,99%
Sony	27	1	28	3,72%	0,32%	2,60%	0,10%	2,70%
CA	7	21	28	0,96%	6,75%	0,68%	2,03%	2,70%
Trend Micro	14	11	25	1,93%	3,54%	1,35%	1,06%	2,41%
Checkpoint	2	21	23	0,28%	6,75%	0,19%	2,03%	2,22%
Bit Defender	8	12	20	1,10%	3,86%	0,77%	1,16%	1,93%
EMC	1	18	19	0,14%	5,79%	0,10%	1,74%	1,83%
Nod 32	12	6	18	1,65%	1,93%	1,16%	0,58%	1,74%
Sonicwall	-	18	18	0,00%	5,79%	0,00%	1,74%	1,74%
Adaware	11	1	12	1,52%	0,32%	1,06%	0,10%	1,16%
Windows Defender	4	6	10	0,55%	1,93%	0,39%	0,58%	0,96%
Fortinet	5	4	9	0,69%	1,29%	0,48%	0,39%	0,87%
Windows	9	-	9	1,24%	0,00%	0,87%	0,00%	0,87%
Linux	4	4	8	0,55%	1,29%	0,39%	0,39%	0,77%
Acer	7	-	7	0,96%	0,00%	0,68%	0,00%	0,68%
Watchguard	-	7	7	0,00%	2,25%	0,00%	0,68%	0,68%
Intel	6	-	6	0,83%	0,00%	0,58%	0,00%	0,58%
Toshiba	4	1	5	0,55%	0,32%	0,39%	0,10%	0,48%
Sun Microsystems	3	1	4	0,41%	0,32%	0,29%	0,10%	0,39%
WebSense	1	3	4	0,14%	0,96%	0,10%	0,29%	0,39%
Avast	2	1	3	0,28%	0,32%	0,19%	0,10%	0,29%
Epson	3	-	3	0,41%	0,00%	0,29%	0,00%	0,29%
Lanix	2	1	3	0,28%	0,32%	0,19%	0,10%	0,29%
Lenovo	3	-	3	0,41%	0,00%	0,29%	0,00%	0,29%
Zone Alarm	1	2	3	0,14%	0,64%	0,10%	0,19%	0,29%
ISS	2	1	3	0,28%	0,32%	0,19%	0,10%	0,29%
Aspel	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Gateway	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Oracle	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
PC Cillin	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
Prodigy	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Otros	50	17	67	6,89%	5,47%	4,82%	1,64%	6,46%
NS/NC	186	11	197	25,62%	3,54%	17,94%	1,06%	19,00%
	1.203	**685**	**1.888**					

TABLA 8

Marcas percibidas como DEFICIENTES para enfrentar problemas relacionados con Seguridad en Informática

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Muestra =	**726**	**311**	**1.037**	**xni/726**	**xi/311**	**xni/1037**	**xi/1037**	
Norton/Symantec	44	61	105	6,06%	19,61%	4,24%	5,88%	10,13%
Microsoft	34	60	94	4,68%	19,29%	3,28%	5,79%	9,06%
Piratas	57	35	92	7,85%	11,25%	5,50%	3,38%	8,87%
Panda	28	49	77	3,86%	15,76%	2,70%	4,73%	7,43%
Windows	29	42	71	3,99%	13,50%	2,80%	4,05%	6,85%
McAfee	10	34	44	1,38%	10,93%	0,96%	3,28%	4,24%
Dell	11	28	39	1,52%	9,00%	1,06%	2,70%	3,76%
Prodigy	13	3	16	1,79%	0,96%	1,25%	0,29%	1,54%
IBM	12	4	16	1,65%	1,29%	1,16%	0,39%	1,54%
PC Cillin	9	5	14	1,24%	1,61%	0,87%	0,48%	1,35%
Apple / Macintosh	12	2	14	1,65%	0,64%	1,16%	0,19%	1,35%
Sin marca	10	2	12	1,38%	0,64%	0,96%	0,19%	1,16%
Acer	10	1	11	1,38%	0,32%	0,96%	0,10%	1,06%
Compaq	10	-	10	1,38%	0,00%	0,96%	0,00%	0,96%
Kaspersky	4	5	9	0,55%	1,61%	0,39%	0,48%	0,87%
HP	7	-	7	0,96%	0,00%	0,68%	0,00%	0,68%
Toshiba	6	1	7	0,83%	0,32%	0,58%	0,10%	0,68%
Software Gratuito	4	1	5	0,55%	0,32%	0,39%	0,10%	0,48%
Sony	4	1	5	0,55%	0,32%	0,39%	0,10%	0,48%
AVG	3	1	4	0,41%	0,32%	0,29%	0,10%	0,39%
Gateway	4	-	4	0,55%	0,00%	0,39%	0,00%	0,39%
Adaware	1	3	4	0,14%	0,96%	0,10%	0,29%	0,39%
Aspel	3	-	3	0,41%	0,00%	0,29%	0,00%	0,29%
Cisco	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
Fortinet	-	2	2	0,00%	0,64%	0,00%	0,19%	0,19%
Internet Explorer	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Lanix	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Lime Wire	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
Linux	1	1	2	0,14%	0,32%	0,10%	0,10%	0,19%
Productos chinos	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Windows Vista	2	-	2	0,28%	0,00%	0,19%	0,00%	0,19%
Otros	33	21	54	4,55%	6,75%	3,18%	2,03%	5,21%
NS/NC	405	57	462	55,79%	18,33%	39,05%	5,50%	44,55%
	774	**421**	**1.195**					

¿Qué más les gustaría conocer acerca de Seguridad en Informática?

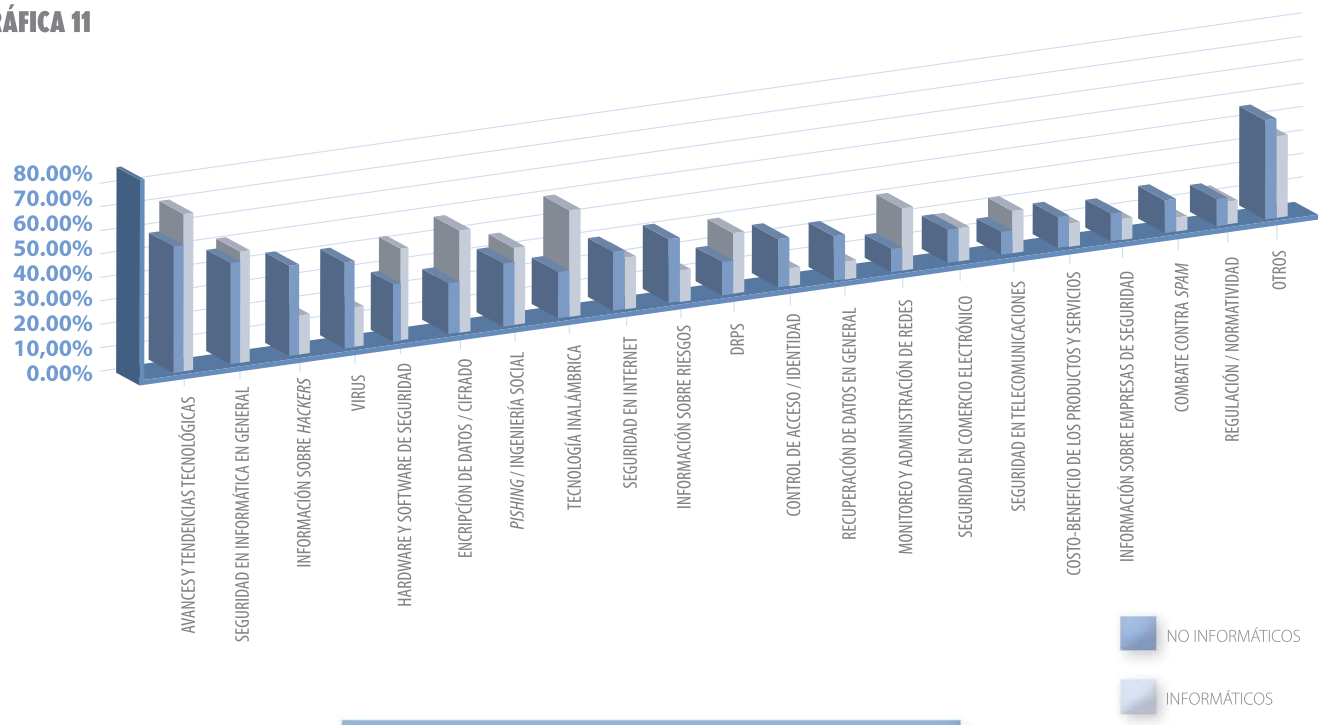
Pregunta: De las siguientes opciones, por favor seleccione los 5 temas sobre los cuales quisiera usted ampliar sus conocimientos.

Ver tabla de frecuencias y gráfica de respuestas en la Tabla 9 y en la Gráfica 11.

TABLA 9

	FRECUENCIA(fx)			% DE SU CATEGORIA		% DEL TOTAL DE RESPUESTAS		
Concepto	No Informáticos	Informáticos	Total	No Informáticos	Informáticos	No Informáticos	Informáticos	TOTAL
Avances y tendencias tecnológicas	380	210	590	52,34%	67,52%	36,64%	20,25%	56,89%
Seguridad en Informática en general	315	151	466	43,39%	48,55%	30,38%	14,56%	44,94%
Información sobre *Hackers*	288	42	330	39,67%	13,50%	27,77%	4,05%	31,82%
Virus	264	36	300	36,36%	11,58%	25,46%	3,47%	28,93%
Hardware y software de seguridad	174	123	297	23,97%	39,55%	16,78%	11,86%	28,64%
Encripción de datos / cifrado	157	139	296	21,63%	44,69%	15,14%	13,40%	28,54%
Phishing / Ingeniería social	187	106	293	25,76%	34,08%	18,03%	10,22%	28,25%
Tecnología inalámbrica	138	141	279	19,01%	45,34%	13,3´%	13,60%	26,90%
Seguridad en Internet	195	68	263	26,86%	21,86%	18,80%	6,56%	25,36%
Información sobre riesgos	199	23	222	27,41%	7,40%	19,19%	2,22%	21,41%
DRPs	101	83	184	13,91%	26,69%	9,74%	8,00%	17,74%
Control de acceso / identidad	159	20	179	21,90%	6,43%	15,33%	1,93%	17,26%
Recuperación de datos en general	146	20	166	20,11%	6,43%	14,08%	1,93%	16,01%
Monitoreo y administración de redes	72	85	157	9,92%	27,33%	6,94%	8,20%	15,14%
Seguridad en Comercio Electrónico	105	46	151	14,46%	14,79%	10,13%	4,44%	14,56%
Seguridad en telecomunicaciones	78	65	143	10,74%	20,90%	7,52%	6,27%	13,79%
Costo-Beneficio de los productos y servicios	101	27	128	13,91%	8,68%	9,74%	2,60%	12,34%
Información sobre empresas de Seguridad en Informática	89	26	115	12,26%	8,36%	8,58%	2,51%	11,09%
Combate contra *spam*	95	17	112	13,09%	5,47%	9,16%	1,64%	10,80%
Regulación / Normatividad	78	28	106	10,74%	9,00%	7,52%	2,70%	10,22%
Otros	309	99	408	42,56%	31,83%	29,80%	9,55%	39,34%
	3.630	**1.555**	**5.185**					

GRÁFICA 11



Temas que interesan más a los No-Informáticos que a los Informáticos:

- *Información sobre Hackers*
- *Información sobre Virus*
- *Información sobre riesgos*
- *Control de acceso / Identidad*
- *Recuperación de datos en general*

Temas que interesan más a los Informáticos que a los No-Informáticos:

- *Hardware y software de seguridad*
- *Encripción de datos / cifrado*
- *Phishing e ingeniería social*
- *Tecnología inalámbrica*
- *DRPs*
- *Monitoreo y administración de redes*

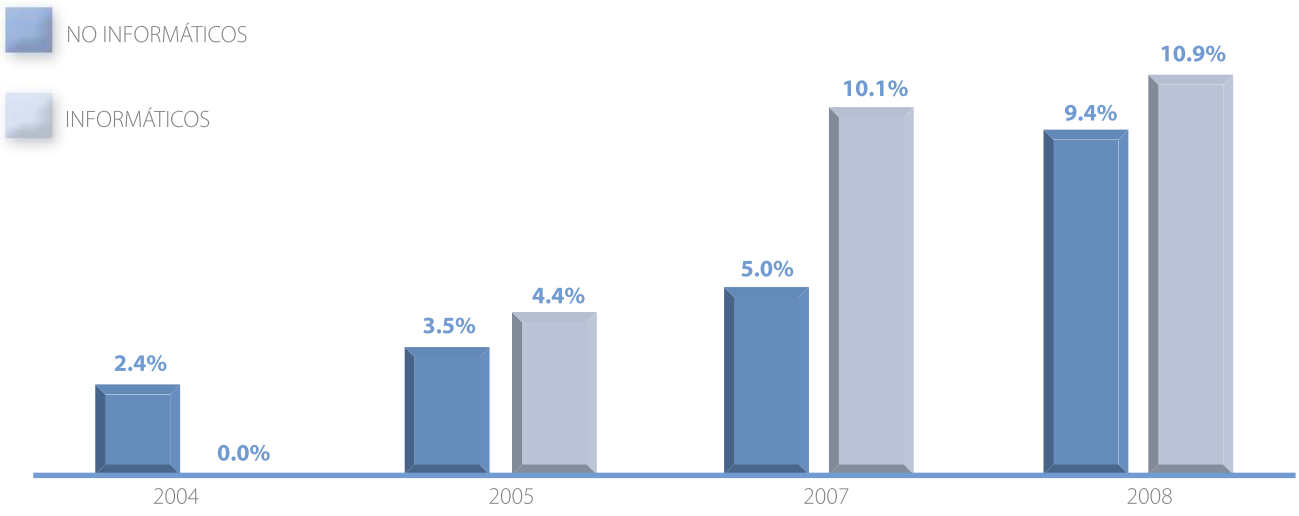
Fotografía: Doug Olson / Fotolia.com

Ambos grupos de entrevistados, en su mayoría, mostraron interés por conocer más acerca de Avances y Tendencias Tecnológicas y sobre Seguridad en Informática en General.

En cuanto a los otros conceptos, el interés de ambos grupos es marcadamente distinto. A pesar de que los dos perfiles mencionaron tener cierto interés en todos los temas, los usuarios No-Informáticos quisieran profundizar sobre algunos aspectos, en mayor medida que los Informáticos, y viceversa. A continuación mencionamos algunas de las principales diferencias.

El rubro de Políticas y Procedimientos sigue estando bajo, en el interés de los entrevistados en general. Sin embargo ha mantenido una tendencia creciente desde 2004, como puede apreciarse en la Gráfica 12.

GRÁFICA 12



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.
2. Recabar la opinión de expertos y proveedores líderes de soluciones informáticas que operan en México, respecto de la situación actual de Seguridad en Informática en el país, 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 o telefónica, como auto-administrado y enviado por correo electrónico.

Relación de entrevistados

Empresa	Nombre	Puesto
Andresen y Asociados Consultores	Carlos Carranza Andresen	Director General
Asiste	Moisés Polishuk	Director
Atos Origin	Sergio Banuet	Director General
Bolsa Mexicana de Valores	Efraín Baldenebro Ortiz	Oficial de Seguridad de la Información
Cablevisión	Israel Madiedo Luna	CTO
Citigroup	Erika Mata Sánchez	Audit. Manager (Information Security Management)
Corporación Unisol	Mauricio Jessurun	Presidente
Grupo Financiero Banorte	Salvador Sierra Hernández	Director de Sistemas
Grupo Yves Rocher de México	María de Lourdes León Castillo	Directora de Sistemas
Fundación Ealy Ortiz, A.C.	Enrique Bustamante Martínez	Director General
ITESM, Campus Edo. de México	Ricardo González Vargas	Director de Seguridad Computacional
KIO Networks	Srikan Emmanuel Ruiz Mora	Coordinador del área de seguridad informática
Mattica	Andrés Velázquez	Director de Investigaciones Digitales
Microsoft	Francisco José Camargo Santacruz	Gerente de Proyectos, Enterprise Services
Secure Information Technologies	Mario Ureña Cuate	Director General
SeguriData Privada	Javier Alarcón Irigoyen	Director General
Universidad del Valle de México	Eduardo de Jesús García García	Director de Investigación e Innovación Tecnológica
Vera Abogados	Luis Vera Prendes	Socio Director

Resultados

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

El el ámbito general , casi de manera consensuada se diría: "México presenta rezagos importantes en materia de Seguridad en Informática". Esto se matiza, al haber diferencias significativas entre organizaciones empresariales y gubernamentales e inclusive, entre usuarios de sistemas informáticos o profesionales del ramo.

Principales rezagos

Algunos de los aspectos considerados como rezagos más significativos por parte de los entrevistados, fueron los siguientes:

- Existen huecos legales y de normatividad.
- No se ha logrado difundir una cultura de seguridad entre los usuarios de tecnología ni se tiene una actitud proactiva a nivel organizacional.
- México no ha logrado ser un país productor de soluciones tecnológicas. Aún son muy escasos el desarrollo y la investigación.
- La Dirección de la mayoría de las empresas, no ha identificado a la Seguridad en Informática como una actividad estratégica del negocio.

OBSERVACIONES MÁS RELEVANTES
"La delincuencia organizada también genera investigación y constantemente está buscando la forma de saltar estas mallas de seguridad informática y logran, por diversos medios, engañar al cliente dándoles acceso a servicios apócrifos, los cuales no son controlados… voltean a ver a países en donde las regulaciones respecto de la seguridad informática prácticamente no existen".
"Tendemos a ser reactivos y tratar de minimizar el impacto una vez que nos ocurre algo".
"Tenemos mucho que aprender y madurar, pues todavía en gran parte de las empresas mexicanas se piensa que la seguridad es "problema" del área de Sistemas, además de considerar a la seguridad como un "lujo", algo en lo que invertiré sólo si me sobra dinero, si ya me pasó algo o si me lo pide alguna regulación, por lo que sólo se implementa lo necesario para cumplir".
En México aún nos hace falta ver a la seguridad como: • Un facilitador para hacer negocio. • Una inversión. • Algo que en lugar de generar gasto ayudará a reducir pérdidas cuando un evento desfavorable ocurra.
"En un nivel intermedio, hay empresas que han tomado con responsabilidad el tema y forma parte de su estrategia corporativa, hay otras que no tienen todavía una conciencia del impacto de la misma en su negocio. En la gente en particular, pienso que se ha generado mayor conciencia en los últimos años".
"No se ha podido crecer en este rubro en la misma proporción, en relación con el acelerado crecimiento en el uso de la tecnología por parte de la población en general de nuestro país".
"Como usuarios finales, que los mexicanos tenemos muy poca cultura de la seguridad, estamos poco informados y solemos ser confiados, por lo que podemos caer fácilmente en ataques de ingeniería social".
"Después de Brasil y Chile, podríamos considerar que México es el país latinoamericano que más recursos ha estado invirtiendo en materia de seguridad informática".
"Debe destacarse los esfuerzos y las inversiones realizadas por los sectores bancario y de telecomunicaciones para reforzar sus sistemas internos de protección en contra de la vulnerabilidad de las infraestructuras de TIC en el país".
"Con la publicación de la norma internacional ISO-27001 se identifica un incremento en el interés de empresas gubernamentales, financieras, educativas, manufactureras y de servicios, hacia el tema de la seguridad de la información desde un punto de vista más gerencial".
"La administración de la continuidad del negocio es un tema en donde México se encuentra en un nivel por debajo de lo esperado".
"A pesar que cada día hay más información sobre estos temas, no se le da la importancia requerida para las organizaciones medianas y pequeñas".

Principales progresos

- Cada vez más se cuenta con personas capacitadas de primer orden, en el país.
- La figura del Oficial de Seguridad empieza a ser cada vez más frecuente, al menos en organizaciones grandes.
- Los grandes corporativos y el gobierno, empiezan a ser más conscientes de la importancia de contar con programas específicos de Seguridad en Informática y de promover buenas prácticas al interior.

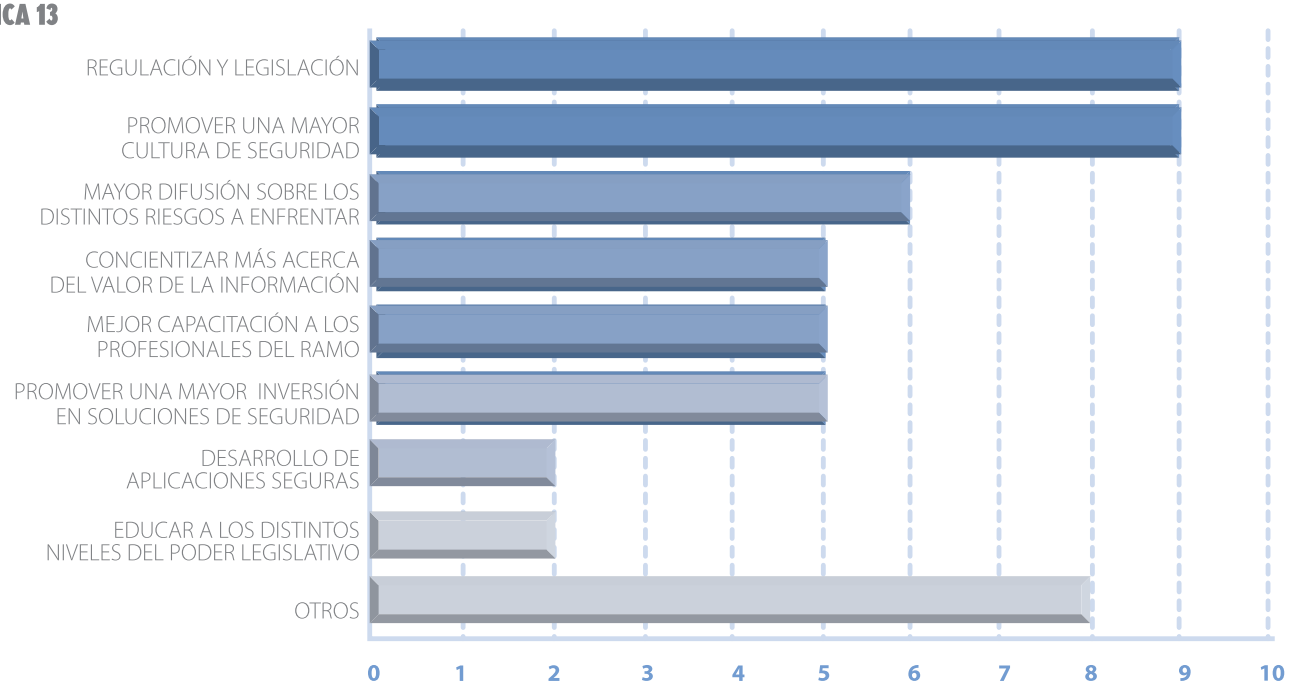
En México aún nos hace falta ver a la seguridad como:

- ***Un facilitador para hacer negocio.***
- ***Una inversión.***
- ***Algo que en lugar de generar gasto ayudará a reducir pérdidas cuando ocurra un evento desfavorable.***

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

Las respuestas codificadas de todos los entrevistados pueden observarse en la Gráfica 13.

GRÁFICA 13



En los últimos años, ha crecido la preocupación por los huecos que existen a nivel jurídico respecto del uso de tecnología y, de manera especial, en el uso de Internet. Si bien éste ha sido un rubro mencionado en todos los estudios anteriores, resalta en esta ocasión el número de menciones que hacen referencia a estas deficiencias. Por un lado, existe una percepción acerca de que quienes tienen a su cargo la labor legislativa en la materia, no cuentan con los conocimientos suficientes como para llegar a esquemas regulatorios prácticos, efectivos y equitativos. No hay penalizaciones tangibles y específicas para los delincuentes informáticos y, en algunos, en donde hay interacción entre organizaciones para el intercambio de información, de productos o servicios, vía electrónica,existe poca claridad en cuanto a quién responsabilizar, bajo qué circunstancias, en un caso de fraude cibernético.

Asimismo, se percibe que los esfuerzos por crear una cultura de Seguridad en Informática, tanto a nivel personal como de empresa e institución, han sido insuficientes. Se deben incrementar los esfuerzos en materia educativa (a nivel de educación formal) y de capacitación, así como dar mucho mayor énfasis a la difusión oportuna de riesgos.

El rubro de "Otros", se compone de las respuestas que sólo fueron mencionados por uno solo de los entrevistados (fx=1). Éstas son las siguientes:

- Creación de áreas formales de seguridad computacional
- Fomentar más el análisis de riesgos
- Incluir aspectos de Seguridad en Informática en los programas educativos
- Mayor cobertura de comunicaciones
- Mayor difusión sobre los últimos avances tecnológicos en la materia
- Promover la actualización de los equipos protegidos
- Promover una industria unificada de seguridad
- Protección del patrimonio de las personas

"Debe existir un marco legal que ampare los derechos de los usuarios de la información, fomente la preocupación tanto de proveedores como consumidores de servicios y penalice adecuadamente al infractor".

OBSERVACIONES MÁS RELEVANTES
"Debe existir un marco legal que ampare los derechos de los usuarios de la información, fomente la preocupación tanto de proveedores como consumidores de servicios y penalice adecuadamente al infractor".
"Es necesaria una mayor capacitación del personal responsable de vigilar y actuar ante delitos informáticos, quienes muchas veces no tienen la formación adecuada para hacer pesquises informáticas, forénsica o siquiera alguna preparación de *hacker* ético".
"Se requiere, principalmente: •"Un marco regulatorio que dirija esfuerzos a una cultura de seguridad y prevención, no hacia esquemas reaccionarios que atacan síntomas y no causas raíz. •"Fomentar una cultura de seguridad (awareness) basada en la prevención desde los más altos niveles de las organizaciones •Análisis de riesgos que permitan identificar y conocer todos los procesos de negocio *front, middle* y *back office*".
"Formalizar la educación tecnológica en materias de seguridad informática, para que las nuevas generaciones piensen en la seguridad como el día a día de los avances tecnológicos; que no lo vean como un tema separado, sino integrado en la tecnología misma".
"Incrementar la cultura de respuesta a incidentes, respuesta a emergencias, manejo de crisis, recuperación en caso de desastre y continuidad del negocio".
"Es de suma importancia que los usuarios conozcan las amenazas que existen, las políticas de seguridad de la empresa y, principalmente, que se apeguen a ellas".
"La empresa debe de invertir en la seguridad de sus sistemas tomando en cuenta el valor que la seguridad de IT ofrece a la compañía, más que en un Retorno de la Inversión".

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

Entre los retos mencionados con mayor frecuencia, se encuentran los siguientes:

- Entender la Seguridad en Informática como una parte estratégica del negocio y de la operación de la organización.
- Incrementar la inversión en el rubro.
- Promover una cultura de seguridad hacia el interior de la organización, a través de mayor difusión y capacitación.
- Creación y seguimiento de políticas y procedimientos bien establecidos y bien comunicados.
- Implementación de estándares internacionales.
- Ofrecer servicios transaccionales seguros a sus clientes.
- Mantener actualizada su plataforma tecnológica.
- Considerar con mayor detenimiento las opciones de *"Outsourcing"*, ya que pueden facilitar el obtener alta tecnología a costos accesibles

Principales retos de los proveedores de *hardware* y *software*, en materia de Seguridad en Informática

Una demanda recurrente, es que los fabricantes de soluciones tecnológicas tomen conciencia de que la Seguridad de la Información debe ser parte intrínseca de su producto. Sea *software* o *hardware*, el producto debe incluir elementos seguros desde su diseño, ya sean herramientas de actualización permanente, utilidades de monitoreo, etc.

Entre otras de las demandas más mencionadas, están las siguientes:

- Hablando concretamente de los comercializadores de soluciones e integradores, hace falta que estén mejor capacitados y conozcan a profundidad los productos que manejan.
- Que no sólo se dediquen a la venta de equipos y *software*, sino que ahonden más en la consultoría respecto de Seguridad de la Información.
- Que sus productos cumplan con todos los estándares necesarios y estén desarrollados bajo las mejores prácticas.
- Que los mecanismos de seguridad sean fáciles de manejar y comprensibles para los usuarios.
- Que siempre estén a la vanguardia en esta materia.

OBSERVACIONES MÁS RELEVANTES
"Crear mecanismos y piezas que ya integren seguridad implícita, así como mecanismos de autodestrucción en caso de violación; por ejemplo, en temas como tarjetas con chip, que éste se bloquee cuando se intenta leer cierta información especial, o cajeros que quemen o manchen el efectivo en caso de apertura de caja, quemar directamente los certificados de las empresas en dispositivos como POS o Kioskos, etc."
"Entender que las soluciones incluyen *hardware, software* y servicio; por lo que hay que ver sus productos como habilitadores".
"Desarrollar productos que cumplan con los requisitos de salvaguarda de la información, con la calidad y mecanismos de protección adecuados. Cuando se habla de calidad, implica hacer las cosas bien a la primera y no tener un mercado de "parches y actualizaciones" que pudieran entregar desde el inicio".
"Diseñar y desarrollar productos cumpliendo con las mejores prácticas y/o estándares de desarrollo en temas de seguridad, control de calidad, verificaciones de código, manuales, soporte, etc. Esto impacta en los tiempos de salida de productos y costos de producción, pero ofrece un grado de confiabilidad".
"Convertirse en socios tecnológicos de sus clientes para conocer a fondo las necesidades que éstos tienen y así poder dimensionar, implementar y actualizar los procesos y herramientas que se refieren al área de seguridad".
"Ver el tema de seguridad como una parte propia de la tecnología que se entrega, no verlo como algo adicional".
"Necesitan ofrecer herramientas más sofisticadas, de fácil actualización e igualmente que su uso no enfrente una resistencia al cambio dentro de las organizaciones".
"Tratar de incorporar en sus equipos y programas, herramientas, dispositivos y rutinas que permitan monitorear".
"Probar sus aplicaciones y someterlas a rigurosos análisis para detectar posibles vulnerabilidades o huecos de seguridad, antes de ofrecerlas al cliente".
"Liberar y notificar de manera oportuna los parches de seguridad en caso de ser necesarios".
"Reducir la brecha que existe entre las nuevas tecnologías de seguridad con respecto al costo de las mismas".

"Ver el tema de seguridad como una parte propia de la tecnología que se entrega, no verlo como algo adicional".

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

La gran mayoría de los entrevistados coinciden en que la Seguridad en Informática debe formar parte de los programas educativos de todas las carreras a nivel profesional e inclusive inculcarse desde los niveles intermedios de educación (secundaria y preparatoria).

No es una cuestión de profunda especialidad o alquimia, sino una respuesta a la adopción de modos de vida altamente tecnificados y comunicados, de la población en general hoy en día.

Los contenidos bien podrían estar desarrollados de diferentes maneras para su fácil comprensión, al nivel que cada programa, cada carrera o especialidad, requiera.

En este sentido, es importante que las instituciones educativas no pierdan de vista la importancia de mantener actualizados sus programas, conforme los avances tecnológicos y la aparición de nuevos riesgos.

Asimismo se plantea la necesidad de que se creen asignaturas de mayor especialización sobre este tema, en las carreras relacionadas con tecnología y comunicación, inclusive a nivel de posgrado.

Se considera que la participación de estas organizaciones debe ser intensiva en cuanto a investigación y desarrollo de estrategias y herramientas de Seguridad en Informática

OBSERVACIONES MÁS RELEVANTES
"Generar una cultura de legalidad y protección de la información educando a las nuevas generaciones sobre la importancia de mantener confidencial aquello que debe serlo y proteger los derechos intelectuales y de propiedad de los demás".
"Desarrollo de programas que contemplen todos los aspectos de la seguridad informática. Que estos programas se actualicen constantemente y que se incluyan prácticas, eventos y actividades que den objetividad y realidad a los programas".
"Lograr establecer programas de trabajo conjunto con empresas e instituciones para conocer las necesidades reales que se tienen en materia de seguridad".
"Involucrar los temas de seguridad informática en todas las carreras, ya que en las nuevas generaciones todos son usuarios de tecnologías de la información".
"Educación formal sobre el tema. CSO como una rama de especialización de las carreras informáticas, con posibilidad de obtener certificaciones".

"Involucrar los temas de seguridad informática en todas las carreras, ya que en las nuevas generaciones todos son usuarios de tecnologías de la información".

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

Más allá de la difusión de noticias relacionadas con eventos de inseguridad y casos sufridos por personas e instituciones (sin minimizarlas como ejemplo de riesgos latentes), se considera que los medios de comunicación deben tener una función orientadora que apoye los esfuerzos de las entidades educativas. Se menciona la orientación al público en general acerca de los diferentes riesgos, vulnerabilidades y amenazas, complementando esta difusión con recomendaciones concretas de prevención y control que permitan minimizar los ataques, haciendo énfasis en las situaciones vigentes más comunes.

La creación de conciencia y el fomento de una cultura de Seguridad de la Información, es una de las principales funciones mencionadas, a desempeñar por este tipo de organizaciones.

También se menciona "la forma" en la comunicación, como uno de los aspectos que deben ser cuidados por la mayoría de los comunicadores que hablan sobre el tema. La información debe ser correcta, fidedigna, confiable, fácil de entender y sin amarillismo.

OBSERVACIONES MÁS RELEVANTES
"Apoyar el conocimiento y concientización en temas de seguridad de la información, homogeneizando los conceptos de seguridad".
"Ser responsables en el manejo de la propia información, favoreciendo una educación basada en la prevención y no en la corrección y crítica, que por sensacionalista quizá es más vendible, pero no soluciona los problemas de raíz".
"Informar de manera veraz los temas de seguridad, buscando siempre el soporte de personal que cuente con bases sólidas para poder emitir su punto de vista, ya que hay muchos charlatanes en el medio".
"Mejorar la cobertura a los eventos de seguridad de la información, así como a los trabajos de investigación desarrollados por universidades y asociaciones".
"A nivel medios impresos especializados hay ya suficiente difusión, es necesario incorporar información muy orientada a despertar conciencia en foros y en medios impresos dirigidos a la alta dirección".
"Desarrollar campañas informativas en contra de la piratería de *software*".

"Apoyar el conocimiento y concientización en temas de seguridad de la información, homogeneizando los conceptos de seguridad".

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

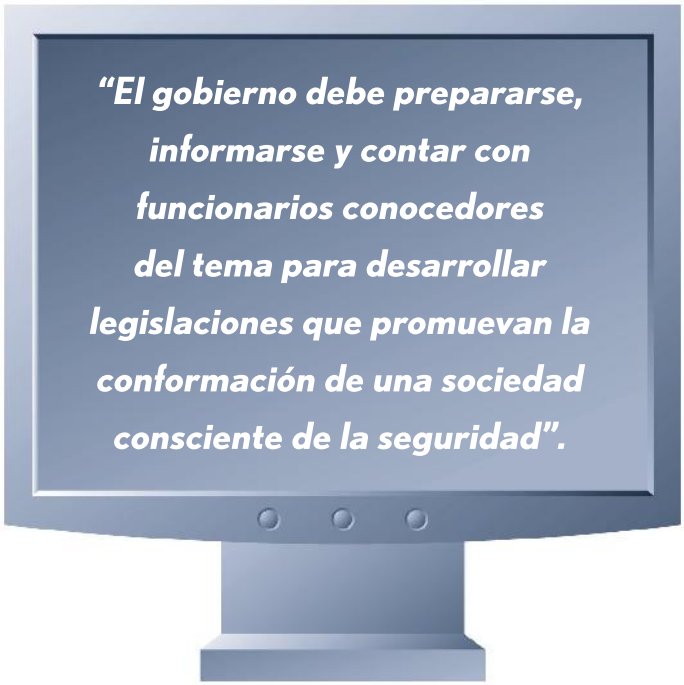
El establecimiento de marcos jurídicos y legales es considerado prioritario, encaminado a resolver algunas de las principales problemáticas, como son:

- Protección de la información, con transparencia y respeto a la privacidad.
- Sanción a los delitos informáticos.
- Protección de la propiedad intelectual y derechos de autor.

En este sentido, no sólo se requiere que exista la normatividad y legislación claras, sino también que el mismo gobierno soporte la infraestructura para poder llevar a cabo su adecuada implementación y continuidad.

El otro aspecto que más sobresale como reto a resolver de manera indispensable, es que las entidades gubernamentales que brindan servicios a la ciudadanía vía Internet, garantice la seguridad de sitios y de sus aplicaciones.

OBSERVACIONES MÁS RELEVANTES
"La adhesión a convenios como el de Budapest para el combate al cibercrimen, donde se permitirá obtener de parte de las empresas, proveedores y del mismo gobierno, las herramientas para realizar las investigaciones necesarias".
"Instrumentar una política de protección de la información y derechos "digitales" de las personas (no sólo de propiedad intelectual, también de datos personales, bancarios, etc.).
"Desarrollar nuestros propios estándares y modelos de seguridad nacionales".
"El gobierno debe prepararse, informarse y contar con funcionarios conocedores del tema para desarrollar legislaciones que promuevan la conformación de una sociedad consciente de la seguridad".
"Fomentar el compartir experiencias en el área".
"Apoyar en el proceso de culturizar a la ciudadanía en temas de seguridad informática".
"Las entidades de gobierno deben procurar y promover el uso de buenas prácticas y estándares de control y seguridad de la información".



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

Andresen y Asociados Consultores
Carlos Carranza Andresen
Director General

"En Andresen y Asociados, nos mantenemos al día en todo lo referente a Informática (incluyendo la seguridad), para poder ofrecer a nuestros Clientes soluciones confiables y orientarlos sobre los riesgos a los que están expuestos, muchas veces sin saberlo, y cómo pueden evitarlos".

Atos Origin
Sergio Banuet
Director General

"Contamos con una línea de servicio especializada en Seguridad Lógica, donde apoyamos a clientes fundamentalmente en los sectores financiero y público. Sin embargo, no estamos inscritos a ninguna asociación y no estamos haciendo nada por esta industria, por no ser una línea de servicio estratégica para nosotros".

Cablevisión
Israel Madiedo Luna
CTO

"No sólo basta con la implementación de tecnología de punta para el aseguramiento de los medios informáticos. El contar con el asesoramiento de expertos y la continua revisión de métodos y procedimientos, es clave para apoyar las iniciativas en este rubro. Esto no queda sólo, en el caso de empresas proveedoras de acceso a Internet, a nivel interno de la corporación. Se debe hacer extensivo a los clientes finales. Nos encontramos en esa etapa y buscamos que se propaguen de manera positiva los temas afines a la seguridad en todo ámbito informático".

Citigroup
Erika Mata Sánchez
Audit. Manager (Information Security Management)

- "Mucha difusión con propósitos de concientización hacia el público en general y clientes.
- "Fortalecimiento de controles en los diferentes procesos de negocio, involucrando todos los niveles de la organización a nivel local, regional y global, incluyendo capacitación constante en diferentes temas de seguridad informática y de procesos de negocio.
- "Fomento de una cultura de *Self Assessment* que permita tomar medidas preventivas y detectar incidentes en etapas tempranas de ocurrencia.
- "Fortalecimiento de las áreas de auditoría en temas de seguridad informática, con un enfoque de riesgo".

Corporación Unisol
Mauricio Jessurun
Presidente

"Nuestra empresa ha mejorado mucho la cultura de seguridad, mediante una difusión interna oportuna y con las evidencias del caso acerca de los riesgos de ejecutar programas de fuentes no conocidas. Una persona que "infecta" a la red es inmediatamente boletinada a toda la organización, explicando qué hizo y los efectos de hacerlo. Esto ha permitido que hace ya varios meses o incluso años, hayamos estado exentos de aspectos nocivos a la organización en materia de seguridad en TI, al haber mejorado la cultura de calidad en estos temas".

Grupo Yves Rocher de México
María de Lourdes León Castillo
Directora de Sistemas

"Inversión en auditorías de IT cada año e implementación de planes de acción a nivel empresa, para dar importancia a la seguridad informática tanto en inversión, como en entrenamiento y cultura dentro de la organización".

ITESM, Campus Estado de México
Ricardo González Vargas
Director de Seguridad Computacional

"Educar a los alumnos que van a salir a trabajar a las empresas, acostumbrándolos a desempeñarse en ambientes seguros".

KIO Networks
Srikan Emmanuel Ruiz Mora
Coordinador del área de seguridad informática

"Día con día se generan nuevos virus informáticos, surgen nuevas vulnerabilidades en el sistema operativo o nuevos tipos de ataques, por lo que la arquitectura de seguridad diseñada para un cliente se vuelve obsoleta. Una de las funciones que el SOC de KIO ofrece, es la de verificar que el perímetro de seguridad de nuestros clientes se encuentre protegido ante estas nuevas amenazas, lo cual logramos con la implementación de Planes de Mejora Continua (PMC).

"Los ingenieros del SOC de KIO Networks se encargan de validar que las políticas configuradas en los equipos de seguridad perimetral estén bien definidas y no provoquen algún hueco en la seguridad. Asimismo, se realizan escaneos de vulnerabilidades a los equipos antes de entrar a producción para validar que éstos entran a producción en forma segura.

"Con esta forma de trabajo buscamos ser lo más proactivo posibles en la seguridad de la información de nuestros clientes, con lo que obtenemos su confianza y satisfacción".

Mattica
Andrés Velázquez
Director de Investigaciones Digitales

"En Mattica, al ser el primer laboratorio de cómputo forense en América Latina, se han alcanzado varios logros:

- "Atendió a un promedio de 20 a 25 investigaciones digitales al mes, de diferentes rubros.
- "Participó en el evento 'Creando un Consejo Nacional para la Seguridad en Línea', organizado por Telmex para convocar a la Sociedad Civil a promover un ambiente de navegación en Internet más seguro, en beneficio principalmente de los niños y los adolescentes.
- "Capacitó a 400 elementos de las fuerzas públicas de diversos países de América Latina, junto con Internet Safety, una iniciativa de Microsoft Latinoamérica
- "Ha dado conferencias a nivel nacional e internacional para la divulgación de los temas relacionados con los delitos cibernéticos.
- "Apoya con conferencias y pláticas acerca de cómo navegar y mantener la seguridad en Internet para menores de edad y adolescentes".

Microsoft
Francisco José Camargo Santacruz
Gerente de Proyectos, Enterprise Services

"Un compromiso de Microsoft a largo plazo es el tema de seguridad computacional, tanto en una estrategia de herramientas, cultura y soluciones para personas como para empresas. Esto se observa en la línea de soluciones personales y empresariales, como *OneCare y Forefront*, entre otros."

Secure Information Technologies
Mario Ureña Cuate
Director General

"Nuestra empresa participa activamente en programas de concientización, entrenamiento y educación, con el fin de mejorar el conocimiento general sobre el tema de la seguridad de la información.

"Participamos activamente en asociaciones relacionadas con la seguridad de la información, en proyectos de investigación y definición de prácticas y estándares de seguridad de la información.

"Promovemos el uso de mejores prácticas y estándares de seguridad de la información, así como el cumplimiento con leyes y regulaciones.

"Contamos con un estricto programa de capacitación y certificación para nuestros consultores encargados de desarrollar proyectos relacionados con la Seguridad de la Información.

"Apoyamos el desarrollo de estudios relacionados con la seguridad de la información, con el fin de conocer el estado que guarda actualmente en nuestro país".

SeguriData Privada
Javier Alarcón Irigoyen
Director General

"Creamos soluciones para dar seguridad a la información involucrada en los procesos de negocio. La tecnología que desarrollamos se basa en estándares internacionales y en algoritmos criptográficos sólidos.

"Garantizamos la Confidencialidad, Integridad, Autenticidad y Autoría de la información en medios electrónicos, utilizando tecnología en temas de Certificación Digital, Firma Electrónica Avanzada y Criptografía en general".

Universidad del Valle de México
Eduardo de Jesús García García
Director de Investigación e Innovación Tecnológica

"Favoreciendo programas de educación respecto a la seguridad informática. Fomento de una cultura de legalidad y uso correcto de la información, a nivel general de la comunidad de nuestra empresa, pero también capacitando a los profesionales del ramo a través de congresos, seminarios y diplomados en el área."

IV. CONCLUSIONES DE LA INVESTIGACIÓN

Panorama general

Al observar las tendencias generales, es claro que sigue avanzando la consciencia de seguridad en informática en nuestro país. Sin embargo, este avance es más lento que el que sería deseable. Sigue siendo muy bajo el número de personas que entiende que la seguridad en informática está íntimamente ligada a los procesos y a las políticas.

El robo de identidad ha seguido cobrando importancia a través de los años, en la mente de todos los usuarios de tecnología.

Si bien el conocimiento acerca de estándares de seguridad se a incrementado, sigue habiendo mucha confusión entre los usuarios respecto de cuáles son estos estándares. Se confunden estándares de calidad o financieros, con estándares de seguridad en informática, y aún así, sólo el 10% de la muestra global afirmó conocer algún estándar. Dentro de este rubro, se notó una caída importante en el porcentaje de Informáticos que conocen algún estándar. La proporción de Informáticos que admitió no conocer ninguno, subío del 69% en 2007 al 80% en 2008.

El aumento en la conciencia respecto de la Seguridad en Informática aumentó ligeramente de 2007 a 2008, lo cual es positivo, pero se esperaba y era deseable que fuera mayor el incremento.

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

Coincidencias

Ambos grupos están más conscientes del incremento en los riesgos que se derivan de ataques que buscan generar algún beneficio para quien lo lleva a cabo, en lugar de causar un daño por el daño mismo de manera aleatoria. De ahí que las amenazas consideradas de mayor riesgo sean aquéllas en donde existe una persona detrás, con la intención de obtener una ganancia, principalmente económica, como consecuencia del ataque. Esta percepción coincide con lo que está ocurriendo a nivel mundial, en donde cada vez se ven más ataques con un claro objetivo de obtener información para uso fraudulento (sobre todo bancaria) y ya no son tan comunes, como lo fueron hace algunos años, los virus que simplemente borran datos o congelan computadoras.

Diferencias

Resulta evidente que la Transmisión Segura de Datos es mucho más tomada en cuenta por el grupo de Informáticos que por el de No-Informáticos. Considerando que en el mundo actual de informática casi toda la información se transmite en algún momento, es claro que este rubro debe ser considerado por todos los usuarios, como uno de lo más importantes. El grupo de los No-informáticos percibe que la seguridad en informática es un tema muy importante en las empresas en las que laboran, en tanto que para los Informáticos éste no es el caso. Resulta muy interesante esta diferencia de percepción, sobre todo si se considera que hay casos en donde ambos usuarios laboran en una misma empresa.

Para los Informáticos resulta ser prácticamente igual de importante el nivel de seguridad ofrecido por un producto, que la confianza en el proveedor del mismo, mientras que para los No-Informáticos el nivel de seguridad del producto es el rubro más importante a considerar.

Principales demandas por parte de los usuarios

Tanto los Informáticos como los No-Informáticos coinciden en solicitar a los proveedores más servicio: Asesoría, capacitación y soporte técnico, más allá de las características del producto como tal, son el tipo de cosa que ambos usuarios piden a los proveedores de tecnología.

Principales retos de las organizaciones en México

Al igual que en años anteriores, el marco regulatorio y legal sigue siendo percibido como el mayor problema para el país. Si no existe este marco jurídico, es difícil que pueda lograrse una verdadera cultura de Seguridad en Informática.

Difusión y promoción de una mayor cultura de seguridad sigue siendo un reto que el país no ha podido superar, a pesar de que se notan esfuerzos notables en este sentido.

Falta entender la Seguridad en Informática como una parte estratégica del negocio y de la operación de la organización.

Nuevamente surge el reclamo a proveedores de tecnología de entender que la seguridad debe ser parte inherente al producto, no algo adicional. Este tema es recurrente en estudios anteriores.
Los esfuerzos educativos deben ser horizontales y verticales. Horizontales en el sentido de que todas las carreras y niveles escolares deben contemplar aspectos de seguridad en informática y verticales en la creación de especialización en el tema.

Un concepto muy interesante que surge este año, es la idea de que los medios de comunicación no sólo deben difundir los aspectos verídicos de los acontecimientos relacionados con seguridad en informática, sino que también tienen una labor importante de homogenizar conceptos, lo cual ayudará evidentemente a su comprensión por parte de una mayor parte de la población.

El gobierno, además de sus funciones de protección a la información y sanción de los delitos, debe preocuparse por desarrollar funcionarios competentes en el tema, que apoyen la creación de legislación coherente para el mundo actual, en este rubro.

Principales rezagos en el país

- Existen huecos legales y de normatividad.
- No se ha logrado difundir una cultura de seguridad entre los usuarios de tecnología ni se tiene una actitud proactiva a nivel organizacional.
- México no ha logrado ser un país productor de soluciones tecnológicas. Aún son muy escasos el desarrollo y la investigación.
- La Dirección de la mayoría de las empresas, no ha identificado a la Seguridad en Informática como una actividad estratégica del negocio.

Principales avances en el país

- Cada vez más se cuenta con personas capacitadas de primer orden, en el país.
- La figura del Oficial de Seguridad empieza a ser cada vez más frecuente, al menos en organizaciones grandes.
- Los grandes corporativos y el gobierno, empiezan a ser más conscientes de la importancia de contar con programas específicos de Seguridad en Informática y de promover buenas prácticas al interior

V. ARTÍCULOS SOBRE SEGURIDAD EN INFORMÁTICA

CUANDO EL RÍO HACE RUIDO ES PORQUE AGUA LLEVA, Y EN ESTE ESTUDIO DE PERCEPCIÓN 2008, APLICA MUY BIEN.

Por Raúl Aguirre
CISSP,CISA,CISM
Presidente de la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI)

Introducción

Es harto sabido que este tipo de indicadores de comportamiento de la Seguridad Informática es necesaria para la toma de decisiones, que no hay suficiente información y prácticas en México que busquen contar con ellas, pese a esfuerzos ingentes por contar con ello, o lo que existe son comportamientos de otros ambientes y presentan sesgos importantes a nuestro ambiente y necesidad.

A nombre de ALAPSI y de la Mesa Directiva, nos complace haber formado parte de este logro que JFS y las empresas patrocinadoras han realizado, el cual nos integra en varias actividades para su logro, para poder continuar en este proceso de difusión y definición de reflexiones y propósitos que sustentan sus eventos y actividades.

Nuestro reconocimiento y agradecimiento a todos los miembros e invitados por participar en la entrega de esta información, no sólo de ALAPSI, sino de todas las firmas que lo patrocinan.

Señores miembros y participantes en la Mesa Directiva de ALAPSI, éste es un llamado a la acción, a la acción en equipo, sumando nuestros esfuerzos con nuestra experiencia y tiempos.

Mejorar las obtención de estadísticas

Entre las experiencias logradas es donde tenemos que buscar fuentes para reducir los riesgos y ganar más confianza en los resultados obtenidos.

Tenemos que ejecutar la obtención de esta información, con medios más efectivos para que los Directivos y Profesionales expertos, sean o no informáticos, proporcionen información acerca de su experiencia, sin riesgos a su institución o a su persona. Hay dudas y razones por política interna de abstención. Encontremos y apliquemos esos medios.

Entre las propuestas que hacemos está:

- El definir un proyecto y designar a los responsables de ALAPSI que quieran participar en este esfuerzo, coordinado por JFS.
- Involucrar a profesionales acreditados por JFS, bajo reglas bien puestas en la obtención de esta información.
- Participar en la definición de los propósitos de investigación.
- Participar con todas las instituciones posibles.

Proyectos de ALAPSI relacionados con este estudio, que nos motivan a su realización:

Relativo a la pregunta 3. "Amenazas de mayor riesgo":

- Organizar eventos de Concientización, ejercer la ética profesional y lograr el control de las amenazas, a los 3 niveles funcionales (E,T,O), para iniciar y mantener el programa de Seguridad.
- Promover capacitación a las empresas para lograr su plan de 'Awareness'.

- Promover capacitación a las empresas para homologar conceptos y prácticas en las tareas, tanto tácticas como operativas.

Relativo a la pregunta 10.- "Qué más le gustaría conocer", considerar las resupuestas como temas en los eventos de ALAPSI:

- Avances y Tendencias tecnológicas, para un desayuno o tertulia.
- Curso de inducción y homologación de conceptos, el cual se estará implementando para el segundo semestre de 2008. Este curso estará orientado a las personas con funciones tácticas y operativas de seguridad informática (administradores de BD, aplicaciones, Manejo de Incidentes, Operación de Fw, Antivirus, IDS, Cifrado de Información, IPS, Control de Accesos, Elaboración, implantación y Supervisión de Normas y Procedimientos de Seguridad).
- Promover pláticas de concientización a los niveles Estratégicos, Tácticos y Operativos, para iniciar con el programa de seguridad en la institución.

Las preguntas orientadas a los servicios y las herramientas:

- Invitar a apoyar a las empresas en la relación con ALAPSI, sin entrar en conflicto con la MISIÓN Y VISIÓN.
- Hacer sinergias o buscar patrocinios con proveedores de productos y/o de servicios de Seguridad, con reglas y controles para evitar conflictos de interés con ALAPSI.
- Promover el patrocinio para laboratorios con herramientas de diferentes proveedores.
- Saber relacionar las herramientas con las metodologías, la normatividad y las prácticas de Seguridad internacionales.

Conclusiones según diferentes enfoques o necesidades

Enfoque estratégico: La direcciones de empresas y el comité de Seguridad

- Sigue siendo imperante el concientizar. En este sentido, ALAPSI es una excelente opción para recibir resultados de plataforma sustanciales, para fundamentar la estrategia y las funciones de seguridad.
- Las empresas pueden apoyar a la ALAPSI, haciéndose miembros de la misma y participando en sus eventos.
- La Administración del Riesgo: los indicadores JFS son puntos a relacionar en los elementos de riesgo.
- Proyectos habilitadores para soportar la estrategia de Seguridad:
- La capacitación básica del CBK para: Las funciones estratégicas, la conciencia de la Alta Dirección y el comité de Segurdidad
- Capacitación para la definición de las funciones, roles y responsabilidades.
- Capacitación para la definición de Políticas y Normas.
- Capacitación para la definición de la estrategia de Seguridad Informática.

Enfoque táctico, quienes tienen la asignación de implementar las soluciones de Seguridad:

- Preparación para la identificación de soluciones.
- Preparación de Certificación de los Profesionales.
- Capacitación para definir y ejecutar el programa de Concientización y Entrenamiento, contar con las guías básicas y necesarias de protección de la información.
- Capacitación para elaborar normatividad, políticas, estándares, procedimientos y controles. Contar con un BCP/ DRP práctico.
- Capacitación para ejecutar procedimientos técnicos con las herramientas de seguridad, para fw, ids/ips, antivirus, control de accesos, procesos de escaneo y monitoreo, que se establezcan en las actividades operativas con los equipos de cómputo.
- Capacitación para definir el costo de la seguridad, indicadores de comportamiento y de logro de objetivos de control.
- Capacitación para elaborar los procedimientos de los planes de continuidad.
- Capacitación para prepararse y definir el Sistema de Gestión de Seguridad.
- Capacitación para identificar qué acciones pueden o deben ser atendidas por externos y cuáles no.

Enfoque para las operaciones de seguridad

- Homologar conceptos y las tareas básicas operativas realizarlas con calidad, efectividad en cumplimiento de los estándares y controles establecidos.

CONCLUSIÓN DE LA PRESIDENCIA DE ALAPSI: Este estudio refuerza nuestra estrategia ya definida y las acciones que estamos aportando a la membresía. FELICIDADES!

Administración de la Seguridad

Por Francisco Argüelles Arredondo
Sr. Consultant
CA Software de México

Transforming
IT Management

¿Alguna vez se ha preguntando qué es lo más importante de una organización?, es decir, qué parte de la misma es la que, si desapareciera, la organización detendría sus operaciones. La pregunta la formulo porque muchas veces, sin contar el factor humano, las empresas tienen desafíos cada vez más difíciles que superar en cuanto a la administración de la tecnología.

Si podemos tomar una pequeña parte de lo que esto conlleva, si podemos delimitar el texto a la Administración de la Seguridad, es decir, ya no sólo definir qué es lo que tenemos que hacer para proteger la información de la organización, considero que desde hace ya unos años ha quedado claro que el uso de herramientas como antivirus, *firewalls,* bloqueadores de *Spam*, entre otros, han sido adoptados por las empresas de manera continua. Sin embargo, dentro de un entorno multifacético y aunado a la complejidad del uso de la misma tecnología, los requisitos regulatorios, las presiones del mercado y, en este caso, las amenazas a la seguridad, existe una parte de la interacción de los usuarios con la información que no ha sido totalmente aceptada por los administradores de sistemas.

El aspecto económico, como la disminución de costos, el mejoramiento de sus propios servicios y la innovación para conseguir mejores resultados, son aspectos que no deben de ninguna manera dejar de relacionarse con la tecnología.

Los principales objetivos de la Administración de la Seguridad, aunque no son los únicos, incluyen:

- La disponibilidad de los recursos
- La integridad de la Información
- Confidencialidad de la información

Los servidores, los datos y los equipos de comunicaciones, deben de estar disponibles siempre, para lo cual es necesario prevenir todo aquello que podría interrumpir el servicio y controlar, en la medida de lo posible, los tiempos de interrupción cuando se encuentren debidamente planeados.

El problema radica en la falta de servicios, cuando éstos no son controlados debido a amenazas tales como, entre otras:

- *Malware*
- Intrusiones no autorizadas a los sistemas
- Falta de políticas y procedimientos relacionados con los servicios de la red
- Servicios innecesarios corriendo en los servidores
- Fallas en la programación de los sistemas hechos en casa
- Falta de parches a los sistemas operativos

Entonces, si tomamos en cuenta que no sólo las regulaciones son la única fuente de requisitos para tener en cuenta la administración de la seguridad, las empresas tienen también la responsabilidad de asegurar la protección adecuada de la infraestructura y los activos de información. Esto se traduce en nuevos requisitos operacionales no sólo para los departamentos de sistemas, sino para la alta gerencia también.

Dentro de este complejo entorno, y después de aceptar que la seguridad informática es un punto fundamental para la organización, se entiende también que la administración de identidades y accesos constituyen la primera línea de defensa contra las personas externas a la organización. La Administración de Identidades garantiza que una persona o proceso del sistema sea realmente lo que aparenta ser. Una vez que los mecanismos mediante los cuales se logra la identificación de manera convincente permiten el acceso a las persona que realmente lo necesita, se mitiga también el riesgo al limitar la exposición de la información, la ejecución de mecanismos de monitoreo para asociar eventos con usuarios específicos, además de administrar grupos de usuarios con similitudes dentro de los sistemas.

Esta administración de identidades, cuenta con tres elementos clave: el primero es la identificación del usuario, es decir, quién es la persona que necesita entrar a los sistemas; después, la autentificación de que quien se identifica sea quien dice ser, y por último, se verifica mediante la autorización que el usuario acceda a los sistemas que debe utilizar. Si tomamos en cuenta todos los aspectos anteriores, nos percataremos de que sólo son algunos de los problemas que enfrentan los administradores de sistemas y, más aún, a medida que pasa el tiempo, cada vez están más envueltos en la administración de algo que crece día con día. Ante esta perspectiva, sería bueno analizar cómo llevar a cabo la administración no sólo de la seguridad, sino también de toda la infraestructura computacional existente en la organización. Una herramienta o tecnología no resolverá el problema, la capacitación de los usuarios tampoco hará que una empresa sea más segura. Mantener la seguridad y administración de los sistemas demanda la coordinación planificada de múltiples tecnologías, personal de TI y administradores del negocio.

Francisco Argüelles Arredondo es Sr. Consultant en CA Software de México. Para mayor información, contactarlo en: *francisco.arguelles@ca.com*

Definiendo un modelo Pragmático para enfrentar exitosamente los retos de Seguridad Informática en México

Gilberto Vicente,
CISSP
Security Business Development Manager
Cisco Systems de México

Partiendo de que la tecnología es un componente fundamental en cualquier arquitectura o programa de seguridad, con frecuencia se me cuestiona respecto a lo que está sucediendo en el mercado y cómo la industria de Tecnologías de Información y Comunicaciones está reaccionando ante el entorno de inseguridad que enfrentamos. Todo esto con la intención de que los responsables de Seguridad de la Información puedan tomar decisiones estratégicas en la materia.

La intención de este artículo es documentar brevemente el escenario y proporcionar recomendaciones que permitan a las áreas responsables de seguridad, entender el entorno para llevar a cabo una correcta evaluación de planteamientos tecnológicos que los ayuden a mitigar riesgos en sus organizaciones.

Es necesario cambiar la fórmula

Hace algunos años el universo de ataques informáticos era muy pequeño, las organizaciones operaban de forma aislada y los medios o vectores que se utilizaban para vulnerar la seguridad de las empresas estaban muy acotados y eran casi siempre los mismos (email, web, etc.). Los ataques se manifestaban descaradamente inhabilitando e infectando PCs, redes, cambiando páginas web y/o afectando la operación de las empresas. En esos tiempos no era descabellado pensar en adquirir tecnología puntual que ayudara a identificar, prevenir y detener ataques en específico, en la medida en la que éstos tenían aparición. En general, era relativamente sencillo justificar proyectos de seguridad informática ante la alta Dirección.

Actualmente, el escenario es totalmente opuesto y resulta prácticamente imposible enlistar la cantidad de ataques informáticos que existen. Las empresas se apoyan en tecnologías de información que incrementan su competitividad y productividad, pero que al mismo tiempo incrementan exponencialmente la cantidad de puertas y ventanas en la empresa; los ataques son más sofisticados e incorporan mecanismos que les permiten permanecer ocultos para robar información, utilizando al mismo tiempo distintos vectores para vulnerar la seguridad. Se ha convertido esta situación en un tema caótico para las empresas, quienes naturalmente ven esto como una historia de nunca acabar en lo que a inversión en seguridad informática se refiere.

No se trata de vislumbrar un escenario fatalista, sino entender que lo que antes funcionaba, actualmente ha dejado de ser práctico y que los responsables de Seguridad de la Información tienen que replantear la estrategia que les permita posicionar Seguridad Informática como un tema de inversión y no de gasto dentro de sus empresas.

Retos para los responsables de Seguridad de la Información en México

•Identificar los drivers de negocio y posicionar la práctica de Seguridad como un habilitador en la organización.

Detener ataques informáticos es una actividad importante en la práctica de seguridad, pero por sí sola no podría considerarse un driver de negocio; se convierte en habilitador cuando incrementa la competitividad y rentabilidad en la entrega de nuevos servicios (Comercio en línea, Banca Electrónica, acceso remoto a usuarios de la empresa y socios de negocio, conexión inalámbrica dentro de la empresa, etc.), cuando representa ahorro en costos y apoya el cumplimiento con marcos regulatorios y/o estándares de Industria (Decreto de austeridad, circular única de la CNBV, PCI DSS, SOX, etc.) que norman el comportamiento de muchas empresas.

•Asumir una postura estratégica

Lograr un balance entre los servicios que la empresa tiene que entregar para alcanzar sus objetivos, con el nivel de riesgo aceptable y cumplimiento con marcos regulatorios, implica y demanda una postura estratégica. Si logramos documentar y vender el caso de negocio que la inversión en seguridad representa, estaremos dando un paso importante en la materia.
Atender de manera reactiva el escenario de inseguridad ha sido la práctica por excelencia, es decir, las empresas compran PCs con sistemas operativos y después evalúan y compran el antivirus que la protege, instalan o liberan servicios web y después implementan Firewalls, implementan VoIP, redes inalámbricas y posteriormente adquieren soluciones de Detección y Prevención de Intrusos para garantizar la seguridad y disponibilidad de los servicios, etc. Es precisamente esta práctica obsoleta la que naturalmente genera la percepción de que la Seguridad de la Información es un tema de gasto.

•Entender el entorno para llevar a cabo decisiones estratégicas

A partir de las demandas del mercado, la principales empresas de la industria de Tecnologías de Información y Comunicaciones han evolucionado, adquiriendo empresas de nicho o desarrollando soluciones propietarias que permiten integrar seguridad en cada uno de sus planteamientos tecnológicos. Se trata de un entorno de consolidación donde las empresas con productos o tecnología de nicho continúan haciendo sentido, pero como parte de un servicio o arquitectura; de forma independiente, se convierten sólo en parches que difícilmente justifican su existencia desde el punto de vista de negocio (costo de propiedad, retorno de inversión, etc.).

Recomendaciones para la correcta evaluación de Tecnología de Seguridad informática

•No evalúe sólo la capacidad de detener ataques

Detener ataques es lo más sencillo, ya que en la mayor parte de los casos la tecnología está diseñada exclusivamente para ello; sin embargo, es importante tener presente que en muchas ocasiones esas soluciones de seguridad, que son muy buenas deteniendo lo que consideran maligno, son incapaces de garantizar el desempeño de la red y de aplicaciones críticas, llegando en algunos casos al extremo de impedir servicios fundamentales en la organización (VoIP, aceleración de aplicaciones, acceso al web, etc.)

Hace algunos años era común hablar de un sacrificio en el desempeño para contar con cierto nivel de seguridad. En la actualidad esto es cuestión del pasado y es factible tener lo mejor de los dos mundos si se implementa la seguridad en el lugar y momento indicados.

•Demandar Seguridad como un adjetivo real en cada planteamiento de tecnologías de información

No todas son malas noticias. Si bien los ataques seguirán existiendo lo mismo que quienes pretenden vulnerar la seguridad de las organizaciones, actualmente es factible encontrar planteamientos de tecnologías de información donde la seguridad es un componente integrado o bien un servicio que acompaña la oferta; la tendencia es que, así como nosotros recibimos agua limpia de las tuberías, lo mismo podamos exigir a quien nos otorga el servicio de Internet, convirtiéndose en un servicio de Internet seguro, sistemas operativos seguros, redes inalámbricas seguras, comunicaciones unificadas seguras. La tecnología puntual seguirá existiendo, pero como servicio o como parte natural de una propuesta de TI que claramente le permitirá a la empresa ser más productiva, competitiva y segura.

Un ejemplo es cuando adquirimos un automóvil: éste viene acompañado del equipamiento que garantiza no sólo el servicio, sino la seguridad del pasajero. Como usuarios no tenemos que configurar los frenos ABS, bolsas de aire, etc. Por eso la siguiente vez que evalúe cualquier tipo de planteamiento tecnológico, cuestione la seguridad que dicho planteamiento trae consigo, no acepte respuestas como "lo ve después con su proveedor de seguridad y/o es ajeno a mi planteamiento".

•Evaluar las capacidades de ejecución de quien pretende responder a las necesidades de la empresa

Existen en el mercado cientos de compañías dedicadas a ofrecer soluciones puntuales de seguridad. Ha resultado en el pasado todo un negocio vender tecnología puntual, sin embargo, y como lo hemos comentado, el escenario ha cambiado y es factible encontrar muchas de esas funcionalidades que se promocionan como la panacea de forma independiente en la misma plataforma de conectividad, sistemas operativos, etc.

Cuestione la presencia en México (personas, distribuidores, tiempo en el mercado, etc.), la capacidad financiera, el futuro de la tecnología, niveles de servicio, investigue si su producto o servicio puede ser adquirido a través de Proveedores de Servicio de Internet (ISPs), alguna plataforma de TI (centro de datos, comunicaciones unificadas, redes inalámbricas, etc.).

Cisco Systems

Cisco Systems, compañía fundada en 1984 y con cerca de 40,000 empleados a nivel mundial, es la empresa líder en soluciones de conectividad y seguridad a nivel mundial.
Desde su fundación, Cisco se ha caracterizado por su constante innovación y por la entrega de arquitecturas seguras de red que responden a las necesidades de negocio de las organizaciones, lo que ha permitido alcanzar más del 38% de market share en seguridad en redes a nivel mundial.

La estrategia de Cisco, denominada "Redes Autodefensivas", ofrece una serie de arquitecturas que dan cumplimiento a las necesidades de seguridad de las organizaciones y que permiten cumplir con marcos regulatorios y/o mejores prácticas de Industria. A través de la oferta de Cisco, nuestros clientes pueden encontrar, en cada uno de nuestros planteamientos, la respuesta a sus necesidades de negocio con seguridad integrada, representando esto los mejores beneficios de costo de propiedad y retorno de inversión, lo que fomenta que la adquisición de seguridad se convierta en un tema estratégico para su organización.

Cisco cuenta con oficinas en México, Monterrey y Guadalajara. De los casi 350 empleados en México, un gran número se encentra dedicado a atender las necesidades de seguridad del mercado mexicano en los distintos segmentos productivos (Sector Público, Iniciativa Privada, Proveedores de Servicio, Pequeñas y Medianas Empresas, etc.). Esto, sumado a la amplia cobertura de canales certificados a nivel nacional, nos permite responder a los niveles de servicio que las empresas demandan.

Para mayor información le recomendamos visitar la pag www.cisco.com/security y/o comunicarse al 52671000 en la Ciudad de México.

International Association of Financial Crimes Investigators (IAFCI)

Por Lic. Luis Raúl Vidales Sánchez
Presidente de IAFCI Capítulo México
International Association of Financial Crimes Investigators

Capítulo México

¿Quiénes somos?

IAFCI es una organización sin fines de lucro, cuyo objetivo es prevenir los crímenes financieros, proveyendo recursos para la investigación en un ambiente de intercambio de información, cursos y entrenamiento para la adecuada prevención de fraudes, en beneficio de sus miembros.

IAFCI proporciona a sus miembros una comunicación efectiva en un ambiente seguro para promover el intercambio de información, redoblando esfuerzos para aprender y perseguir a los criminales.

Nuestra Historia

En 1968, un grupo de investigadores de fraudes de tarjetas de crédito y algunas autoridades, organizaron y formaron la *Association of Credit Card Investigators,* (ACCI), expandiéndose en 1974 a la *International Association of Credit Card Investigators,* (IACCI).

Más tarde, en 1996, nuestros miembros reconocieron que los métodos para cometer fraude se estaban modificando, convirtiéndose en fraudes financieros, lo que hacía necesario el intercambio de información sensible en un ambiente seguro. Muchos cambios importantes se hicieron en la organización a partir de entonces, hasta llegar a convertirnos en la International *Association of Financial Crimes Investigators* (IAFCI).

Nuestra Misión

La Asociación es una organización internacional sin fines de lucro, que provee servicios y un ambiente en el cual la información acerca de los fraudes financieros, investigación de fraudes y prevención de métodos de fraude, será recolectada, intercambiada y mostrada en beneficio de la industria financiera y de nuestra sociedad global.

Nuestra Visión

La Asociación cree firmemente en la filosofía de que todo fraude con cheque, tarjeta o financiero en general, deberá ser investigado y perseguido.

La expansión de IAFCI es reflejo del uso y aceptación de la Asociación a través del mundo. Capítulos locales y regionales han sido formados alrededor de todo el mundo. Nuestros miembros provienen de los segmentos de la comunidad financiera, sector legal y privado, nuestro objetivo es detener los fraudes financieros y colaborar con los diferentes organismos de impartición de justicia, poniendo a disposición de los mismos, expertos en cada materia.

Capítulo México

Nuestro país no está al margen de la lucha contra la delincuencia, por lo que en el año 2002 un grupo integrado por siete honorables ciudadanos, provenientes de diferentes ámbitos relacionados con el sector financiero, legal y privado, unieron esfuerzos con el fin participar en la lucha contra los delitos financieros desde sus respectivos escenarios, creando así IAFCI Capítulo México, el cual es presidido actualmente por el Lic. Luis Raúl Vidales Sánchez.

IAFCI Capítulo México, se rige por las mismas normas y lineamientos de la sede internacional, y con ese espíritu mantiene sus propios objetivos que son:

a) Fomentar el desarrollo, superación y unión entre los profesionales y/o participantes de las actividades de prevención y combate de ilícitos en el ámbito financiero.

b) Procurar el desarrollo de tecnologías y servicios que permitan la compilación, intercambio y enseñanza de los métodos preventivos y de combate de ilícitos en el ámbito financiero, para proveer un ambiente dentro del cual la información sobre el objeto de asociación pueda fluir confiable y seguramente para el bien común de la industria financiera y la sociedad en general.

c) Procurar la dignificación y honorabilidad de los asociados y sus actividades, vigilando el estricto cumplimiento de las normas éticas en su actuación profesional.

d) Establecer lineamientos éticos y profesionales para el trabajo de la prevención y combate de ilícitos en el ámbito financiero y la conducta de los asociados, así como patrocinar e impulsar la observancia de los mismos.

e) Publicar y distribuir libros, folletos, revistas, periódicos y artículos de apoyo para los objetivos y actividades de la sociedad, recopilar y mantener listas, registros y archivos de aquellas personas que sean responsables y promover y llevar a efecto las funciones de prevención y combate de ilícitos en el ámbito financiero; establecer y administrar tantos comités y oficinas como sean necesarios o complementarios para las actividades de la Sociedad (dentro del territorio nacional).

f) Realizar encuestas, sustentar conferencias, simposiums, seminarios y foros y planear la presentación de disertaciones y pláticas sobre aspectos y problemas de prevención y combate de conductas ilícitas en el ámbito financiero.

Porque nuestra razón es promover el intercambio de experiencias y conocimientos para limitar los crímenes financieros.

Si el tema es de su interés, visite nuestra página internacional: www.iafci.org o bien contáctenos al correo electrónico: *capitulomexico@iafcimex.org*

Funciones del SOC

Por Emmanuel Ruiz Mora
Chief Information Security Officer
KIO Networks

KIO Networks provee servicios administrados de seguridad, así como de consultoría. Dichos servicios están basados en un grupo de consultores con certificados (CISSP/CISA, etc.), en un centro de operaciones de seguridad (SOC), así como en una sólida infraestructura de aplicaciones instaladas.

Las instalaciones de KIO Networks México y KIO Networks Querétaro, cuentan con sistemas de vigilancia y acceso de ultima generación, como son los accesos a áreas restringidas a través de lectores de huella o iris. Los sistemas de misión critica, así como el suministro eléctrico y enlaces de comunicación, son redundantes, lo que nos permite contar con una disponibilidad del 99.999%

El SOC de KIO Networks es el encargado de supervisar y administrar en tiempo real, desde un único lugar centralizado y bajo un esquema de 7x24x365, todos los aspectos de la seguridad de sus clientes, dentro de los cuales van incluidas soluciones como seguridad perimetral, administración de reglas de seguridad para FW's, Antivirus, IDS, IDP, Proxys, control de acceso, administración de identidades, sistemas de autenticación, entre otros, los cuales han sido implementados en las diversas arquitecturas de seguridad de nuestros clientes.

Para poder llevar acabo esta tarea, los ingenieros del SOC de KIO Networks, aparte de trabajar bajo los lineamientos que las mejores prácticas de la industria de TI recomiendan y de encontrarse certificados en la mayoría de las plataformas que ofrecen los principales fabricantes de seguridad, cuentan con herramientas de monitoreo de última generación.

El uso de estas herramientas ayuda a los ingenieros del SOC a medir en tiempo real aspectos como disponibilidad, capacidad e integridad de los equipos, logrando ser pro-activos en la detección y resolución de la mayoría de los incidentes de seguridad y salvaguardando las operaciones de nuestros clientes.

Uno de los servicios de seguridad perimetral que KIO ofrece a sus clientes, es el de virtualización de Firewalls. Este servicio ofrece a nuestros clientes la capacidad de contar con un FW en alta disponibilidad (*load balancing*), con sistema de prevención y detección de intrusos incluido.

Por otra parte, la adquisición del servicio de FW's virtuales le genera a nuestros clientes un ahorro económico. Esto debido a que el cliente ya no tiene que preocuparse por comprar las cajas para implementar un FW en alta disponibilidad, las cuales, aparte de generarle los costos de compra, licenciamiento y mantenimiento de los equipos, le consumen espacio físico dentro de su *site*.

Otra de las funciones del SOC de KIO Networks es la de verificar que los nuevos servicios o aplicaciones de nuestros clientes, que van a entrar a su ambiente de producción, se encuentren libre de "huecos de seguridad". Por tal motivo el SOC se encarga de auditar los servicios o aplicaciones antes de su ingreso a producción, ejecutando "Escaneos de Vulnerabilidades".

Estos "Escaneos de Vulnerabilidades" nos generan un panorama de cómo se encuentra configurado el equipo y sobre todo de las correcciones que se deben llevar a cabo para que el servicio o aplicación entre a producción bajo un esquema controlado y libre de vulnerabilidades. Esto al final da como resultado la tranquilidad de nuestros clientes.

En caso de que nuestros clientes deseen que los escaneos de vulnerabilidades se realicen de manera recurrente, contamos con las herramientas para calendarizar y ejecutar estos escaneos de manera automática y en el horario que al cliente mas le convengan. Al finalizar, el SOC de KIO Networks emite un reporte con las vulnerabilidades encontradas.

Es así como el SOC de KIO Networks se encuentra preparado para cubrir la demanda de los servicios de seguridad de la información que los clientes requieran, diseñando y administrando soluciones que tengan como resultado el proteger la confidencialidad, integridad y disponibilidad de la información, basados siempre en las mejores prácticas de la industria y, sobre todo, con la confiabilidad y seguridad que KIO Networks ofrece.

La Alta Dirección como pieza clave de la seguridad de la información

Por Beatriz E. Sánchez Rodríguez,
ISO27001LA
Consultor
Secure Information Technologies

En el entorno actual, las tecnologías de la información son vitales para las empresas, principalmente para sus procesos más críticos, que es donde se encuentra la información más valiosa. Siendo así, llama la atención la diferencia de percepción con respecto a la seguridad de la información entre las respuestas de los Informáticos y los No-Informáticos. Si más del 90% de los No-Informáticos creen que la seguridad de la información es importante o muy importante en la empresa, ¿por qué los Informáticos no muestran la misma convicción?

Podemos encontrar muchas razones por las que esta discrepancia puede ocurrir, incluyendo la falta de comunicación entre el negocio y el departamento de TI, la falta de compromiso de la Alta Dirección hacia la seguridad, la carencia del departamento de TI para entender su papel en el negocio, la deficiencia de la Alta Dirección para entender cómo TI puede ayudar a la empresa y muchas más. Sin embargo, lo que esta discordancia indica, en general, es una falla en el gobierno de la empresa y el gobierno de TI, empezando por una falta de alineación de los objetivos de TI con los objetivos del negocio.

Este tema debe tratarse no sólo para la seguridad de la información, sino para todos los objetivos y requerimientos del negocio que deben proveer dirección y estar claramente definidos a lo largo de la organización. En el caso de TI, un apropiado gobierno asegura que sus objetivos estén alineados con los de la empresa, que las responsabilidades estén claramente definidas, que TI genere valor a la organización, que los recursos se utilicen óptimamente y que los riesgos sean administrados.

Las acciones de TI deben estar basadas en la dirección proporcionada por objetivos de negocio específicos y los requerimientos necesarios para alcanzarlos. Los requerimientos del negocio, incluyendo los de seguridad, deben ser comunicados y deben reflejarse en las metas de TI para poder satisfacerlos y, a su vez, lograr los objetivos del negocio. El desempeño deberá medirse para aportar retroalimentación y así poder trabajar en los puntos de oportunidad y presentar resultados de progreso a la Alta Dirección.

Para alcanzar esto, existen estándares y guías que proveen un marco de referencia e incorporan las mejores prácticas en la industria. Uno de los más reconocidos internacionalmente en el tema de Gobierno de TI es COBIT, creado por el "IT Governance Institute" (ITGI). Además, la mayoría de los estándares de seguridad de la información con mayor reputación, incluyendo ISO/IEC 27001, tratan el tema de la importancia de que la Alta Dirección esté involucrada, mostrando compromiso y una clara dirección y asegurando que las metas alcanzadas se encuentren alineadas con las metas del negocio. Siendo así, ¿por qué no aprovechar el conocimiento de los expertos para mejorar el desempeño de la empresa?

Las tecnologías de la información, en conjunto con la adecuada seguridad de la información, pueden volverse impulsores de la empresa con la participación de la Alta Dirección, al integrar sus propuestas y procesos de negocio con la administración de la seguridad y la tecnología. Una vez que el negocio y TI tengan la misma visión sobre los requerimientos y objetivos, su relación se volverá más constructiva y ambos trabajarán en armonía para que la empresa obtenga los resultados esperados. Así, la organización puede extraer el potencial que ofrece la tecnología, al mismo tiempo que se administran los riesgos, para obtener soluciones seguras y de beneficio que fortalezcan al negocio y le permitan generar ventajas competitivas.

Concientización y conocimiento, grandes aliados para la Seguridad de la Información

Por Héctor Federico Gutiérrez Eriksen,
ISO27001LA
Consultor
Secure Information Technologies

"Invertir en conocimientos produce siempre los mejores beneficios."
Benjamín Franklin

Uno de los puntos que comúnmente se busca reforzar en las empresas, con respecto a la Seguridad de la Información, es la concientización. Ésta siempre resulta ser uno de los más grandes retos, no sólo con los usuarios, también con las mismas áreas de sistemas. Por lo regular, creemos que al usuario es al que tenemos que obligarle a tomar conciencia de lo que hace y cómo lo hace.

El estudio de percepción cambia esto, nos damos cuenta que los usuarios o aquéllos que no están inmersos en las áreas de sistemas, son los más interesados y los que están más preocupados por estos temas. Con sólo ver la pregunta sobre la importancia de la seguridad informática, la mayor parte de los No-Informáticos respondió que es muy importante, lo cual nos hace ver que tal vez el enfoque tiene que cambiar.

Pensamos que lo más complicado es hacer entender al usuario los riesgos de la información que usa y genera. Sin embargo, es recomendable cambiar el enfoque. Si ahora sabemos que le interesa el tema al usuario, nos tenemos que preocupar por darle las herramientas y el conocimiento necesario para que sea él quien tome las riendas de ese conocimiento, el control de su información y, sobre todo, que asuma su responsabilidad de identificar qué información es más importante, crítica, sensible y valiosa; debemos trabajar en conjunto con los Informáticos para asegurar que ésta sea protegida y resguardada.

La concientización debe cambiar su enfoque para hacer entender al usuario que las áreas de Informática están ahí para apoyar y empujar el mejor uso de los sistemas, no sólo respecto a la Seguridad de la Información, sino también en todos los demás ámbitos dentro de su competencia

El tema de concientizar a los usuarios se suele ver, dentro de las áreas de sistemas, como una tarea adicional que pocos están dispuestos a asumir y apoyar, se ve más como una carga que como una oportunidad de negocio y de mejora. Sin embargo, debemos tomar en cuenta que atacando los problemas con conocimiento, podemos ahorrar muchos problemas a futuro, estén o no relacionados con la seguridad de la información. Entendiendo que podemos aprovechar y alentar ese interés, podemos tomar ventaja y enfocar de una mejor manera los temas y la forma de realizar esa concientización.

También podemos ver que existe mucho interés sobre una gran cantidad de temas relacionados a la Seguridad de la Información por parte de los No-Informáticos, dada la pregunta "¿Qué más le gustaría conocer?", nos demuestra que proveyendo la información que les interesa podemos ayudar a mejorar el estado entero de seguridad de una organización, a través de la concientización dirigida y específica a esas dudas.

Pero esto también significa que tenemos que abrir foros dentro de las empresas donde las personas puedan encontrar la información que es de su interés y para mejorar y desarrollar una cultura organizacional enfocada a la Seguridad, donde nuevos ataques, métodos y técnicas, se expongan y donde se publiquen anuncios sencillos, comprensibles y confiables.

De esta manera, aquél que comúnmente es el más grande reto, se convierte en nuestro mejor aliado, nos simplifica el trabajo y lo hace más interesante y agradable, convirtiéndose en una buena herramienta para que los usuarios se involucren a un alto nivel en la protección de su información.

Sistemas de Gestión de Seguridad de la Información: Un camino a la madurez de la seguridad

Por Jorge Lozano Tejera,
MSc, CISSP, ISO27001LA, FCNSP
Director de Sistemas
Secure Information Technologies

El poeta Johann Goethe dijo alguna vez: "No basta saber, se debe también aplicar. No es suficiente querer, se debe también hacer." Esta es una realidad por la que atraviesa la seguridad de la información. Con el paso del tiempo, las empresas se han vuelto dependientes de herramientas automáticas y demandan cada vez más de la tecnología, con el fin de mejorar la forma en que operan y hacen negocios.

Ciertamente, las empresas se han vuelto más competitivas y se debaten entre ellas por entregarnos productos y servicios más vanguardistas con tan sólo darle clic a un botón de nuestra PC, del control remoto de la televisión, de nuestro celular o de los ahora electrodomésticos inteligentes.
Toda esta tecnología ha aumentado la cantidad de información que procesamos, intercambiamos y almacenamos, y por lo tanto han aumentado los riesgos asociados con el uso de la misma. Ahora vivimos en un mundo donde hay secuestros virtuales, donde recibimos correos electrónicos intentado obtener nuestra clave de acceso al banco en línea, donde los ladrones entran a través de un cable de red o por la red inalámbrica.

Lo sabemos, nos lo han dicho, incluso lo hemos vivido, pero aún no sabemos qué podemos hacer. Y no es para menos; hace 15 años vivíamos en otro mundo que ahora parece más un sueño; hemos tenido que aprender cosas a una velocidad marcada por el ritmo de los avances de la tecnología, sin tener suficiente tiempo para poder asimilar o incluso visualizar las consecuencias de su uso.
Este estudio ha demostrado, en sus distintas ediciones, la velocidad de la asimilación y entendimiento de la seguridad de la información, y hoy podemos decir que falta más aplicar y hacer, sin descuidar el saber y el querer.

La seguridad de la información consiste en la preservación de las propiedades de confidencialidad, integridad y disponibilidad de nuestra información. Debemos considerar las necesidades reales que cada organización o individuo requieren; de acuerdo al valor que le den a su información; hay que analizar los riesgos a los que ésta se expone para poder implantar soluciones, ya sean estratégicas, operativas o técnicas; hay que planear qué vamos a hacer cuando algo falle; hay que monitorear que las soluciones estén cumpliendo con los propósitos para los cuales fueron implantadas; y finalmente, este ciclo hay que repetirlo periódicamente para mantenernos vigentes y acordes a la realidad en que vivimos.
Es más fácil decirlo que hacerlo; por esto es que desde hace años se han hecho grandes esfuerzos en el desarrollo de estrategias para la administración de la seguridad de la información y gracias a ello es que actualmente contamos con estándares internacionales, como el ISO27001, que nos ayudan a encontrar ese enfoque estructurado y administrado para poder proteger la información.

Muchos me han preguntado: ¿qué tan necesario es un enfoque administrado como el que define ISO27001? Mi experiencia implementando, e incluso ayudando en el proceso de certificación, me ha dicho que de alguna u otra manera todos hacemos una administración de la seguridad de nuestra información; sin embargo, la formalidad y los recursos que invertimos en ella dependen en gran medida de la importancia que tiene la información para cada uno, ya sea en términos de individuos o de organizaciones, del nivel de riesgo con el que queremos convivir y, en el peor de los casos, de una eventualidad que nos haya hecho abrir los ojos a las consecuencias de no hacer un esfuerzo mayor para proteger nuestra información.
Actualmente, casi todas las organizaciones cuentan con alguna herramienta de seguridad como un antivirus y un *firewall* y, sin embargo, siguen teniendo problemas para proteger su información, ya que éstas son sólo un medio pero no el fin. Más allá de contar con lo último en tecnología para proteger nuestra información, se requiere entender el por qué y para qué de dicha tecnología, y es en ese momento cuando empezamos a administrar formalmente la seguridad de la información.

Como consultor en *Secure Information Technologies*, siempre me resulta muy agradable ver cómo una organización mejora su nivel de seguridad cuando empieza a implantar soluciones más administrativas, como el uso de políticas y procedimientos, que complementan las soluciones técnicas con las que ya contaba. Madurar un proceso de administración de la seguridad de la información, en última instancia es un cambio cultural y, como todo camino hacia la madurez, requiere de tiempo, esfuerzo y paciencia, pero una vez que lo adoptamos y nos hacemos de una disciplina, los resultados se podrán percibir desde el momento en que empezamos a aplicar lo que sabemos y a hacer lo que queremos.

Seguridad de la información... De la percepción a la realidad

Por Mario Ureña Cuate,
CISSP, CISA, CISM
Director General
Secure Information Technologies

"Un ave que vuela de la tierra hasta la cima de un hormiguero, no sabe que aún se encuentra en la tierra"
Proverbio africano-

La seguridad de la información se define, generalmente, como la protección de la Confidencialidad, Integridad y Disponibilidad de la información y justo cuando pensamos que ya todos nos pusimos de acuerdo por lo menos en esto, nos encontramos con que el 23.43% de los participantes en el estudio percibe que seguridad de la información = Integridad / Confiabilidad de la información, poniéndola en el sitio #1, pero dejando a un lado las otras dos definiciones. La Confidencialidad/Privacidad alcanza el 4º lugar con el 14.46% de las menciones y finalmente, la disponibilidad se va hasta el #14 de la lista, con solo el 1.83%.

Tal vez, esta es la razón por la que la realidad nos demuestra que son contadas las organizaciones que toman medidas con respecto a la disponibilidad de la información, incluyendo controles tales como un programa de respaldos, resguardo de registros vitales, plan de recuperación en caso de desastre (DRP) y plan de continuidad del negocio (BCP) y seguramente, es por esta misma razón que el estándar BS25999 relativo a la administración de la continuidad del negocio (BCM) tuvo un total de cero menciones.

Por otra parte, los resultados del estudio nos indican que el 82.92% de los No-Informáticos perciben como muy importante la seguridad de la información en su empresa, mientras sólo el 34.73% de los Informáticos tiene la misma percepción.

Este dato resulta relevante, debido a que pareciera existir una falta de alineación de objetivos y prioridades entre dueños, usuarios y custodios de la información, inclusive, el 2.62% de los No-Informáticos define a la seguridad de la información como "trabajar con confianza", concepto que pareciera acercarse más a las necesidades de gobierno de TI que a la propia seguridad de la información.

El *Information Technology Governance Institute* (ITGI), a través de COBIT define siete criterios que debe cubrir la información para satisfacer los requerimientos del negocio: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad, y de acuerdo con su reporte global de gobierno de TI en 2008, para Norte América, sólo el 12% de las organizaciones han implementado procesos y controles relacionados con el gobierno de TI, mientras que el 17% de la misma muestra no considera siquiera la implementación.

En este mismo reporte del ITGI, se menciona que las organizaciones que consideran importante la administración de riesgos de TI utilizan prácticas y estándares tales como ITIL/ISO20000, ISO9000, COBIT e ISO17799/ISO27001 principalmente, los cuales también fueron mencionados dentro de las respuestas de este estudio de percepción.

En la actualidad, los programas de concientización, entrenamiento, educación y certificación, han tomado mayor importancia dentro de los planes de trabajo de las áreas de TI y seguridad de la información, pretendiendo con esto atender los riesgos asociados con una de las amenazas más importantes para la seguridad de la información: las personas dentro de la organización; a quienes, de acuerdo con los resultados de este estudio de percepción, se perciben como "agresores internos" (43.97%), "desconocimiento del usuario" (31.82%) y "negligencia del usuario" (28.25%).

Los resultados también revelan la necesidad de contar con mayor información relacionada con la seguridad de la información, principalmente respecto a los avances y tendencias tecnológicas, se-

guridad de la información en general, información sobre hackers, virus, *hardware* y *software* de seguridad, encripción y cifrado de datos, phishing e ingeniería social, tecnología inalámbrica, seguridad en Internet, riesgos y Planes de Recuperación de Desastres.

Soy testigo de los esfuerzos que están realizando las asociaciones relacionadas con el tema de la seguridad de la información y gran parte de estas necesidades de información pueden ser cubiertas participando en los congresos organizados por dichas asociaciones, asistiendo a los desayunos y eventos especiales que constantemente se llevan a cabo.
Finalmente, considero que en los últimos años, las organizaciones tanto públicas como privadas, en sectores tan diversos como el financiero, manufactura, educación, bursátil, salud, servicios, etc., han realizado esfuerzos importantes y han asignado presupuestos y equipos de trabajo considerables para administrar sus riesgos y mejorar su ambiente de control y protección de su información, sin embargo, apenas estamos en la cima del hormiguero y quedan muchas cosas por hacer.

Mario Ureña es reconocido especialista en seguridad de la información, gobierno, auditoria y control de TI. Es miembro de la mesa directiva de la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI) y Coordinador CISM de la Information Systems Audit and Control Association (ISACA) para el capitulo Ciudad de México.

Algunas asociaciones e instituciones relacionadas con la Seguridad de la Información son:

ALAPSI	Asociación Latinoamericana de Profesionales en Seguridad Informática	www.alapsi.org
ALAS	Asociación Latinoamericana de Seguridad	www.alas.org.mx
BSI	British Standards Institution	www.bsiamericas.com/mexico
CERT	Computer Emergency Response Team	www.cert.org
CSI	Computer Security Institute	www.gocsi.org
CVE-MITRE	Common Vulnerabilities and Exposures	www.cve.mitre.org
DGSCA	Dirección General de Servicios de Cómputo Académico de la UNAM	www.seguridad.unam.mx
ISACA	Information Systems Audit And Control Association (México)	www.isaca.org.mx
ISACA	Information Systems Audit And Control Association (Internacional)	www.isaca.org
ISC2	International Information Systems Security Certification Consortium	www.isc2.org
ISSA	Information Systems Security Association	www.issa.org

SEGURIDAD; UNA CARRERA INTERMINABLE, PERO VIABLE

Por Salomón Arrache
Director de la práctica de Software
Sun Microsystems de México

La seguridad de la información se define, generalmente, como la protección de la Confidencialidad, Integridad y Disponibilidad de la información y justo cuando pensamos que ya todos nos pusimos de acuerdo por lo menos en esto, nos encontramos con que el 23.43% de los participantes en el estudio percibe que seguridad de la información = Integridad / Confiabilidad de la información, poniéndola en el sitio #1, pero dejando a un lado las otras dos definiciones. La Confidencialidad/Privacidad alcanza el 4º lugar con el 14.46% de las menciones y finalmente, la disponibilidad se va hasta el #14 de la lista, con solo el 1.83%.

En este artículo, nos enfocaremos en una parte de la seguridad, ya que escribir sobre todas sus áreas podría ocuparnos varios volúmenes de libros.

El tema que hemos escogido, es el de Fraudes, gobernanza y regulaciones; cómo protegerse, sin perder viabilidad y agilidad de respuesta en el mercado.

Debido a que estadísticamente está comprobado que entre el 50% y el 80% de los ataques vienen de dentro de la empresa, nos centraremos en cómo proteger de estos ataques a la empresa, asegurando así su reputación e imagen, sus activos, reportes, procesos, agilidad y gobernanza y, a través de ésta última, a sus altos ejecutivos, pues son ellos quienes mayores riesgos corren, especialmente en empresas que cotizan en bolsa.

Es innegable que cada día, en más países, las empresas que cotizan en bolsa, están sujetas a más regulaciones, como Sarbanes Oxley, HIPAA, etc., bajo las cuales, tanto el CEO como el CFO, son directamente responsables por las alteraciones en los resultados financieros de la empresa, corriendo riesgos que van desde la pérdida del empleo y penalizaciones económicas, hasta la privación de su libertad, con cárcel.

Esto hace que sea necesario revisar y documentar los procesos de la empresa, los responsables de cada etapa y la supervisión de los mismos, lo que ha generado una atmósfera, rígida y burocrática, que llega hasta la parte de la tecnología en la que se apoyan para generar los resultados de cada periodo financiero y su reporte, restando agilidad a la empresa.

Por otro lado, las mismas empresas, buscan ser más ágiles en la liberación de nuevos productos y servicios al mercado, a través del aprovechamiento de procesos y tecnologías ya desarrolladas y clasificadas como "Servicios" para captar nuevas oportunidades de negocio, bajo la filosofía de SOA, o Arquitectura Orientada a Servicios, por sus siglas en Inglés.

La respuesta es una solución de manejo de identidades y ciclo de vida del empleado, que aporta a la empresa, de una manera ágil y eficiente:

1) Un repositorio de usuarios, enlazados con su perfil de trabajo, y éste a su vez, con las aplicaciones e información que podrán usar, así como la autoridad, que sobre ellas podrán tener, de modo que cada vez que un nuevo empleado sea contratado, o cambie de puesto, éste será dado de alta, o modificado en el sistema, con la idea de construir un ciclo de vida, respetando su perfil predeterminado y hacia donde puede cambiar, con el acceso a aquellas aplicaciones que necesite para desarrollar su trabajo y con la autoridad correspondiente, lo que, además, representa un ahorro de tiempo para Recursos Humanos y una mayor eficiencia para la empresa. Similarmente, cando un empleado sale de la empresa, se da de baja su usuario, eliminando todos sus accesos a las aplicaciones que usaba, en un solo movimiento.

2) Una vez que se cuenta con el repositorio, se pueden implementar los procesos pre-establecidos por la empresa, como por ejemplo, que para modificar una cifra de algún reporte financiero, ésta deberá ser aprobada por determinados funcionarios, en diferentes áreas.

3) Finalmente, puede entonces implementarse junto con estos procesos el disparador de alarmas, cuando alguien no facultado para ello intente modificar información relevante de la empresa, protegiendo así a la misma y a sus funcionarios de intentos de fraudes.

4) Adicionalmente, se pueden correr reportes de auditoría por usuario, área o empresa, para evaluar el desempeño de la misma, deslindando responsabilidades, según los procesos, asegurando el cumplimiento de gobernanza establecido por las legislaciones que apliquen.

Como supondrán, las implementaciones de estas herramientas requieren de la existencia de los procesos adecuados y documentados de la empresa, ya que son éstos los que se automatizarán y monitorearán con base en las definiciones que se hayan acordado y definido oportunamente.

Por lo anterior, es muy importante seleccionar una solución completa que incluya el manejo de roles y segregación de responsabilidades, (analistas de industria, como Gartner, publican su "Cuadrante Mágico" en el que clasifican de acuerdo con tendencias, visión y viabilidad de implementación, a las soluciones líderes del mercado) y recomendable la contratación de una empresa consultora, que cuente con la metodología de implementación de este tipo de soluciones y experiencia en las mismas, para asegurar el éxito de la iniciativa.

Para más información visite: sun.com/identity

Salomón Arrache es Director de la práctica de Software
de Sun Microsystems de México
salomon.arrache@sun.com

Seguridad informática y la protección de la información a través de la prevención

Por Lic. Luis Raúl Vidales Sánchez
Director General
Técnica Comercial Vilsa, S.A.

Hoy en día, en que nos encontramos inmersos en una vorágine de comunicación, el intercambio constante de información es algo tan rutinario, que lo hacemos casi inconcientemente, originando que en muchos casos otorguemos datos importantes que nos ponen en riesgo tanto a nivel personal como profesional.

Nada es más frustrante que el hecho de que, a pesar de contar con las medidas de seguridad mínimas adecuadas, seamos víctimas de aquellos mal intencionados que sólo esperan el más pequeño descuido de nuestra parte para tomar ventaja.

Pero ¿Cómo evitarlo?. Conforme los medios de intercambio de información avanzan eficientándose en funcionalidad e incrementando su velocidad, más brechas de seguridad quedan alrededor del uso de dichos equipos. No importa el nivel de usuario que sea, desde el más entendido hasta el más básico, todos somos víctimas potenciales y la única forma de evitar esto, es a través de la prevención.

Para ello es necesario establecer una cultura de prevención. Técnica Comercial Vilsa ha desarrollado una amplia experiencia en sistemas de prevención de riesgos con base en tecnologías de vanguardia. La labor del equipo de profesionales técnicos y expertos de esta empresa, ha sido fundamental en la seguridad de eventos internacionales; ha participado en el resguardo de la seguridad de 148 diferentes jefes de estado y 151 ministros, así como de altos funcionarios del gobierno de México y otros países.

Técnica Comercial Vilsa posee una vasta experiencia en la instalación de sistemas de seguridad, tanto en el sector público como en el privado, ha desarrollado innumerables sistemas de identificación, acceso, resguardo de información y comunicación de voz y datos. A lo largo de los años, esta empresa ha ofrecido servicios integrales de seguridad y documentos de alta tecnología.

Técnica Comercial Vilsa es una empresa mexicana con reconocimiento a nivel mundial. Esta labor ha sido posible realizarla con la suma de las más diversas tecnologías de vanguardia, que Técnica Comercial Vilsa logró integrar en sistemas de prevención de riesgos y servicios de seguridad del más alto nivel. Con equipos de la más alta tecnología y personal altamente capacitado, con capacidad de respuesta y cubriendo una amplia gama de necesidades, a fin de iniciar una cultura de prevención básica le sugerimos:

1) En general, si puede evitar el uso de mensajeros instantáneos, hágalo.

2) Si por alguna razón se ve obligado a utilizar los servicios de mensajería instantánea, ya sea a través de los programas destinados a ese fin o vía web, procure que sus contactos sean plenamente reconocidos; si le hacen preguntas fuera de lo ordinario, relacionadas con sus rutinas, cuentas de banco o bienes, no responda y trate de ponerse en contacto con la persona con la que usted cree estar hablando en línea, pues quizá han usurpado su cuenta.

3) No permita el acceso a carpetas compartidas en su PC, esto le deja la puerta abierta a cualquiera que desee acceder a su equipo.

4) No instale programas de íconos gestuales animados, estos generan problemas en los equipos que eventualmente provocan la pérdida de información.
5) No proporcione datos personales como su cuenta de correo y/o contraseña en páginas en las que no está seguro de la información que contienen.

6) No acepte contactos que le resulten completamente desconocidos.

7) No reciba archivos de contactos que no le sean confiables.

8) No publique fotografías personales y/o familiares, evite ingresar información personal y familiar en sitios de contacto en donde cualquiera puede acceder y ver su información.

9) Si recibe correos en donde le invitan a acceder a cierta información a través de ligas directas, no lo haga, podrían tomar información personal de su computadora.

10) Evite la tentación de reenviar los correos cadena, ya que al reenviarlos, los envía con las direcciones de sus contactos incluyendo la suya propia.

Asimismo, cuando hablamos de empresas, es necesario implementar una serie de políticas preventivas basadas en las necesidades de cada área en particular, para evitar tanto fugas de información, como la contaminación de la misma.

Para ello es necesario tomar en cuenta los siguientes puntos:

a) Analizar las consecuencias de la pérdida de información en cuanto a costos y productividad, por la pérdida de datos sensibles.

b) Establecer tiempos críticos y niveles de prioridad e importancia para la elaboración de respaldos de información. Estos plazos dependerán de las cargas de trabajo de cada usuario y la relevancia para la empresa de la información que produce y maneja.

c) Identificar y seleccionar por parte de cada usuario la información que se debe proteger, para evitar el desperdicio de espacio en las unidades de almacenamiento extraíbles, en donde se almacenará la información respaldada.

d) Establecer una ubicación física segura y con las condiciones necesarias para almacenar los respaldos.

e) Identificar las diferentes amenazas directas e indirectas, así como la vulnerabilidad de la red y de los equipos compartidos.

f) Analizar los costos de recuperación de la información en caso de perderla y hacer un comparativo de los costos de la implementación de las medidas prevención de pérdida o daño de la información.

g) Implementar planes de emergencia para responder a incidentes y lograr la pronta recuperación para disminuir el impacto en la empresa.

Propiciar una cultura de prevención en nuestras empresas, es la única manera de que éstas operen en un mundo globalizado.

Información sin seguridad, común denominador

Por Enrique Bustamante Martínez
Director General
Fundación Ealy Ortiz, A.C.

Sin lugar a dudas una importante tendencia que la sociedad mundial está adoptando en sus diversas formas, es la información como un vehículo de intercambio en los distintos mercados globales. Los analistas expertos en tendencias mundiales hablan hoy de que, "la moneda de cambio para las nuevas generaciones es la información". "Information must be free" proclaman, y por eso la tendencia a que se distribuya libremente.

Como es del conocimiento del gran público, el objetivo inicial del Internet, fue militar y posteriormente académico, para el manejo e intercambio de información especializada y principalmente para que entre las grandes universidades, primero en Estados Unidos y después en el mundo, pudiera existir un proceso dinámico que facilitara los procesos de investigación.

Hoy en día esa primera función de la red ha sido superada por una enorme cantidad de nuevos servicios y una importante demanda por mejores tecnologías, tanto en hardware como en software, para el procesamiento de información.

Es importante identificar que los estándares son medidos en millones de bits de información por segundo y en resoluciones de hasta millones de pixeles, con el fin de satisfacer las necesidades de los "nuevos mercados" de entretenimiento, negocios y telecomunicaciones.

Si tomamos en cuenta lo anterior, resulta evidente que el tema de "seguridad informática" se convierte en uno de los tópicos centrales de análisis y preocupación, no sólo en los medios de comunicación, sino en todas las empresas en el mundo.

De acuerdo a estudios realizados en todo el mundo, como una tendencia constante se señala que, la mayoría de los usuarios de Internet, lo emplean para consultar correo electrónico, pero muchos más también para navegar el ciberespacio en la búsqueda de información de diversa índole. Entre los usos no académicos destaca la búsqueda de entretenimiento, la transferencia e intercambio de archivos e información, la creación de espacios virtuales para realizar negocios y, en menor medida pero de forma creciente también, para fines empresariales.
En el caso que nos ocupa, en México ya es posible comprar toda clase de mercancías, pago de impuestos, tomar toda clase de cursos o hasta trabajar a distancia.

No hemos llegado al punto de generar individuos totalmente ajenos a su realidad y viviendo a través de la llamada realidad virtual, con poco o inclusive, sin contacto social, como ha sucedido en algunos lugares del mundo, pero de acuerdo a expertos investigadores de diversas universidades que han dedicado recursos y mucha experiencia en el estudio de este factor, los resultados apuntan a que cada vez más existan redes sociales trabajando en esa dirección, en especial los más jóvenes.

El tema de seguridad informática en las empresas ha llegado a ser motivo de investigaciones dentro de marcos legales del más profundo rigor.

Es un hecho que hasta este 2008 no existe un mecanismo o sistema efectivo de regular y controlar la veracidad y seriedad de t-o-d-a la información que se sube a Internet (sería una tarea

imposible), pero este hecho ha llevado a que muchísimos sitios entreguen información mal estructurada, distorsionada o incluso falsa. Otros logran obtener su contenido a través de otros sitios sin autorización de sus autores, o de la empresa que la genera.

Los estudiosos de la sociología de redes y la conformación histórica del mundo, afirman que, 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 amplia encuesta en donde se pidió a los participantes 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 una antes y después, de la misma manera que ocurrió hace muchas décadas con la invención y popularización de la televisión, el teléfono o 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. Esta revolución tecnológica ha tenido un crecimiento más acelerado y un impacto mucho más importante, debido a la enorme cantidad de información disponible y la velocidad con que se puede acceder a ésta.

Coincido con aquellos estudiosos de Internet que han afirmado que la red 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.

Por esta razón es fundamental entender que junto con el crecimiento de Internet y el uso cada vez más extendido de las tecnologías de información, se desarrolle una cultura de la seguridad informática que, hasta hoy, nos ha demostrado un retraso y que es considerada fundamental en el desarrollo futuro de un mundo cada vez más interrelacionado.

Seguridad en Dispositivos Móviles: Principales Riesgos y Tips para minimizarlos

Por Juan Francisco Serrano
Director General
Joint Future Systems

JFS

La seguridad en informática no aplica únicamente a las computadoras tradicionales de escritorio y tampoco está limitada a las computadoras portátiles. Cada vez más, la información crítica de una persona se encuentra en un dispositivo pequeño, como por ejemplo teléfonos celulares inteligentes y asistentes digitales personales (PDA's). Cada vez es más común que tengamos todo tipo de documentos, como listas de contactos, listas de clientes, contratos, presentaciones ejecutivas y prácticamente toda nuestra oficina, en un aparato que no es propiamente una computadora. Conocidos como "handhelds", son aparatos que el usuario tiene consigo todo el tiempo y que tienen funciones de acceso a datos, telefonía, cámaras de video y foto fija, reproductores de música y video, correo electrónico, manejo de documentos, juegos y herramientas de productividad.

Estos dispositivos tienen acceso a diferentes tipos de redes, CDMA, GSM, 3G, Wimax, WiFi, EVDO, Bluetooth, entre otras, con lo cual se vuelven terminales de datos que se pueden ligar directamente a los sistemas de una empresa, lo cual los hace herramientas muy poderosas de trabajo, pero también aumenta los riesgos de seguridad al utilizarlos. En este campo, es responsabilidad del administrador principal de una red determinar los puntos de contacto remoto que deben tener las personas que tengan acceso remoto a ella y limitarlos al mínimo necesario.

Cada vez existen mayores usos para este tipo de aparatos. El acceso a bancos, por ejemplo, en muchas partes del mundo ya puede hacerse vía mensajes de texto. Uno puede consultar saldos, transferir fondos, hacer pagos, comprar acciones y muchas otras actividades, a través de un dispositivo móvil, sin tener que entrar a Internet, lo cual por supuesto es posible con la gran mayoría de estos aparatos.

Al ser pequeños y móviles, es muy fácil que un usuario pierda algún aparato de este tipo, lo cual, además de provocarle pérdida de información, deja expuesta esta información a la persona que lo encuentre o lo haya robado.

Adicionalmente, estos aparatos son susceptibles de ataques informáticos de diversas maneras. Los teléfonos celulares pueden ser utilizados como micrófonos activados de manera remota para espiar a las personas, instalándoles un software, también de manera remota. Personas mal intencionadas pueden monitorear la información que se está transmitiendo a través de un teléfono celular, interceptando tanto la voz como los datos. También se puede "ordeñar" un teléfono celular, copiando toda la información que contiene, de manera remota.

La manera de atacar estos dispositivos es muy similar a los ataques que se hacen con computadoras tradicionales. El programa espía puede transmitirse al dispositivo mediante un correo electrónico, un mensaje de texto, un programa que se transmita directamente desde otro teléfono o escondido dentro de software que el usuario instala en su aparato.

La mayoría de estos dispositivos tienen ya incluidos ciertos elementos de seguridad que el usuario puede activar. Los teléfonos que cuentan con comunicación bluetooth, por ejemplo, pueden apagar dicha función cuando no la utilizan y, además, cuentan con una opción para que no sean visibles para otros equipos, aun cuando tengan la conectividad activada.

Dependiendo del sistema operativo del dispositivo, existen programas que específicamente están diseñados para aumentar la seguridad de los mismos. Warden Security, por ejemplo, funciona bajo Windows Mobile o Palm OS, y permite al usuario encriptar sus datos, ponerle candados al teléfono (inclusive de manera remota, por teléfono, email o mensaje), e inclusive permite de manera remota borrar los datos del dispositivo (tanto de la memoria principal como de tarjetas adicionales de memoria). De esta manera, si uno pierde el teléfono, puede inmediatamente enviar un mensaje al mismo, el cual borrará todo el contenido de datos, antes de que el ladrón tenga acceso a ellos. Una funcionalidad adicional interesante, es la que permite hacer llamadas a través del teléfono, pero sólo a números de emergencia o a un número predesignado por el dueño. Esto permite que si una persona bien intencionada encuentra el teléfono, puede dar aviso al dueño, sin tener acceso a otros datos ni conocer el número telefónico del propietario.

Las tarjetas de memoria portátiles, como memory sticks, tarjetas SD, USB's etc. también cuentan con software especial que permite esconder datos en particiones ocultas y encriptar información.

Estos son algunos consejos prácticos para mejorar la seguridad de los dispositivos móviles:

- No abrir correos o mensajes de personas desconocidas, sobre todo si tienen archivos adjuntos.
- Sólo instalar programas de fuentes reconocidas.
- Evitar bajar tonos, música y protectores de pantalla, sin estar seguros de la fuente.
- Dedicar el tiempo necesario para entender las protecciones que el dispositivo ya tiene instalado de fábrica, cómo y cuándo aplicarlas.
- Instalar *software* de seguridad específico para el dispositivo.
- Apagar el celular cuando se esté en juntas muy confidenciales y pedir que las otras personas hagan lo mismo.
- Limitar la cantidad de información altamente sensible que se encuentra en el dispositivo, dejando sólo la que se requiere para las actividades del día o la semana.
- Tener respaldos de la información importante.
- Evitar tener datos de contacto muy evidentes dentro del teléfono, tanto por razones de seguridad personal como por seguridad empresarial. Es mejor utilizar nombres en clave que tener grabados los nombres de los hijos, por ejemplo.
- Limitar los accesos a información que se tengan a las redes corporativas, por parte de cualquier tipo de dispositivos móviles.
- Tener los datos que se encuentren en dispositivos de almacenamiento masivo portátiles siempre encriptados y en particiones ocultas.

A medida que nuestra sociedad se vuelva más conectada electrónicamente, en donde vamos a tener acceso a las redes de información mundial en prácticamente cualquier lugar en el planeta, y a medida que los dispositivos se vuelvan cada vez más poderosos, aumentará el riesgo del manejo inadecuado de la información. Se espera que la protección inherente a los dispositivos sea cada vez mejor, pero nunca podrá ser independiente de un uso adecuado por parte del usuario.

Si desea saber algo más sobre el tema, enviar correo a *corp@jfs.com.mx.*

Seguridad infantil en Internet: guía útil para padres

Por Alberto Vázquez V.
Catedrático de la
Escuela de Ciencias Económicas y Empresariales
Universidad Panamericana, Campus México

Internet ofrece a niños y jóvenes múltiples oportunidades para explorar nuevas ideas, visitar otras tierras, conocer a otros niños y participar en excitantes juegos.
Sin embargo, también puede ser peligroso.

Contexto

Cada vez más los niños cibernautas, al utilizar una computadora, quedan fácilmente expuestos ante una gran cantidad de información e imágenes disponibles en Internet. Si a esto agregamos que los padres de familia, maestros y otras personas no siempre pueden estar disponibles para prevenir que los niños y jóvenes visiten sitios que contengan material dañino o inaceptable, o para hablar con ellos sobre este tipo de material, la situación se torna compleja.

Además, los niños conforman un segmento de la sociedad altamente comerciable donde los expertos de mercadotecnia concentran sus esfuerzos en recopilar información sobre las preferencias y gustos de los niños con fines comerciales.

Del concepto a la realidad

En Internet, las palabras "dañino" e "inaceptable" se utilizan para describir material pornográfico, palabras obscenas y lenguaje de odio. En esta guía, las utilizaremos también para incluir publicidad e imágenes que manipulan a los niños.

La recopilación de datos de páginas de Internet para niños es sólo una de las preocupaciones que tienen los padres. Otro tema preocupante es el acceso que tienen los niños a sitios de Internet que contienen información no apta para menores: pornografía, obscenidades, violencia y mensajes de odio.

Por otra parte, Internet puede ser un lugar altamente seductor con un ambiente potencialmente manipulador para los niños, donde existen muchas oportunidades de recaudar datos de niños para después mandarles mensajes personalizados.

Muchos niños dicen tener problemas con otros usuarios en los cuartos de chateo. La mayoría de los problemas son profanidades; solicitudes de contraseña entre usuarios; solicitud de información como nombre, dirección, teléfono y correo electrónico; propuestas amorosas y visitas de adultos pretendiendo ser niños.

Guía para padres

La siguiente guía está dedicada a los padres que deseen maximizar los beneficios en el uso de Internet para sus hijos y a la vez minimizar los peligros:

1. Sugerencias sobre seguridad y privacidad

- ***Política sobre la privacidad***. Lea las políticas sobre la privacidad que ofrecen los sitios que visitan sus hijos y enseñe a sus hijos mayores a que hagan lo mismo. Los mejores sitios explican qué tipo de información contienen, el uso que le dan y si usted tiene opciones en tanto a permitirles o no que obtengan información sobre sus hijos.

- ***Sellos.*** Busque en la página principal un "sello de garantía" de privacidad como TRUSTe *(www.truste.org)*. La organización *Council of Better Business Bureaus* también cuenta con un programa de "sellos de garantía" *(www.bbbonline.org)*.

- ***Contratos.*** Hable con sus hijos y anímelos a responsabilizarse del uso de Internet. La comisión comercial Federal Trade Commission ofrece una sección con sugerencias sobre cómo comunicarse con sus hijos sobre este tema en *www.ftc.gov/bcp/conline/pubs/online/sitesee.htm*

- ***Reglas de familia.*** Establezca reglas familiares sobre el uso de Internet en casa. Por ejemplo, el centro de niños extraviados *National Center for Missing and Exploited Children (www.missingkids.com) s*ugiere:

  - No proporcionar información que pueda identificarlos, como: datos familiares, dirección, número telefónico o nombre de la escuela a la que asisten. Tampoco deben mandar fotos personales o de su familia sin su permiso.

  - Explique a sus hijos que una contraseña jamás debe compartirse con alguien, ni siquiera con una persona que diga que trabaja para la compañía que provee el servicio de Internet.

  - Adviértale a sus hijos que no deben responder a mensajes que amenacen, humillen o que sugieran algo que los incomode. Dígales que le informen sobre estos mensajes a usted.

  - Esté pendiente del uso de Internet a altas horas de la noche, ya que puede ser una alerta de que existe un problema.

  - Convierta el uso de Internet en una actividad familiar. Sitúe la computadora en un cuarto familiar y no en el cuarto del niño o niña.

  - Procure conocer a las "amistades" cibernéticas de sus hijos de la misma manera en que lo hace con otras amistades.

  - Explíqueles que las personas no necesariamente son lo que aparentan ser en línea. Alguien que aparenta ser una niña de 12 años puede ser un señor de 40.

  - Conozca los servicios de Internet que utilizan sus hijos. Si usted no es un usuario hábil de Internet, pídale a su hijo o hija que lo orienten en tanto al tipo de sitios que visitan. O mejor aún, tome clases de Internet y aprenda a navegar.

2. Mercadotecnia en Internet dirigida a los niños

Cuando los niños visitan sitios comerciales, pueden tener la tentación de llenar encuestas a cambio de regalos, inscribirse en clubes, intercambiar información por juegos o simplemente proveer datos personales en cuartos de "chat". Una vez que alguien conozca el nombre de su hijo, es posible que su hijo o hija reciba un correo electrónico de parte de su súper héroe favorito. Puede que los pequeños no sepan diferenciar entre la ficción y la realidad.

Algunos sitios de Internet pueden estar diseñados para recopilar información de manera invisible sobre los intereses de sus hijos, mientras estos "brincan" de un sitio web a otro (*clickstream).* Por lo general activa la inserción de "cookies" en la computadora del niño, lo cual permite que la publicidad especializada comience a aparecer en la pantalla.

Desactive en el navegador de Internet la inclusión de "cookies" (mayor información en *www.privacyrights.org/fs/fs18-cyb.htm)* o consulte la guía de privacidad del centro tecnológico Center for Democracy and Technology en *www.consumerprivacyguide.org*

Programas que bloquean el traspaso de la información personal

Aunque no son totalmente efectivos, el objetivo principal de este tipo de programas de "control paterno" (también conocidos como programas de filtro) es por lo general bloquear sitios pornográficos. Existen otros programas que bloquean información personal como nombre, dirección, números telefónicos, servicios de *"chat"* y de mensajes instantáneos o "instant messaging". Algunos de ellos son *CyberPatrol, CyberSitter y NetNanny.*

Para aprender más sobre este tipo de productos y programas, realice una búsqueda en Internet con las palabras *"parental control software"* o visite *www.getnetwise.org*

Bloqueo de publicidad cuando visiten sitios comerciales

Existen programas como AdDelete y AdWiper que previenen que la publicidad sea dirigida directamente a sus hijos y aceleran la navegación. En www.junkbusters.com/guidescope.html o en *www.junkbusters.com/links.html#More detallan* su uso.

3. Material dañino y servicios de filtración

Existen varios programas de filtrado como *NetNanny, CyberSitter y CyberPatrol.* El sitio de *GetNetWise* enlista sus programas de filtro en la sección de *"tools"* o "herramientas" o en la sección para niños de Yahoo. Yahooligans, provee información para padres e incluye una lista de productos *(www.yahooligans.com/parents).*

Busque programas que:

- Limiten el acceso a Internet durante horas específicas y por tiempo total.
- Den a conocer cuál es el criterio que utilizan para elegir qué sitios serán bloqueados y permitan a los padres leer una lista de éstos.
- Ofrezcan opciones fácilmente accesibles para padres y que puedan ser modificadas para ajustarse a las necesidades personales.
- Permitan al usuario activar o desactivar el programa por medio de una contraseña.
- Se actualicen con frecuencia.
- Bloqueen imágenes (JPEG y GIF) y otras descargas que puedan contener fotos o imágenes con alto contenido pronográfico.
- Filtre obscenidades.
- Bloquee Chats, IRCs y Newsgroups.

Sobre los programas de filtro

Esté consciente de que los servicios de filtraje tienen las mismas limitaciones que los programas de filtro, en tanto al tipo de información que bloquean. Tómese el tiempo necesario para leer cuidadosamente los criterios para filtrar información.

Los padres de familia también pueden canalizar a sus hijos a sitios que proveen el contenido deseado.

Por ejemplo, la asociación de bibliotecas *American Library Association* ofrece una lista de los mejores sitios para niños, como parte de su guía *"Librarianís Guide to Cyberspace for Parents and Kids" en www.ala.org/parentspage/greatsites/guide.html.*

El columnista de periódico Larry Magid ofrece una lisa de sitios de búsqueda para niños*:*
www.safekids.com

Servicios de evaluación

Otro método es elegir sitios que han sido evaluados de acuerdo a los niveles de contenido sexual, desnudez, violencia y lenguaje.

Algunos son:

- Internet Content Rating Association.
  www.icra.org
- SafeSurf, que basa sus evaluaciones en 12 categorías.
  www.safesurf.com
- Entertainment Software Rating Board, cuyo principal objetivo es evaluar videojuegos de computadora.
  www.esrb.net

4. Seguridad para servicios de chat y mensajes instantáneos

Los niños pueden tomar varias medidas para maximizar su privacidad y seguridad mientras visitan un cuarto de chateo.

- Participar en cuartos que están bajo supervisión.
- Utilizar un nombre de pantalla cuyo uso sea exclusivo para chatear y que no contenga información personal.
- Evitar nombres que atraigan atención no deseable como "*sexyteen*".
- No proveer información personal que pueda rastrearse, como el nombre, dirección, número telefónico y nombre de escuela.
- Para obtener mayor información visite *www.irchelp.org*

Muchas de las estrategias de seguridad utilizadas para el chateo pueden utilizarse con los mensajes instantáneos:

- No incluir identificación personal en el perfil del usuario.
- No transmitir información personal en los mensajes.
- Haga clic en la opción que requiere que otros obtengan autorización suya antes de que ellos puedan agregarlo a su lista de contactos.
- Si los usuarios utilizan este servicio para transmitir documentos como canciones o fotos, entonces deben tomarse precauciones para prevenir un virus o gusanos cibernéticos.

Para mayor información sobre el comportamiento en cuartos de chateo, consejos para los mensajes instantáneos y la seguridad en Internet, visite el sitio *web de CyberAngels (www.cyberangels.org/101/index.html)* o el sitio web de *WiredPatrol (www.wiredpatrol.org/wiredhelp/internet101/index.html).*

5. Privacidad en Internet y otros recursos

- Sitio web para niños de la Federal Trade Commission *www.ftc.gov/bcp/conline/edcams/kidzprivacy*
- Sitio web de seguridad de la FTC que cuenta con la tortuga cibernética Dewie the e-Turtle *www.ftc.gov/bcp/conline/edcams/infosecurity www.ftc.gov/bcp/conline/edcams/infosecurity/espanol.html.*
- GetNetWise. Es una fuente de recursos para padres patrocinada por compañías de Internet y otras organizaciones de interés público *www.getnetwise.org.*
- Guía de TRUSTe para la privacidad en línea para padres y maestros *www.truste.org/education/users_parents_teacher_guide.html*
- I-Safe. Organización sin fines de lucro que enseña seguridad en Internet en las escuelas. *www.isafe.org*
- Media Awareness Network ofrece juegos interactivos infantiles en su sitio y por medio de un CD-ROM. *www.media-awareness.ca/eng/cpigs/cpigs.htm*
- Organización National Consumers League *"Essentials for Children Online" www.natlconsumersleague.org/essentials/family.html*
- National Center for Missing and Exploited Children ofrece una guía titulada *"Child Safety on the Information Highway" (Seguridad infantil en Internet) www.missingkids.org*

- SafeKids es un servicio del columnista de periódico Larry Magid, donde incluye varios de sus artículos sobre la seguridad de adolescentes.
  www.safeteens.com.

- Familia de sitios WiredSafety, que ofrecen varios recursos para padres, niños y autoridades.
  www.wiredsafety.org,
  www.wiredpatrol.org,
  www.wiredkids.org/index2.html

Conclusiones

No existen soluciones fáciles para asegurar que su hijo tenga una experiencia cibernética sin toparse con algunos peligros, ni existen programas cien por ciento confiables y en vista de que no puede sustituirse la supervisión de un adulto.

Por otra parte, tome en cuenta que un niño con habilidades computacionales puede "encontrar un camino para llegar a contenido no deseable", por lo tanto, la mejor manera de asegurar que las actividades cibernéticas de sus hijos sean positivas, requieren de un verdadero programa de seguridad y prevención cibernética integrado a una estrategia efectiva de comunicación padre-hijo.

Alberto Vázquez V. es catedrático de la Escuela de Ciencias Económicas y Empresariales de la Universidad Panamericana, Campus México y autor del libro Internet para la MpyME.

Para cualquier información adicional, contactarlo en:
avazquez@up.edu.mx